

SEGUNDO CICLO DE ESTUDOS
CRIMINOLOGIA

**DIFERENÇAS INDIVIDUAIS ENTRE
HACKERS E *NÃO-HACKERS* E ENTRE
HACKERS BLACK HAT, WHITE HAT E
*GREY HAT***

Maria Filipa Freire Carapinha Canudo

M

2024

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 e co-orientação do Professor Doutor Samuel Moreira.



Resumo

A acentuada evolução tecnológica leva à criação de novos comportamentos criminais, surgindo o *hacking*. Este pode ser visto, de forma abrangente como “o acesso, autorizado ou não, a sistemas informáticos” (Holt, 2007), englobando propósitos éticos e não éticos. Existem ainda muitas lacunas na investigação científica quando a este fenómeno. Procurando colmatar algumas destas, este estudo tem como objetivo explorar as diferenças individuais que relevam para a prática de *hacking* e para a prática de diferentes tipos de *hacking* (*black hat*, *grey hat* e *white hat*). De forma a alcançar este objetivo, foi construído e aplicado um inquérito a uma amostra de 593 indivíduos, tendo o mesmo sido divulgado por universidades, fóruns e empresas de informática. Havendo um enfoque em variáveis individuais, foram analisadas variáveis sociodemográficas, autocontrolo, traços de personalidade (recorrendo ao Modelo *Big Five*, de Costa & McCrae, 1992 e ao Modelo *Dark Triad*, de Paulhus & Williams, 2002) e motivações para a prática de *hacking*. No total, 20.4% (n=121) dos participantes reportou ter praticado pelo menos um comportamento de *hacking* nos últimos 12 meses. Destes, 17.4% autoidentificaram-se como *black hats*, 24.4% como *grey hats* e 58.1% como *white hats*. Os resultados demonstram que os *hackers* tendem a ser do sexo masculino, mais jovens e a estudar ou a trabalhar na área informática. Apresentam também um menor autocontrolo. Relativamente aos traços de personalidade, apresentam menor agradabilidade e maior neuroticismo, maquiavelismo e psicopatia. Face às diferenças entre os tipos de *hackers* observou-se que, em termos sociodemográficos, os *white hat* encontram-se mais envolvidos na área informática e os *black hat* menos. O autocontrolo revelou-se mais baixo nos *black hats* e mais alto nos *white hats*, tal como a agradabilidade. Finalmente, o maquiavelismo e a abertura à experiência foram mais elevado nos *black hat* e mais baixo nos *white hat* e o narcisismo foi mais elevado nos *grey hat* e mais reduzido nos *black hat*. Finalmente, no que diz respeito às motivações, “proteger e defender” e “fazer o bem/ajudar os outros” foram as motivações mais importantes para os *white hat* e menos importantes para os *black hat*, enquanto a “procura de sensações” foi significativa, sendo mais importante nos *black hat* e menos nos *white hat*.

Palavras-chave: hackers; personalidade; black hat; white hat; grey hat; autocontrolo

Abstract

The sharp rise in technological developments has led to the creation of new criminal behaviors, with the emergence of hacking. Hacking can be seen broadly as ‘access, authorized or not, to computer systems’ (Holt, 2007), encompassing both ethical and unethical purposes. There are still many gaps in scientific research regarding this phenomenon. In an attempt to fill some of these gaps, this study aims to explore the individual differences that are relevant to the practice of hacking and to the practice of different types of hacking (black hat, grey hat and white hat). To achieve this, a survey was constructed and applied to a sample of 593 individuals, sent to universities, forums and IT companies. With a focus on individual variables, sociodemographic variables, self-control, personality traits (using the Big Five Model by Costa & McCrae, 1992 and the Dark Triad Model by Paulhus & Williams, 2002) and motivations for hacking were analyzed. In total, 20.4% (n=121) of the participants reported having practiced at least one hacking behavior in the last 12 months. Of these, 17.4% self-identified as black hats, 24.4% as grey hats and 58.1% as white hats. The results show that hackers tend to be male, younger and studying or working in IT. They also have less self-control. In terms of personality traits, they are less agreeable and more neurotic, machiavellian and psychopathic. As for the differences between the types of hackers, it was observed that, for sociodemographics, white hats are more involved in IT and black hats less so. Self-control was lower in black hats and higher in white hats, as was agreeableness. Finally, Machiavellianism and openness to experience were higher in black hats and lower in white hats and narcissism was higher in grey hats and lower in black hats. Finally, regarding motivations, “protect and defend” and “do good/help others” were the most important motivations for white hats, contrary to black hats, while sensation-seeking was significant, being more important for black hats and less for white hats.

Keywords: hackers; personality; black hat; white hat; grey hat; self-control

Agradecimentos

Gostaria de expressar a minha profunda gratidão aos meus orientadores, Doutora Inês Guedes e Doutor Samuel Moreira, cujo apoio inabalável, orientação e valiosas contribuições foram fundamentais para a realização desta tese. A vossa paciência, conselhos e dedicação foram uma motivação ao longo de todo o processo. Agradeço por estarem sempre disponíveis para discutir ideias, oferecer *feedback* construtivo e encorajar sempre a superação dos desafios que se foram apresentando no decorrer deste ano. Sem a vossa orientação, este trabalho não teria sido possível. Muito obrigada por acreditarem em mim e por serem verdadeiros mentores e exemplos académicos.

Ainda, a todos, particularmente família e amigos que, direta ou indiretamente, me motivaram e contribuíram para a concretização desta tese, o meu sincero agradecimento.

Lista de abreviaturas e acrónimos

BAC – Baixo autocontrolo

DDoS – *Distributed Denial of Service*

TIC – Tecnologias de Informação e Comunicação

TGC – Teoria Geral do Crime

TMRC – *Tech Model Railroad Club*

Índice

RESUMO.....	II
ABSTRACT	III
AGRADECIMENTOS.....	IV
LISTA DE ABREVIATURAS E ACRÓNIMOS	V
INTRODUÇÃO	1
CAPÍTULO I: ENQUADRAMENTO TEÓRICO	2
1. A INTERNET E O CIBERCRIME	2
2. O <i>HACKING</i> E OS <i>HACKERS</i> : CONCEPTUALIZAÇÃO	4
2.1. A evolução do hacking por décadas	4
2.2. Conceptualização atual	6
2.3. Tipologia de hackers	8
2.3.1. Black Hats, Grey Hats e White Hats	11
3. CARACTERÍSTICAS INDIVIDUAIS EXPLICATIVAS DO <i>HACKING</i>	14
3.1. Características sociodemográficas	14
3.2. Motivações.....	17
3.2.1. Diferenças entre hackers white hat, grey hat e black hat a nível das motivações	18
3.3. Baixo Autocontrolo.....	19
3.4. Fatores da Personalidade	22
3.4.1. Traços de Personalidade do Modelo Big Five	22
3.4.1.1. Diferenças entre hackers white hat, grey hat e black hat a nível do Modelo dos Cinco Fatores da Personalidade	25
3.4.2. Traços de Personalidade do Modelo Dark Triad	26
3.4.2.1. Diferenças entre hackers white hat, grey hat e black hat a nível da Dark Triad ..	28
CAPÍTULO II – ESTUDO EMPÍRICO.....	29
1. OBJETIVOS DO ESTUDO	29
1.1. Objetivos gerais e específicos.....	29
1.2. Hipóteses de Investigação	29
2. DESENHO DA INVESTIGAÇÃO.....	30
3. AMOSTRA E AMOSTRAGEM.....	31
4. OPERACIONALIZAÇÃO DAS VARIÁVEIS E CONSTRUÇÃO DO QUESTIONÁRIO.....	31
4.1. Construção do questionário.....	32
Grupo I – Questões sociodemográficas	33
Grupo II – Prática de hacking	34
Grupo III – Tipo de <i>Hacking</i> praticado	35
Grupo IV - Motivações	38

Grupo V – Medição de Baixo autocontrolo.....	38
Grupo VI – Medição de traços de personalidade do Modelo Big Five	39
Grupo VII – Medição dos traços de Personalidade do Modelo Dark Triad	40
5. PROCEDIMENTOS DE RECOLHA DE DADOS	40
6. PROCEDIMENTOS ESTATÍSTICOS	41
6.1. Criação da Base de Dados	41
6.2. Screening	41
6.3. Estatística Descritiva	42
6.3.1. Análise Fatorial	42
6.3.2. Testes de fiabilidade	43
6.3.3. Estatística univariada	43
6.3.4. Estatística bivariada	43
6.4. Estatística Inferencial	44
CAPÍTULO III – RESULTADOS DO ESTUDO EMPÍRICO	45
1. CARACTERIZAÇÃO DA AMOSTRA	45
1.1. CARACTERIZAÇÃO COM BASE NAS VARIÁVEIS SOCIODEMOGRÁFICAS	45
1.2. Caracterização com base nas variáveis individuais do BAC e traços de personalidade	47
2. DIFERENÇAS ENTRE HACKERS E NÃO-HACKERS.....	48
2.1. Diferenças sociodemográficas	49
2.2. DIFERENÇAS INDIVIDUAIS A NÍVEL DE AUTOCONTROLO E TRAÇOS DE PERSONALIDADE ...	51
3. MOTIVAÇÕES DOS HACKERS	52
4. REGRESSÕES LOGÍSTICAS	53
4.1. Modelo 1: Características sociodemográficas	53
4.2. Modelo 2: Características individuais com base no autocontrolo e traços de personalidade	54
4.3. Modelo 3: Modelo final	55
5. DIFERENÇAS ENTRE GRUPOS DE HACKERS (BLACK HAT, GREY HAT, WHITE HAT).....	56
5.1. Diferenças sociodemográficas	56
5.2. Diferenças individuais a nível de autocontrolo e traços de personalidade	59
5.3. Diferenças a nível de motivações	61
CAPÍTULO IV – DISCUSSÃO.....	63
A) DIFERENÇAS ENTRE HACKERS E NÃO-HACKERS	63
B) DIFERENÇAS ENTRE HACKERS BLACK HAT, GREY HAT E WHITE HAT	69
6. LIMITAÇÕES E LINHAS DE INVESTIGAÇÃO FUTURAS	74
REFERÊNCIAS BIBLIOGRÁFICAS	75
ANEXOS	83

ANEXO I: QUESTIONÁRIO	83
ANEXO II: CODIFICAÇÃO DAS VARIÁVEIS	100
ANEXO III – MODELO EXPLICATIVO DA PRÁTICA DE HACKING COM BASE NAS VARIÁVEIS SOCIODEMOGRÁFICAS	106
ANEXO IV – MODELO EXPLICATIVO DA PRÁTICA DE HACKING COM BASE NAS VARIÁVEIS INDIVIDUAIS – AUTOCONTROLO E TRAÇOS DE PERSONALIDADE	107

Índice de tabelas

Tabela 1 - Caracterização da amostra segundo as variáveis sociodemográficas.....	45
Tabela 2 - Caracterização da amostra segundo as variáveis individuais.....	47
Tabela 3 - Caracterização da amostra segundo a prática de <i>hacking</i>	48
Tabela 4 - Comparação de médias de idades entre hackers e não-hackers.....	49
Tabela 5 - Comparação de proporções entre a prática de <i>hacking</i> e as variáveis sociodemográficas categóricas.....	50
Tabela 6 - Comparações de médias entre hackers e não-hackers ao nível das variáveis individuais de autocontrolo e traços de personalidade.....	51
Tabela 7 - Caracterização da subamostra de <i>hackers</i> segundo as motivações para o <i>hacking</i>	53
Tabela 8 – Modelo explicativo final da prática de <i>hacking</i>	55
Tabela 9 – Caracterização da subamostra de <i>hackers</i> com base no tipo de <i>hacking</i> que praticam.....	56
Tabela 10 – Comparação a nível da variável idade entre os tipos de <i>hackers</i>	57
Tabela 11 – Comparação de proporções entre os tipos de <i>hackers</i> e as variáveis sociodemográficas categóricas.....	58
Tabela 12 – Comparações a nível de autocontrolo e traços de personalidade entre tipos de <i>hackers</i>	59
Tabela 13 – Comparações entre tipos de <i>hackers</i> a nível das motivações.....	60

Introdução

Nas últimas décadas, tem-se assistido a diversas mudanças nas interações entre indivíduos, possibilitada pelo avanço e desenvolvimento tecnológico. Apesar das inúmeras vantagens trazidas pela tecnologia, esta veio também possibilitar novas formas de crime para além das tradicionais (Wall, 2007), nomeadamente, o *hacking*. Devido ao seu carácter danoso, o *hacking* tornou-se um problema generalizado na Era da informação (Back *et al.*, 2018). Em 2023 o custo estimado de apenas uma violação de dados foi de 4.45\$ milhões (Cybersecurity Ventures, 2023), número problemático tendo em conta a crescente prevalência do fenómeno, não só internacionalmente, mas também em Portugal. O Relatório Anual de Segurança Interna (IASI) de 2021, apresentou um total de 632 ofensas participadas de acesso indevido ou ilegítimo/interceção ilegítima, ao passo que em 2023 foram registadas 1141 ofensas do mesmo tipo. Apesar de necessário, o estudo do *hacking* enfrenta desafios acrescidos, sendo um fenómeno que possui um elevado número de cifras negras e, como tal, é difícil conseguir retratá-lo de forma aproximada à realidade (Richardson, 2008). A segmentação em tipos de *hacking* (*e.g.*, ético e não ético) leva a uma dificuldade ainda maior de chegar à prevalência deste fenómeno, sendo que as estatísticas oficiais retratam apenas o *hacking* criminoso. Não obstante o seu rápido crescimento, a investigação científica a respeito deste é ainda escassa e demarcada por inconsistências. Particularmente, em Portugal, é quase inexistente. Desta feita, o presente estudo pretende abordar o *hacking* de uma maneira abrangente, procurando entendê-lo nas suas várias manifestações e não apenas o malicioso. Como tal, procura-se aceder diretamente aos *hackers* e compreender, a nível individual, o que os distingue não só de não-*hackers*, mas também como se diferenciam entre si, partindo da tipologia de Moore (2015) que os divide em *hackers black hat*, *grey hat* e *white hat*.

Esta dissertação divide-se em quatro capítulos principais: no primeiro capítulo fornece-se uma revisão bibliográfica acerca do fenómeno, passando pela sua evolução, desde a emergência até à sua conceção atual e explorando as várias manifestações do *hacking*, a nível de diversas tipologias e motivações. O maior enfoque será a exploração do que caracteriza os *hackers* e cada tipo de *hacker*, de acordo com variada bibliografia, tomando, assim, uma abordagem individual, analisando-se: 1) características sociodemográficas; 2) o autocontrolo; 3) os traços de personalidade; e 4) as motivações. Esta revisão servirá para orientar a formulação dos objetivos e hipóteses do estudo, presentes no capítulo II, que inclui ainda a metodologia adotada para ir de encontro aos

mesmos, descrevendo detalhadamente as medidas e forma de construção do questionário final, bem como procedimentos seguidos. Seguem-se, no Capítulo III, os resultados obtidos com a aplicação deste mesmo questionário e, por fim, no Capítulo IV realiza-se uma apreciação crítica dos achados principais, analisados à luz das hipóteses elencadas e recorrendo a bibliografia que ofereça a melhor justificação para os resultados alcançados, quer estejam, ou não, de acordo com o previsto. Ainda neste capítulo, conclui-se o presente trabalho, com algumas considerações finais a respeito de possíveis limitações encontradas ao longo da realização deste projeto, implicações e sugestões para linhas de investigação futuras.

CAPÍTULO I: ENQUADRAMENTO TEÓRICO

1. A Internet e o Cibercrime

A *Internet* foi criada nos anos 60, tendo captado a atenção de governos e criminólogos apenas em meados de 1990, ao tornar-se um meio de grande escala para a população em geral (Koops, 2011). Esta merece um cuidado especial, pelas suas variadas características, nomeadamente o seu carácter global e o facto de possibilitar ligações em tempo real entre indivíduos, independentemente da sua localização (Koops, 2011), podendo ser definida como uma “rede de redes” (Castells, 2002, p.11). Desta forma, tempo, distância e fronteiras nacionais são facilmente transponíveis e perdem a importância que lhes é dada no crime tradicional. Como rede digital, a *Internet* possibilita o processamento de dados e de informação de forma automatizada e numa escala sem precedentes. Assim, devido às características previamente elencadas, a *Internet* oferece não só a possibilidade de estender a prática de crimes já existentes, mas também de fomentar a criação de novas formas de crimes merecendo, portanto, uma especial atenção por parte da Criminologia, bem como da lei e política criminal (Koops, 2011).

A criação e evolução da *Internet* leva à existência de um novo local, que se destaca pela falta de uma presença física, o ciberespaço. Nye (2010, p.3), descreve o ciberespaço como uma “*Internet* de computadores em rede”, mas também de “*intranets*, tecnologias relacionadas com telemóveis, cabos de fibra ótica e comunicações espaciais”. O ciberespaço refere-se, assim, não só a “todas as redes de computadores do mundo”, mas também a “tudo o que estas conectam e controlam” (Clarke & Knake, 2010, p.57). Atualmente, existem 5.44 mil milhões de usuários no ciberespaço (DataReportal, 2024)

e é estimado que este número suba para mais de 7.5 mil milhões, até 2030 (Cybersecurity Ventures, 2020).

Com a crescente proliferação da *Internet*, tem-se observado, igualmente, um aumento significativo na prevalência de cibercrimes. O termo ‘cibercrime’ foi cunhado em 1995, por Sussman e Heuston e uma das maiores lacunas encontradas na literatura face ao estudo do mesmo é a ausência de uma definição universal. Num sentido lato, o termo “cibercrime” descreve os crimes que têm lugar no ciberespaço, um ambiente virtual dentro do qual a atividade computadorizada é realizada (Wall, 2007, p.10) e onde conhecimento especial acerca deste local é utilizado com intuito de praticar atos ilícitos e ilegais (Furnell, 2002; Wall, 2001). Thomas e Loader (2000, p.3) oferecem a definição mais funcional: os cibercrimes são “atividades mediadas por computador, que são ilegais ou consideradas ilícitas por determinadas partes, e que podem ser conduzidas através de redes eletrónicas globais”. São, assim, um conjunto de atos ou condutas, baseados em ofensas e *modus operandi* que afetam dados ou sistemas informáticos.

A par disto, é importante também fazer uma distinção entre crimes *cyber-dependent* e crimes *cyber-enabled*. Os primeiros podem apenas ser cometidos através da tecnologia, como, por exemplo, o *hacking*, objeto central deste estudo. Já os últimos, podem ser conduzidos tanto ‘*online*’ como ‘*offline*’, ou seja, com ou sem uso de tecnologias de informação e comunicação, mas através do uso destas aumentam de escala e alcance (McGuire & Dowling, 2013). Como exemplos destes temos 1) o *stalking* que, ao ser conduzido no ciberespaço, ganha a designação de *cyberstalking* e 2) as fraudes, que quando realizadas no ciberespaço, geralmente são chamadas de fraudes online (*e.g.*, phishing). Uma outra classificação de ofensas cibernéticas recorrente é a de Wall (2007), que as categoriza em três tipos distintos, a saber: 1) *computer-assisted offenses*, sendo estas ofensas tradicionais ampliadas ou facilitadas pelo uso da tecnologia, tendo como exemplos a fraude online e o roubo de identidade; 2) *computer content crimes*, crimes que envolvem conteúdo armazenado ou distribuído por meios digitais, como é o caso de crimes como disseminação de material ilegal (*e.g.*, pornografia infantil); e 3) *computer integrity crimes*, consistindo em crimes que atentam contra a integridade, confidencialidade ou disponibilidade de redes ou sistemas eletrónicos, em que se insere o *hacking*.

A vasta maioria da investigação feita no âmbito da cibersegurança tem-se focado nos aspetos tecnológicos, colocando uma menor ênfase nos fatores humanos. Concretamente, no âmbito do *hacking*, a condução de estudos que recorreram diretamente

a populações de *hackers* revela-se escassa e é dificultada pela baixa colaboração destes e pelo seu carácter oculto e de difícil acesso, que facilmente ultrapassa jurisdições tradicionais e fronteiras físicas nas suas atividades (Rogers, 2010). De seguida apresento em profundidade o fenómeno do *hacking*, sob diversas perspetivas, com o objetivo de apresentar uma visão holística deste tema complexo.

2. O *Hacking* e os *Hackers*: Concetualização

Os termos “*hack*”, “*hacking*” e “*hacker*” detiveram vários significados ao longo das últimas décadas (Oliver & Randolph, 2020). As investigações sugerem que os *hackers* variam na sua identidade, práticas e motivações. Assim, as definições, tanto do que constitui “*hacking*”, como um “*hacker*” variam consoante a história de origem (Beltrán, 2022). Por conseguinte, para atingir uma melhor compreensão acerca dos *hackers* é crucial examinar a forma como evoluíram a par da tecnologia e da história moderna, acompanhando esta evolução até onde se situam hoje (Holt, 2020).

2.1. A evolução do *hacking* por décadas

Levy (2010) atribui a origem dos termos à década de 1950, a um clube de modelos de caminhos-de-ferro, o TMRC, do Massachusetts Institute of Technology (MIT), composto por estudantes cujo interesse se dirigia aos sistemas eletrónicos dos modelos ferroviários (Steinmetz, 2016). Estes utilizariam o termo de *hacking* para se referirem aos atos que praticavam nas suas explorações (Holt, 2020). Neste contexto, o termo ‘*hack*’ foi cunhado para descrever um projeto reconhecido pela sua “*inovação, estilo e virtuosismo técnico*” (Levy, 2010, p. 34) e os seus criadores foram apelidados de “*hackers*”. Estes começaram a ser atraídos para sistemas tecnológicos mais complexos e disponíveis na altura, os computadores (Beltrán, 2022; Steinmetz, 2016), sendo considerados os pioneiros da moderna informática clandestina, responsáveis por desafiar os paradigmas tradicionais da informática (Thomas, 2002). Esta primeira geração de programadores era apaixonada pela conceção de computadores e sistemas informáticos que fossem úteis e acessíveis a larga escala (Levy, 2010; Turgeman-Goldschmidt, 2005). Deparavam-se, nesta altura, com sistemas que ocupavam uma sala, como um “gigante gigantesco”, com uma capacidade de processamento e memória limitadas e sem qualquer rede conectora entre estes (Levy, 2010, p.25). Desta forma, procuravam a criação e operacionalização de *hacks* (que mantêm a originalidade e sentido do termo) para os problemas encontrados (Franklin *et al.*, 2019; Ward, 2011) e para a melhoria da eficiência, capacidade e desempenho destes sistemas computacionais (Brooks, 2022). Com este fim, procuravam explorar detalhes em sistemas informáticos e testar as suas capacidades, por oposição à

maioria dos utilizadores da altura, que se limitava a aprender o mínimo necessário para fazer uso dos mesmos (Szpor & Gryszczyńska, 2022). Esta primeira conceção pinta os *hackers* com uma conotação positiva e um desejo de melhorar os sistemas, ao invés de causar danos (Oliver & Randolph, 2020; Franklin *et al.*, 2019). A par disto, começara a formar-se um conjunto de ideais, conhecido como a ética dos *hackers* (Levy, 2010). Os indivíduos que se regiam por estas premissas denominavam-se como “verdadeiros *hackers*”, mostrando-se fiéis às intenções primordiais do *hacking* (Jaquet-Chiffelle & Loi, 2020). Estes princípios incluíam: a crença de que toda a informação deve ser livre; a desconfiança em relação à autoridade; a ideia de que os *hackers* devem ser julgados pelas suas capacidades técnicas e não por fatores como idade, etnia ou estatuto; e a descentralização do acesso aos computadores e à informação e conhecimento produzidos por estes. Ainda, a ética *hacker* reconhece que os computadores podem ser usados para criar arte e beleza e que, aderindo a estes pressupostos, a evolução da tecnologia teria o potencial de melhorar a vida das pessoas em vários domínios (Levy, 1984).

Na década de 60, a tecnologia passa por significativas melhorias e começa a ganhar destaque na indústria pública e privada, tornando-se o *hacking* cada vez mais comum (Holt, 2020). Para tal, muito contribuíram duas evoluções tecnológicas decorridas neste período: a conexão dos sistemas informáticos universitários e militares, que colmata na criação da *Internet*, passando a permitir a partilha de informação a larga escala; e a diminuição das dimensões e preço dos computadores, facilitando a sua aquisição e posse por parte da população geral (Holt, 2020; Taylor, 1999; Levy, 1984). Desencadeado por estes desenvolvimentos, na década de 70 assiste-se a um ponto de viragem fundamental na evolução do *hacking*, com a emergência do *hacking* criminoso. Surge, aqui, uma conotação negativa atribuída ao *hacking*, devido à mudança de interesses e intenções dos indivíduos que o perpetraram (Holt, 2020; Jaquet-Chiffelle & Loi, 2020; Steinmetz, 2016; Yar, 2006), que passam a priorizar o ganho pessoal ao invés da resolução de problemas (Oliver & Randolph, 2020).

A década de 80 veio solidificar esta noção do *hacker* como um criminoso (Brooks, 2022), registando-se uma escalada de comportamentos criminosos entre estes (Oliver & Randolph, 2020). Com o foco da população e meios de comunicação social nos *hacks* maliciosos, geraram-se debates em torno do direito à privacidade (Levy, 1984; Yar, 2006) e da necessidade de formação de leis abrangentes do acesso não autorizado a sistemas informáticos, procurando regular estas novas interações (Hollinger & Lanza-Kaduce, 1988; Holt, 2020). Esta tensão entre a restante população e os *hackers* culminou numa

obra materializada em 1986 na revista periódica “Phrack”, denominada por “The Conscience of a Hacker” ou, como é mais comumente conhecida, “The Hacker Manifesto”. A obra, de autoria de um reconhecido *hacker*, defende o interesse central dos *hackers*, observado nos primórdios do *hacking* - adquirir conhecimento -, ainda que por vezes esta procura possa conduzir à quebra de leis (Holt, 2020). O “Manifesto Hacker” procurava desafiar a visão de *hackers* como criminosos, apresentando-os como exploradores curiosos. Contudo, não só instigou uma rutura entre a comunidade *hacker* e a restante sociedade (Furnell *et al.*, 1999; Thomas, 2002), como causou divergência na própria comunidade *hacker*, ao conceder o uso de *hacks* maliciosos ainda que exploratórios, premissa com que muitos hackers originais não concordavam (Holt, 2020). Nesta altura começa a emergir também a indústria da segurança informática, incorporando muitos dos *hackers* ativos nos anos 80 em posições legítimas, procurando aplicar os seus conhecimentos para fins de proteção (Taylor, 1999).

Com o início do novo milénio, a inovação tecnológica tinha já causado transformações significativas no mundo. O crescimento do comércio eletrónico e dos prestadores de serviços financeiros passou a possibilitar a compra e transação de bens, a qualquer altura, criando oportunidades económicas para os *hackers*, que começam a visar instituições financeiras para obtenção de informações sensíveis e realização de transações fraudulentas (Wall, 2007; Holt, 2020). Assiste-se, ainda, a uma evolução dos meios utilizados no *hacking*, incorporando diversas técnicas (*e.g.*, vírus) e venda destas como ferramentas a agentes menos qualificados que os possam usar (Holt, 2020).

2.2. Concetualização atual

Vários investigadores têm tentado definir o termo “*hacker*”, mas, de um modo geral, estas tentativas têm sido inconsistentes. O termo “*hacker*” foi inicialmente utilizado na década de 1960 para descrever programadores inovadores que procuravam explorar os limites tecnológicos (Young *et al.*, 2007), contudo, desde esta ‘golden age’ do *hacking*, as perceções têm vindo a alterar-se (Steinmetz, 2016) e, desde então, as atividades praticadas por *hackers* sofreram uma grande expansão (Oliver & Randolph, 2020). Face a isto, a definição é muitas vezes pouco clara, gerando confusão sobre quem se qualifica, ou não, como *hacker*. Isto complexifica-se, ademais, pela existência de diferentes tipos de *hackers*, com características diversas. Assim, ao longo das últimas décadas várias definições têm surgido, optando por colocar ênfase em diferentes elementos. Alguns autores (*e.g.*, Madarie, 2017; Oloyede *et al.*, 2023; Taylor, 1999), partem da definição original de *hack*, definindo *hackers* como indivíduos que fazem uso da tecnologia de

forma inovadora, para objetivos distintos dos inicialmente pensados. Por vezes, optam também por abordagens mais técnicas (e.g., Oloyede *et al.*, 2023; Bachmann, 2010), realçando a configuração de *hardware* e *software*. Apesar de abrangentes, são definições focadas no aspeto técnico e, para efeitos desta tese, melhor se enquadraria uma definição que confrontasse o aspeto criminológico e comportamental. Outros autores (e.g., Holt & Leukfeldt, 2020; Marcum *et al.*, 2014) têm utilizado definições semelhantes entre si que refletem o possível carácter criminoso do *hacking*. Face à evolução do fenómeno e atenção que tem recebido pela população geral e *media*, estas definições têm tido um rápido alastramento pela literatura, definindo um *hacker* como um indivíduo que utiliza os seus conhecimentos de tecnologia para obter acesso não autorizado a sistemas informáticos.

Embora estas definições descrevam um tipo de *hacker*, não são exaustivas. A literatura referente ao *hacking* tende a assumir um carácter binário, optando por enaltecer ou denegrir os *hackers* (Coleman & Golub, 2008). Uma definição abrangente deve, assim, reconhecer as características positivas e negativas dos *hackers* sem favorecer um ponto de vista específico, sem ser tendenciosa (Oliver & Randolph, 2020).

O *hacker*, ético ou não, procede da seguinte forma: em primeiro lugar, deteta uma vulnerabilidade; de seguida, desenvolve ou procura uma ferramenta que lhe permita explorar essa vulnerabilidade encontrada; por fim, ganha um acesso mais profundo ao sistema no qual detetou a vulnerabilidade (Furnell, 2002). Após essas etapas, o *hacker* malicioso, ao ter controlo do sistema, poderá praticar atividades como, por exemplo: roubo de recursos computacionais, roubo de propriedade ou informação confidencial, sabotagem/alteração/destruição do sistema, desfiguração de *sites* (Yar, 2006). Para tal, utilizam estratégias e instrumentos como *malware*, sabotagem informática, vírus, *DOS*, entre outros (Furnell, 2002). Apesar de serem estes os comportamentos associados a *hackers* maliciosos, verifica-se que podem também partir dos restantes. A título de exemplo, *hackers* maliciosos (e.g., *black hats*) e *hackers* éticos (e.g., *white hats*) podem utilizar as mesmas técnicas, contudo, enquanto o *hacker* malicioso o faz com o propósito de causar dano efetivo no sistema, o *hacker* ético pode fazê-lo no âmbito, por exemplo, de testes de penetração¹ (Chowdappa *et al.*, 2014).

Tendo em conta o apresentado, por conseguinte, uma definição de *hacker* mais apropriada, para efeitos deste projeto de investigação, seria a de Holt (2007), que contempla os *hackers* como indivíduos que utilizam o seu conhecimento para aceder a

¹ Testes que procuram testar a segurança de um sistema, procurando ganhar acesso a este, de forma a perceber como o fortalecer (Chowdappa *et al.*, 2014).

sistemas informáticos com ou sem a permissão do proprietário do sistema, abrangendo assim a vertente ética e não ética.

Alguns autores optam pela criação de outras designações para *hacking* malicioso, perante a controvérsia que envolve o termo. Em resposta à constante atribuição de um significado malicioso e ilegal ao termo *hacker*, surge o *cracker*, sendo este o termo mais conhecido, de oposição ao primeiro. Os *crackers* utilizam as suas competências em matéria de segurança informática para criar *malware* (*software* malicioso) e infiltram-se ilegalmente em sistemas seguros com a intenção criminosa e de lhe causar danos (Raymond & Steele, 2001). Assim, estes diferenciaram-se dos *hackers* (indivíduos não-criminosos), que manteriam o seu significado positivo original. Esta é apenas uma das muitas distinções que começam a ser feitas dentro da comunidade. Como mencionado, para a população em geral, “*hacker*” é um termo atualmente sinónimo de cibercriminoso (Kirsch, 2014), mas nem todo o *hacking* é igual. Os propósitos, técnicas e intenções empregues diferem grandemente, entre os indivíduos desta comunidade (Kirsch, 2014). De acordo com estes, e outros, fatores, várias tipologias têm sido elencadas, no estudo deste fenómeno crescente, a analisar de seguida.

2.3. Tipologia de *hackers*

Historicamente, os *hackers* eram conhecidos como um grupo genérico. Contudo, isto é similar a agrupar todos os cibercriminosos numa categoria genérica, ignorando as suas ações e motivações (Rogers, 2006). Assim, para perceber os problemas criados pelos *hackers*, é necessário começar a entender os indivíduos por detrás dos ataques (Skinner & Fream, 1997) e, desta forma, alguns autores (*e.g.*, Moore, 2015; Seebruck, 2015), têm tentado criar uma taxonomia de *hackers* através de divisões com base em critérios como ética (*e.g.*, Taylor, 1999), motivações (*e.g.*, Seebruck, 2015; Rogers, 2006), forma de entrada no sistema (*e.g.*, Moore, 2015), nível de competência (*e.g.*, Rogers, 1999), entre outros. Esta procura por uma categorização consensual inicia-se nos anos 80. A primeira tipologia a ganhar celeridade entre a comunidade científica foi a de Landreth & Reingold (1985), que propõem 5 diferentes tipos de *hackers*, distintos a nível de competência e motivações (desafio intelectual, procura de sensação, ego, lucro e *mischief*). Em ordem de competência, primeiro, surge o *Novice*, que teria como principal motivação a diversão, sendo jovens iniciantes no *hacking*. o *Student* designa um jovem aborrecido, com desejo de algo novo para aprender. Já o *Tourist* procura um desafio, sendo o *hacking*, para si um jogo mental em que a recompensa é a emoção da vitória. O *Crasher* é um tipo de *hacker* destrutivo, cujo objetivo é tornar-se visível. Este tipo de *hacker* é pouco conceituado no

que toca à visão dos outros *hackers*, pois contribui para a reputação negativa dos *hackers* e procuram causar destruição até em sistemas que os restantes membros da comunidade utilizam para comunicar. Por fim, o *Thief*, de acordo com Landreth e Reingold (1985, p.68), “não é um *hacker*, de todo: é um criminoso”. Este é geralmente funcionário numa empresa que se tornará na sua vítima, empregando técnicas de espionagem.

Após a tipologia estabelecida por Landreth e Reingold em 1985, surgiram duas adicionais, propostas por Hollinger, em 1988 e Chantler, em 1996 (*cit in* Rogers, 1999). A classificação de Hollinger (1988) centrava-se nas competências tecnológicas, categorizando os *hackers* em três níveis de proficiência crescente: piratas, navegadores e *crackers*. Em 2001, o termo de *cracker* volta a ressurgir, com o propósito de afastar a conotação negativa dos *hackers* e, ao invés, redirecionando-a para o termo *cracker*, que passa a designar um *hacker* criminoso (Raymond & Steele, 2001). Em contrapartida, a abordagem de Chantler constitui a sua tipologia com base em quatro critérios distintos: atividades, competência técnica, motivações e duração de envolvimento. Chantler identificou três categorias: *elite group*, consistindo em indivíduos com um elevado nível de conhecimento, motivados principalmente pelo sucesso, autodescoberta e desafio intelectual; *neophytes*, possuíam conhecimentos intermédios, frequentemente seguidores do grupo de elite; *losers and lamers*, caracterizados por um baixo nível de conhecimento e motivações centradas no lucro, vingança, roubo e espionagem (Chantler, 1996, citado em Rogers, 1999).

Das tipologias mais comumente abordadas atualmente, destaca-se a de Rogers. Esta teve várias evoluções, sendo primeiramente exposta em 1999 e sofrendo posteriores alterações em 2006 e, novamente, em 2010. Na sua tipologia de 2006², o autor parte de conceções prévias (Rogers, 1999; Furnell, 2002; e Gordon, 2001) e produz uma tipologia que abarca nove classificações distintas: *Novice*, *Cyber-punks*, *Internals*, *Petty Thieves*, *Virus Writers*, *Professional Criminals*, *old guard hackers*, *Information Warriors* e *political activists*. Esta tipologia conjuga dois aspetos centrais: por um lado, o nível de competência técnica, com o grupo *Novice* a ocupar o último lugar e o grupo *Information Warriors* o primeiro; por outro, o aspeto motivacional. As motivações que tem em conta são quatro: 1) curiosidade, referente ao desejo de conhecimento, procura de sensações e desafio intelectual; 2) notoriedade, alcançada através da atenção por parte dos media,

² Esta é a versão da tipologia de Rogers mais relevante para a presente dissertação, devido a um dos objetos de estudo ser a questão motivacional do *hacking*.

fama, estatuto e prestígio; 3) vingança, contra instituições, indivíduos ou nações; e 4) financeira, caracterizada pelo ganho monetário. Assim, a tipologia a que chega é a seguinte: 1) *Novice*, indivíduos que iniciaram a sua atividade de *hacking* recentemente, sendo motivados por procura de sensações e notoriedade; 2) *Old Guard*, não possuem intenção negativa, mas sim um desrespeito para com a propriedade pessoal, sendo motivados por crescimento intelectual e curiosidade; 3) *Internals*, consistem em (ex)empregados, em empregos relacionados com a tecnologia, possibilitando-lhes oportunidade para realizar os seus ataques, são motivados por vingança, agindo contra o sistema da própria instituição; 4) *cyber-punks*, que detêm a motivação de notoriedade, partindo do desejo de atenção dos *media*, mas também financeira 5) *Professional Criminals*, *hackers* treinados e contratados para efeitos criminosos, motivados financeiramente; 6) *Petty Thieves*, sendo Rogers (2006) influenciado pela categoria “*Thief*” de Landreth (1985), movida pelo aspeto financeiro, ganância e, alguns casos, vingança; 7) *Virus Writers*, codificadores, com capacidade de utilizar *malware* avançado, motivados por prestígio; 8) os *Information Warriors* são financiados para participar em ciberataques desenhados para destabilizar a integridade de dados ou sistemas, frequentemente assentes em motivações políticas ou patriotas. 9) *Political Activists*, semelhantes à categoria anterior, são indivíduos cujo comportamento é justificado moralmente, designadamente por assuntos políticos (Rogers, 2006).³

Seebruck (2015), resumindo as discussões recentes e estudos de caso sobre *hackers*, procura dar uma visão unificada sobre estas. Influenciado pelas tipologias suprarreferidas, que começam a colocar uma ênfase no aspeto motivacional, parte da premissa de que os *hackers* são afetados por múltiplas motivações e organiza a sua tipologia em forma do que designa de “*arc circumplex model*”, de modo a capturar motivações e as suas intensidades, procurando captar motivações desde primárias a quinárias, se aplicável. Desta forma, em contraste com as tipologias previamente apresentadas, a de Seebruck (2015) propõe-se a representar a natureza multidimensional das motivações dos *hackers* sendo, assim, mais atual. O estudo de Seebruck (2015) parte do seu interesse em estudar a ideologia como motivação para o *hacking*, algo que escasseava nos estudos prévios a este, para discórdia deste e outros autores (e.g., Rogers,

³ Em 2010 o autor volta a atualizar a sua tipologia uma última vez, passando agora a ser composta por 7 categorias: *Script Kiddies* (que vem substituir a categoria *Novice*), *Cyber-punks*, *Professionals*, *Virus Writers*, *Thieves*, *Cyberterrorists*, categoria recuperada de 1999, e *Hactivists*. O autor optou por descartar as categorias *Internals* e *Old Guard*.

2006). Parte das quatro motivações que Rogers (2006) elenca (financeira, notoriedade, curiosidade e vingança), utilizando-as como base do modelo que constrói e ao qual acrescenta a ideologia, que abarcaria os ativistas políticos e nacionalistas. As restantes, re-nomeia de: lucro, referente a ganhos materiais; prestígio, que surge associado a ganhos não materiais, como notoriedade; lazer, referente à prática de *hacking* por prazer, tal como curiosidade intelectual, procura de sensação ou brincadeiras; e, por fim, vingança, que inclui vingança pessoal, como no caso de *insiders*, trabalhadores que se revoltam e atacam os sistemas informáticos do seu local de trabalho, ou uma vingança motivada por causas de justiça social. Assim, partindo destas, chega a uma tipologia de 8 categorias: *novices*, motivados por curiosidade; *crowdsourcers*, estimulam esforços coletivos na procura de vingança; também motivados por vingança, surgem os *punks* e os *insiders*, podendo os últimos ter também como motivador o lucro; igualmente, os *criminals* são motivados por lucro, bem como os *cyber warriors*, cujas atividades também podem ser baseadas na ideologia; finalmente, os *hacktivists* são motivados por ideologia.

Rogers (1999) defende que as descobertas feitas para uma categoria de *hackers* não podem ser generalizadas a nenhuma das outras categorias. Partindo desta premissa, que expõe incontestavelmente a existência de distintos tipos de *hackers* e necessidade de os compreender na sua individualidade, surge este estudo que procura, precisamente, compreender as diferenças individuais à luz de uma tipologia a ser explorada, de seguida, em maior detalhe.

2.3.1. Black Hats, Grey Hats e White Hats

A taxonomia mais utilizada atualmente é a de Moore (2015), que distingue entre seis tipos de *hackers*, de acordo com a forma de ataque nos sistemas. O autor defende, tal como os seus predecessores (Landreth e Rheingold, 1985; Rogers, 2006, 2010; Seebruck, 2015), as categorias de *Script Kiddies*, *Hacktivists* e *Cyberterrorists*. Contudo, acrescenta a estes três outros tipos, os *hackers black hat*, *white hat* e *grey hat*, que têm ganho popularidade entre as comunidades de *hackers*, académicas e com os *media* (Gaia *et al.*, 2021). Para os propósitos deste estudo, é sobre estes últimos que se irá incidir a atenção nas próximas linhas.

Os *black hat hackers* são, fundamentalmente, o “epítome de tudo o que o público teme num cibercriminoso” (Moore, 2015, p. 37). São indivíduos que escrevem programas para danificar os sistemas e redes informáticas, violando assim a segurança informática, por malícia ou ganhos pessoais (*idem*). Estudos recentes (*e.g.*, Chang & Whitehead, 2022; Holt & Kilger, 2008; Kirsch, 2014; Jaquet-Chiffelle & Loi, 2020; Holt, 2010; Zhang *et*

al., 2011; Bachmann, 2008; Hutchinson, 2001; Naicker & van Niekerk, 2021; Gaia *et al.*, 2021), que fazem uso da taxonomia de Moore (2015), revelam-se concordantes quanto à participação deste tipo de *hackers* em comportamentos ilegais, nas suas atividades, para propósitos ilegais, bem como à atribuição de razões maliciosas, produção de dano ou ganhos pessoais (Mubeen *et al.*, 2022; Goerzen & Matthews, 2019; Franklin *et al.*, 2019).

Moore (2015) defende que a atividade deste tipo de *hackers* vai levar à necessidade de desenvolvimento de maior segurança informática e fabrico de antivírus, bem como à constituição de carreiras para este efeito, à medida que indivíduos são pagos para desenvolver redes e sistemas com uma melhor proteção, sendo neste âmbito que surgem os *hackers white hat*. Estes são o oposto dos anteriores, tendo como objetivo fornecer programas que protejam os sistemas de serem ilegal e maliciosamente penetrados (Moore, 2015). Neste sentido, estes *hackers* são muitas vezes contratados por empresas, numa tentativa de evitar ataques por *hackers* maliciosos, ou contra-atacá-los (Barber, 2001; Abeoussi, 2019; Goerzen & Matthews, 2019). Por vezes, comportam-se como os restantes tipos de *hackers*, procurando o acesso aos sistemas (*i.e.*, *Pen Testing*), contudo, ao serem bem-sucedidos, cessam a sua atividade e alertam o proprietário para as vulnerabilidades descobertas (Moore, 2015; Gaia *et al.*, 2021), demonstrando a existência de limites legais e morais no desempenho das suas atividades. Surgem, assim, muitas vezes, como sinónimo de *hackers* éticos (*e.g.*, Abeoussi, 2019; Zhang *et al.*, 2011; Hutchinson, 2001) e *hackers* legítimos (*e.g.*, Chang & Whitehead, 2022; Mubeen *et al.*, 2022). A literatura é concordante quanto à definição de Moore (2015) e quanto à frequente empregabilidade de *hackers white hat* por agências governamentais ou empresas, para testar e/ou fortalecer as suas redes (Chang & Whitehead, 2022; Kumar, 2018; Kirsch, 2014; Bachmann, 2008). Alguma literatura (*e.g.*, Holt & Kilger, 2008; Matulessy & Humaira, 2016) defende que podem aceder de forma não autorizada aos sistemas, desde que para benefício exclusivo da indústria de segurança. No entanto, a grande maioria consente que para denominação de *hacking white hat* é necessária a existência de autorização, sendo um dos critérios principais o respeito pela lei (Barber, 2001) e a não exploração de vulnerabilidades encontradas, divulgando-as apenas ao proprietário (Holt, 2010). Assim, muitas vezes, tomam parte em atividades de teste de *software* recentemente lançado, nomeadamente em *bug bounty programs* que oferecem “*bounties*” (*e.g.*, dinheiro, reconhecimento) a quem identificar vulnerabilidades e as comunicar ao fornecedor (Votipka *et al.*, 2018).

Como visto, as definições de *white hat* e *black hat hackers* apresentadas por outros autores vão, em grande medida, de encontro às de Moore (2015). A maior divergência encontra-se ao nível da definição dos *grey hat hackers*, explorada em seguida.

A definição de *grey hat* tem sido distinta na literatura, mas o consenso é de que são uma combinação dos anteriores. De acordo com Moore (2015) estes são *hackers* oportunistas, que procuram alvos e, caso ganhem acesso a um sistema, notificarão os proprietários, propondo uma oferta de reparação através de uma quantia monetária. Outros autores (*e.g.*, Kirsch, 2014; Jaquet-Chiffelle & Loi, 2020; Matulessy & Humaira, 2016) não lhes apontam esta intenção de proveito. Focam-se, ao invés, nos propósitos não éticos, que os distinguem dos *white hat*, pois estão preparados para quebrar a lei através das suas explorações tecnológicas, com a justificação de atingir uma melhor segurança, não obstante a falta de consentimento ou autorização prévia. A ausência de ética dos *grey hat* é demonstrada pelo facto de, por vezes, exporem as falhas de forma pública, não só oferecendo soluções às empresas sobre como as retificar, mas também demonstrando a outros *hackers* como as explorar (Kirsch, 2014). Assim, são por vezes caracterizados por uma ambiguidade que pode levar a atos ilegais, mas não necessariamente com más intenções, ou propósitos de ganhos pessoais (Matulessy & Humaira, 2016).

Por outro lado, vários autores não apresentam uma definição direta de *grey hat hackers*. Ao invés, definem-nos como indivíduos que se situam num espectro de *hacking*, uma “mediana entre *black* e *white hats*” (Franklin *et al.*, 2019, p. 25), praticando comportamentos de ambos os extremos (Gaia *et al.*, 2021; Kirsch, 2014; Naicker & Niekerk, 2021; Matta *et al.*, 2020; Holt, 2010). De acordo com Franklin *et al.* (2019), o que os distingue é a prática de ambos os tipos de comportamentos: realizam *hacking* sem autorização (característico de *black hats*) mas, ao descobrirem vulnerabilidades, alertam o proprietário (característico de *white hats*). Não obstante, o facto de alertarem não significa que os seus motivos ou forma como o fazem vá de encontro aos *white hat*. O enfoque dos *grey hat* na melhoria da segurança frequentemente resulta na perceção de que os fornecedores devem ser responsabilizados caso não resolvam as vulnerabilidades dentro de um curto espaço de tempo. Desta feita, procuram aumentar a pressão para causar mudanças nos sistemas, vendo as suas ações justificadas com base na necessidade de assegurar a segurança dos mesmos (Kirsch, 2014; Goerzen & Matthews, 2019). Assim, os *grey hat* violam as expectativas de privacidade dos consumidores para proteger informações privadas da atividade informática maliciosa, mas não mais do que o necessário (Kirsch, 2014). Muitos autores defendem que o rótulo de *grey hat* é também

utilizado quando as motivações ou legalidade das ações do *hacker* não são claras, ou não podem ser facilmente categorizadas (Franklin *et al.*, 2019), ou então são potenciais de alterações (Hutchinson, 2001; Holt & Kilger, 2008). Estes podem trabalhar tanto ofensiva, como defensivamente, e tanto legítima, como ilegitimamente dependendo da situação (Kunar, 2018; Chang & Whitehead, 2022). Assim, para muitos, o *hacker grey hat* é pensado como “um *hacker* de ‘chapéu branco’ que, por vezes, usa um ‘chapéu preto’ para atingir os seus objetivos” (Red Hat, 2003, p. 7).

3. Características individuais explicativas do *hacking*

O *hacking*, pelo seu carácter potencialmente danoso e como fenómeno altamente mediatizado, tem impulsionado o estudo dos fatores que possam influenciar a sua prática. Diversas características têm sido estudadas no âmbito do *hacking* e dos indivíduos deste praticantes, quer a nível individual ou contextual. Na presente revisão, serão apresentados e aprofundados os fatores que incidem na vertente individual, de importância para o estudo do cometimento de *hacking*: em primeiro lugar, as características sociodemográficas, designadamente, o sexo, a idade, a ocupação, a ocupação parental e a escolaridade; em segundo lugar, as motivações associadas à prática de *hacking* e a diferentes tipos de *hacking*; finalmente, o fenómeno será analisado à luz de algumas teorias da psicologia e criminologia tradicional, que a literatura tem vindo a aplicar ao cibercrime e, mais concretamente, ao *hacking*, designadamente a Teoria Geral do Crime (Gottfredson & Hirschi, 1990), o Modelo dos Cinco Fatores (Costa & McCrae, 1992) e o Modelo da *Dark Triad* (Paulhus & Williams, 2002). Esta tese será uma assimilação de todas estas vertentes individuais de análise do *hacking*, procurando-se a obtenção de resultados mais integrados e abrangentes, à luz dos diferentes pressupostos teóricos.

3.1. Características sociodemográficas

A investigação científica tem procurado explorar o perfil do *hacker* com o principal objetivo de aprofundar as características sociodemográficas do mesmo. Esta procura de um perfil tem sido dificultada pelo anonimato destes indivíduos e, igualmente, pela sua relutância em fazer parte de estudos (Marcum *et al.*, 2014). Não obstante, a literatura tem apontado algumas características que aparecem frequentemente associadas a estes indivíduos (Holt, 2020) e que podem servir como um bom ponto de partida para estabelecer um perfil comum.

Uma das características que aparece com maior consistência na literatura, relacionada com o *hacking*, é o sexo. As investigações mais atuais (*e.g.*, Fox & Holt, 2021; Marcum *et al.*, 2014), indicam um ‘gender gap’ observável a nível do *hacking*, em

que os *hackers* são geralmente indivíduos do sexo masculino, o que, de acordo com Taylor (1999) e Steinmetz (2016), tem como possível justificação a socialização do sexo masculino para a tecnologia desde cedo na adolescência. Fox e Holt (2021) realizaram um estudo quantitativo com dados recolhidos no *Second International Self-Report of Delinquency Study* (ISRD-2), sendo este um estudo internacional a uma escala global, que envolveu 66,820 jovens, do 7º ao 9º ano, em 31 países, recrutados através de uma amostragem probabilística. Tinham como objetivo avaliar se fatores de risco criminológicos podiam ser utilizados para distinguir jovens *hackers* de não-*hackers*. Verificam que da sua amostra de 5081 *hackers* juvenis, 75% (n= 3780) eram do sexo masculino, achado que tem sido recorrente em vários estudos (e.g., Bossler & Burruss, 2011; Holt *et al.*, 2010; Marcum *et al.*, 2014; Skinner & Fream, 1997). Quanto à idade, verifica-se que tendem a ser um grupo diverso, com idades que se situam, prevalentemente, entre os 20 e os 30 anos, mas que podem ir desde a adolescência até aos 60 anos (Schell & Holt, 2010; Steinmetz, 2016). Muitos indivíduos a perpetrar *hacking* aparentam ser jovens, parecendo ir de encontro às evidências da curva idade-crime⁴ (Bachmann, 2010; Jordan & Taylor, 1998). O estudo de Goode & Cruise (2006), no qual os autores aplicaram questionários em fóruns de *crackers* (*hackers* que podem ser equiparados a *black hat*), contou com 24 respondentes no total, dos quais 18 relataram a sua idade, sendo que a maioria (n=13) afirmaram ter menos do que 25 anos.

É também relevante abordar a ocupação dos *hackers*, que tem sido abordada na literatura mais recente. Steinmetz (2016) procurou analisar várias características demográficas e de *background* de *hackers*, através de um estudo etnográfico, realizado por observações e entrevistas semi-estruturadas a 14 *hackers*. A sua amostra foi recolhida de locais frequentados por estes indivíduos (i.e., restaurantes, bares), bem como na DEF CON 21, uma convenção anual de *hackers*, que decorre em Las Vegas. No que toca à sua ocupação, constatou que os *hackers*, quando empregados, tendem a sê-lo numa profissão relacionada com a tecnologia. Isto foi corroborado pelos dados da HackerOne (2020), um relatório relativo aos participantes da conferência HackerOne, que verificaram que 54% dos *hackers* exerciam a sua atividade profissionalmente. Já o estudo de Goode & Cruise (2006), apresenta resultados divergentes, sendo que dos 20 indivíduos que responderam, apenas 6 relataram estar empregados no setor tecnológico. Não só a própria profissão,

⁴ Conceção criminológica que denota a variação da criminalidade em relação à idade dos indivíduos. Observa-se o crescimento da criminalidade nos anos da adolescência, atingindo o pico no início da idade adulta e decrescendo posteriormente (Loeber & Farrington, 2014).

mas também a dos seus pais se revela significativa, uma vez que 12 dos 14 entrevistados por Steinmetz (2016) possuía pelo menos um pai empregado no setor da tecnologia, demonstrando uma relação entre os interesses do indivíduo e a ocupação parental.

Um outro fator prende-se com o grau de escolaridade, sendo que o conhecimento técnico e competências possuídas pelos *hackers* podem levar a pensar que se tratam de indivíduos com elevados graus de escolaridade. A evidência empírica é divergente. Alguns estudos vão de encontro ao esperado, designadamente, o estudo de Steinmetz (2016) revela que os *hackers* têm uma tendência para uma instrução de nível mais elevado, sendo que todos os entrevistados tinham alguma forma de educação superior. Também consistente com estes resultados, Goode e Cruise (2006) demonstram que a maioria da sua amostra (n=13) reportaram experiência no ensino superior, sendo que 5 completaram a licenciatura e 4 o mestrado. Outros estudos, contudo, vão em sentido contrário, demonstrando uma maioria de educações de grau secundário, com menor incidência de graus universitários (Bachmann, 2010; Holt *et al.* 2009; Woo, 2003).

A nível sociodemográfico, denota-se a falta de estudos que averiguem diferenças entre *hackers black hat*, *grey hat* e *white hat*. Não obstante, Pinto (2023) realizou um estudo no qual comparou algumas das características previamente elencadas, entre um grupo de *hackers* maliciosos e um grupo constituído (mas não só) por *hackers* não-maliciosos. O seu estudo contou com uma amostra de 680 estudantes portugueses que completaram um inquérito online. Ora, tomando os *hackers* maliciosos como *hackers black hat* (pela definição de Moore (2015) e variados autores anteriormente expostos) e o grupo que integra os *hackers* não maliciosos como os restantes tipos (*hackers white hat* e *grey hat*, também de acordo com as definições previamente utilizadas), será possível fazer algumas inferências. No estudo de Pinto (2023), concluiu-se que *hackers* maliciosos são mais novos, com maior afluência de sexo masculino, não empregados, com um grau inferior a licenciatura e pertencentes às áreas TIC. Assim, pode esperar-se o mesmo dos *black hat*, quando comparados com as restantes categorias tratadas. Indo de encontro a estes resultados, alguma investigação demonstra que a atividade maliciosa provém, maioritariamente, por parte de jovens (menores de 30 anos), havendo uma proporção de *hackers* mais velhos, que parecem estar empregados na comunidade de segurança informática (Holt, 2010; Gilboa, 1996; Jordan & Taylor, 1998; Taylor, 1999), parecendo ir no sentido de que *hackers white hat* seriam mais velhos.

Uma grande parte desta multitudine de características parte de uma conceção baseada em estereótipos, propagados pelos *media* e população geral, acerca dos *hackers*. Contudo,

a evidência empírica, produzida não só a nível quantitativo, mas destacando sobretudo os métodos qualitativos neste âmbito, tem contribuído para a evolução deste pensamento. Ambiciona-se, assim, um perfil consistente do *hacker*, abrindo os olhos a novos fatores e ao seu papel de relevo na prática de *hacking* (Steinmetz, 2016; Back *et al.*, 2018).

3.2. Motivações

Fitch (2004) afirma que a designação de ‘*hacker*’ advém da participação em atividades ilegais no ciberespaço, muitas vezes sem consideração pelas suas motivações e objetivos. Aquando dos primórdios das suas atividades, até ao início dos anos 2000, os *hackers* eram, primariamente, motivados por curiosidade, desejo de reconhecimento ou de promoção de causas sociais ou políticas (Milone, 2003). Mais recentemente, estes motivos têm vindo a ser substituídos, devido a um crescimento do cibercrime motivado financeiramente (Oliver & Randolph, 2020; Jaquet-Chiffelle & Loi, 2020).

A classificação de Seebruck (2015), previamente explanada, é uma das mais notórias, agrupando os *hackers* de acordo com a sua motivação, concluindo que a prática de *hacking* se deve a cinco motivações principais: ideologia, lazer, prestígio, lucro e vingança. Várias outras investigações têm sido conduzidas, tanto a nível quantitativo (*e.g.*, Madarie, 2017; Rogers, 2006), como a nível qualitativo (*e.g.*, Taylor, 1999) e os seus resultados retratam a prevalência destas mesmas motivações, complementando com outras que surgem também frequentemente associadas aos *hackers*.

Madarie (2017), realizou um estudo inovador no qual procurou quantificar as motivações dos *hackers*, analisando as relações entre a frequência de vários comportamentos de *hacking* e as motivações para cometimento destes, numa amostra de *hackers* masculinos e potenciais *hackers*. Para tal, aplicou um questionário a 127 indivíduos, em que 51% afirmaram ser motivados, principalmente, por diversão, um resultado que vai de encontro ao relatório da HackerOne (2020), que demonstra uma prevalência de 49% para a mesma motivação e por procura de sensação, motivação que tem também sido referida por vários autores (*e.g.*, Rogers, 2006; Gaia *et al.*, 2021). 30% revelou ser motivada por motivos sociais e morais (Madarie, 2017). Já no que toca ao lucro, obtido muitas vezes através de estratégias como *ransomware* e e-mails de *phishing* (Back *et al.*, 2018), a literatura apresenta-se divergente, sendo esta uma motivação com importância muito variada, desde 18% (Madarie, 2017) a 53% (HackerOne, 2020).

Para além das já elencadas, alguns estudos (*e.g.*, Woo, 2003) sugerem ainda que “ser desafiado” é uma forte motivação para os *hackers*, de acordo com 68% da amostra

da HackerOne (2020) e 30% da amostra de Bachmann (2010). A HackerOne (2020) avança de seguida com “aprender novas técnicas”, com uma prevalência de 51%, motivação também avançada por Turgeman-Goldschmidt (2005). Rogers (2006), acrescenta o ego, apoiado por Turgeman-Goldschmidt (2005), que refere “sentir-se mais esperto que outros”. A HackerOne (2020), elenca ainda como motivações de importância: “avançar na carreira” (44%), “proteger e defender” (29%), “fazer bem no mundo” (27%) e “ajudar outros” (25%). Por fim, Woo (2003) relata a notoriedade/reconhecimento, indo de encontro ao postulado por Seebruck (2015), como motivação principal.

3.2.1. Diferenças entre hackers *white hat*, *grey hat* e *black hat* a nível das motivações

Rogers (2006) afirma que de forma a entender as motivações dos *hackers*, o termo genérico de *hacker* necessita de ser segmentado em categorias e, de acordo com Franklin et al. (2019), é frequente a atribuição da variação entre categorias às motivações dos indivíduos que as integram. Quanto às categorias de *black hat*, *white hat* e *grey hat*, poucos autores têm tentado compreender quais as motivações que estão por detrás dos seus atos e se variam, sendo escassa a literatura neste âmbito, principalmente empírica.

Na existente, aos *black hat hackers* são frequentemente associadas motivações relacionadas com ganhos pessoais (Sanders et al., 2019), sendo uma das motivações mais apontadas a de procura de sensação, que recebem ao manipular um sistema informático. Gaia et al., (2021) realizaram um estudo quantitativo, através da aplicação de questionários a uma amostra de 474 alunos universitários de gestão e de informática nos Estados Unidos da América, com o objetivo de estabelecer diferenças entre os indivíduos que levam ao interesse em *hacking white hat*, *grey hat* e *black hat*, tendo concluído uma forte associação entre a procura de sensação e o *hacking black hat* ($r=.143$), achado também suportado por Bachman (2010). Gaia et al., (2021) acrescentam ainda que possíveis motivações para este tipo de *hacker* poderiam ser vingança, algo também defendido por Lu e Yau (2022) e notoriedade, contudo, não testam empiricamente estas hipóteses. Contrariamente, Goode e Cruise (2006) conduziram um estudo em que examinaram as motivações de 28 *crackers*, através de um inquérito *online*. Os resultados demonstraram que os *crackers* eram maioritariamente motivados por estimulação. 'Desafio pessoal' foi uma das motivações mais usuais, ao passo que reconhecimento e dinheiro, não foram considerados motivadores importantes (Goode & Cruise, 2006). Este último resultado, demonstra-se contrário a vários estudos não empíricos (Jaquet-Chiffelle

& Loi, 2020; Meyers *et al.*, 2009; Franklin *et al.*, 2019), que afirmam que também o lucro seria uma importante motivação de *hacking black hat*, sendo que, por vezes, vendem os seus serviços ou são contratados para tal.

Seebruck (2015) associa o prestígio como motivação principal para *hackers* não maliciosos, destacando os *white hat*. Aos *white hat*, Meyers (2009) e Franklin *et al.* (2019) associam ainda o desafio intelectual de desenvolver serviços que protejam os sistemas de intrusões. Gaia *et al.*, (2021) demonstraram que, na sua amostra, também para os *white hat* a procura de sensação tinha algum peso como motivação, apesar de menor ($r = .129$), em comparação com os *black hat*.

Já para os *grey hat*, a ideologia surge como principal motivação, sendo estes frequentemente referidos como *hacktivists*, defensores de uma causa e exercendo frequentemente ações contra posições (sociais e políticas) contrárias às suas (Gaia *et al.*, 2021). De acordo com Moore (2015) a motivação principal dos *grey hat* seria o lucro, uma vez que tentam entrar no sistema para depois propor um preço para resolver as falhas encontradas. Por fim Goerzen e Matthews (2019) referem que os *grey hat* seriam motivados por um sentido de interesse público, relacionado com a melhoria dos sistemas informáticos e a advocação por direitos humanos e segurança. Vários autores apontam uma dificuldade em classificar as motivações dos *grey hat*, já que, tal como muitas definições do termo apontam, geralmente são indivíduos que se situam entre *black* e *white hat* e, assim, os seus motivos podem ser difíceis de categorizar (Hutchinson, 2001) ou até passíveis de mudança (Franklin *et al.*, 2019).

3.3. Baixo Autocontrolo

No estudo da perpetração de *hacking*, o autocontrolo é um dos traços individuais mais testados empiricamente, no sentido de se perceber se um menor autocontrolo potencia a perpetração de *hacking*.

Em 1990, Gottfredson e Hirschi avançam com a Teoria Geral do Crime, que toma o autocontrolo como premissa central na explicação do comportamento desviante e criminal. Quanto ao conceito de autocontrolo, os autores caracterizam-no como: 1) preferência por gratificação imediata; 2) preferência por tarefas de execução fácil; 3) preferência por atividades físicas; 4) propensão para o risco; 5) autocentração; 6) baixa tolerância à frustração. De acordo com a forma como os indivíduos se colocam em cada uma destas facetas, estarão mais ou menos propensos a envolver-se no crime. Gottfredson e Hirschi (1990) concluem que “as pessoas com falta de autocontrolo tendem a ser

impulsivas, insensíveis, físicas (...), propensas ao risco, autocentradas e não verbais, e terão, portanto, a tendência a envolverem-se em atos criminais e análogos” (p.90). Assim, é teorizado que indivíduos com níveis mais reduzidos de autocontrolo terão maior propensão para cometer crime, comparativamente a indivíduos com níveis mais elevados.

Esta teoria tem demonstrado capacidade de predição, não só para o cibercrime em geral (e.g., Bossler & Holt, 2010; Holt *et al.*, 2011), mas também para o *hacking* (e.g., Bossler & Burruss, 2011; Holt *et al.*, 2011; Marcum *et al.*, 2014; Pinto, 2023). A premissa base, de que indivíduos com baixo autocontrolo percecionam o crime como atrativo pois este fornece-lhes benefícios imediatos, não considerando os impactos a longo prazo das suas ações, pode ser aplicada aos *hackers* que, pela sua impulsividade e incapacidade de pensarem a longo prazo, não assimilariam a quebra de confiança ao praticarem este comportamento, nem consideram a possibilidade de serem apanhados e de sofrerem consequências legais (Marcum *et al.*, 2014). Assim, vários autores têm demonstrado que o baixo autocontrolo está significativamente associado ao cometimento de *hacking*.

No estudo de Fox & Holt (2021), mencionado anteriormente, tendo por objetivo avaliar se fatores de risco criminológicos se aplicavam ao *hacking* e podiam ser utilizados para distinguir jovens *hackers* de não *hackers*, um dos fatores de risco analisados foi o autocontrolo, pelo que, ao comparar os níveis de autocontrolo dos jovens que praticam *hacking* com os jovens que não praticam, os primeiros revelam-se mais baixos, designadamente, concluíram que apenas 8% dos indivíduos não-*hackers* possuíam baixo autocontrolo, em comparação com 20% dos *hackers*. Ainda, jovens com baixo autocontrolo revelaram uma probabilidade mais elevada, em 43%, de cometimento de *hacking*, em comparação com jovens com elevado autocontrolo ($b = .356$).

Em congruência com este resultado, Back e colaboradores (2018) realizaram um estudo recorrendo também a dados recolhidos do ISRD-2, mas utilizando apenas parte da amostra, que passou a ser constituída por estudantes de ensino médio e secundário de oito países diferentes (Estados Unidos, Venezuela, Espanha, França, Alemanha, Polónia, Hungria e Rússia), escolhidos por estarem incluídos no top 20 de nações com prevalência de perpetradores de cibercrime. A amostra final consistiu em 18,985 jovens. Back *et al.* (2018) tinham como objetivo testar empiricamente algumas teorias criminológicas, nomeadamente a Teoria Geral do Crime, e a sua capacidade explicativa do *hacking*, cometido no ano anterior. Os resultados, tais como os achados dos estudos mencionados anteriormente, apontaram para o baixo autocontrolo como preditor do cometimento de

hacking, causando um aumento da probabilidade de cometer *hacking*, sendo que, tendo em conta a análise feita nos oito países, este aumento variava entre 37% e 86%.

Por fim, na mesma linha de investigação, Marcum e colaboradores (2014), procuram também testar esta teoria aplicada ao *hacking*, em 1617 jovens com menos de 18 anos, do 9º ao 12º ano, de quatro escolas numa zona rural em Carolina do Norte, nos Estados Unidos. O objetivo do seu estudo era chegar à prevalência de jovens de secundário que praticam *hacking*, bem como aos preditores deste comportamento. Para operacionalizarem o *hacking*, questionaram os indivíduos sobre a realização de três comportamentos no ano anterior: entrar no email de outra pessoa sem a sua permissão e enviar um email; entrar na conta de Facebook de outra pessoa sem a sua permissão e postar uma mensagem; e aceder a um site para o qual não está autorizado. Através destas estabeleceram também uma ligação entre o autocontrolo e o *hacking* juvenil, concluindo que o baixo autocontrolo é um forte preditor de comportamentos de *hacking*, designadamente: *hacking* da conta de Facebook, especificamente, o baixo autocontrolo aumenta a probabilidade (em 11%) de fazer *login* na conta de Facebook de outra pessoa sem a sua permissão e publicar uma mensagem ($b = .11$, $\text{Exp}(b) = 1.11$); e *hacking* não autorizado a *websites*, que, devido ao baixo autocontrolo, sofre um aumento de 14% na probabilidade de cometimento ($b = 0.14$, $\text{Exp}(b) = 1.14$) (Marcum *et al.*, 2014). Estudos longitudinais também têm sido realizados neste âmbito, nomeadamente na Coreia do Sul, em que Moon e colaboradores (2010) concluíram que níveis mais reduzidos de autocontrolo conduzem a uma maior probabilidade de prática de *hacking*.

Novamente, à semelhança do encontrado a nível de características sociodemográficas, não foram encontrados estudos que realizassem uma comparação a nível do autocontrolo entre *hackers black hat*, *grey hat* e *white hat*. Partindo dos pressupostos teóricos de Gottfredson & Hirschi (1990), que postulam que indivíduos com menor autocontrolo apresentarão uma maior predisposição para atos ilícitos, é esperado que isto se repercuta a nível de comparação entre os tipos de *hackers*, uma vez que os *hackers black hat* se apresentam como cibercriminosos (Moore, 2015), ao passo que os *white hat* se caracterizam por serem respeitadores da lei e os *hackers grey hat* por se situarem no espectro da legalidade entre ambos (Franklin *et al.*, 2019). Os achados de Pinto (2023) vão no sentido desta inferência, tendo realizado uma comparação entre *hackers* maliciosos e não-maliciosos, verificando que os *hackers* maliciosos revelaram um nível autocontrolo menor, em comparação com os não maliciosos.

Ressalva-se ainda para o facto de que estudos supramencionados (e.g., Marcum *et al.*, 2014, Moon *et al.*, 2010) operacionalizam o *hacking* na sua vertente de “acesso não autorizado”, ou seja, direccionam-se a comportamentos já no espectro ilegal, podendo não retratar, por completo, a população *hacker*, na sua multitude de comportamentos adotados.

3.4. Fatores da Personalidade

Não obstante os rápidos avanços na investigação do cibercrime, há ainda aspetos particulares que carecem de investigação, nomeadamente os crimes ciberdependentes e o papel dos fatores psicológicos. De uma perspetiva aplicada, tal investigação permitiria práticas mais informadas de ciberdefesa (Jones *et al.*, 2021). Segundo Loch e Conger (1996), “as características individuais afiguram-se importantes em determinar decisões informáticas éticas” (p. 82). Apesar do crescimento do fenómeno do *hacking*, e da associação de teorias da personalidade ao crime, poucas investigações empíricas têm sido realizadas para investigar a composição psicológica de cibercriminosos e indivíduos ciberdesviantes (Rogers, 1999) e, como tal, a literatura sobre as características da sua personalidade, particularmente no que toca a *hackers*, é ainda escassa.

3.4.1. Traços de Personalidade do Modelo *Big Five*

O Modelo dos Cinco Fatores, também designado por *Big Five* foi desenvolvido por Costa & McCrae (1992) e postula que a personalidade se segmenta em cinco traços: neuroticismo, extroversão, abertura à experiência, agradabilidade (também designado por amabilidade) e conscienciosidade. De forma sumária: o neuroticismo reflete diferenças individuais a nível da emocionalidade negativa, incluindo vulnerabilidade ao *stress*, ansiedade, depressão, entre outras emoções negativas (Costa & McCrae, 1992); a extroversão está associada à emocionalidade positiva e a uma abordagem energética ao mundo social, incluindo traços como atividade, sociabilidade e assertividade (Clark & Watson, 1999); a abertura à experiência é descrita como “a amplitude, profundidade, originalidade e complexidade da vida mental e experiencial de um indivíduo” (McCrae, 1996, p.323); a agradabilidade é definida por traços como altruísmo, confiança, conformidade e preocupação com outros (Costa & McCrae, 1992); por fim, a conscienciosidade materializa-se na capacidade de concentração, em manter o foco em tarefas e na orientação para objetivos (*idem*).

A literatura tem vindo a tentar estabelecer quais as dimensões da personalidade que revelam uma maior associação ao comportamento delinquente e criminoso. No que

concerne ao *hacking*, alguns autores têm tentado fazer a mesma identificação, referente aos traços presentes nos *hackers* que os distingam de não-*hackers*, sendo a pesquisa empírica ainda escassa e encontrando-se alguma inconsistência nos estudos existentes, que serão expostos de seguida.

A comunicação social tem descrito *hackers* e indivíduos ciberdesviantes como introvertidos e socialmente subdesenvolvidos, que devido à suas naturezas antissociais tendem a passar mais tempo na *internet* e a participar no uso não ético desta (Karim *et al.*, 2009; Roger *et al.* (2006a). Rogers e colaboradores (2006) realizaram um estudo exploratório, aplicando questionários de autorrelato em formato de papel e caneta a uma amostra de 381 alunos universitários num departamento de artes liberais, numa universidade do Canadá, no qual procuram explorar se indivíduos ciberdesviantes diferem de indivíduos não-ciberdesviantes, nos traços de abertura à experiência, extroversão e neuroticismo. Apesar de não analisarem, especificamente, *hackers*, mas sim indivíduos, num termo mais lato, ciberdesviantes, os comportamentos que analisam são, muitos deles, inseridos nos comportamentos que Yar (2006) aponta como típicos de *hackers*⁵. Assim, questionam os participantes quanto a: adivinhar palavras-passe, usar a palavra-passe de outro sem autorização, aceder a ficheiros de outro sem autorização, mudar ficheiros de outro sem autorização, utilizar ou escrever vírus, obter a informação de crédito de alguém sem autorização e utilizar um dispositivo para obter chamadas grátis. Os resultados revelaram não haver relação significativa entre ciberdesviância e qualquer um dos traços.

Contrariamente, Rogers *et al.* (2006a) replicaram os contornos da pesquisa supracitada, alterando a amostra, e chegaram a conclusões diferentes quanto ao traço de extroversão que, neste estudo replicativo, se revelou significativo. Neste estudo, que contou com uma amostra de 77 estudantes universitários do departamento de informação tecnológica, numa universidade ocidental americana, analisaram os mesmos comportamentos e concluíram que a ciberdesviância está negativamente correlacionada com a extroversão ($r = -0.29$, $p < 0.01$), isto é, indivíduos que cometem atos ciberdesviantes tendem a ser mais introvertidos do que indivíduos que não os cometem. Uma comparação entre os grupos revelou que o grupo cibercriminoso demonstrou níveis significativamente

⁵ Yar (2006) menciona que uma das etapas essenciais do hacking é o acesso a um sistema ou rede. Uma vez este acesso garantido, os *hackers* realizarão atividades tais como alteração e roubo de recursos computacionais, de propriedade ou informação confidencial, sabotagem/alteração/destruição do sistema, desfiguração de *websites*, DDoS, distribuição de *software* malicioso, entre outros.

inferiores na extroversão do que a seu contraparte. Por fim, realizando uma regressão logística, de forma a determinar um modelo preditivo com as variáveis utilizadas no estudo, entre elas os cinco traços de *Big Five*, os resultados indicaram que apenas a extroversão era significativa a predizer os comportamentos analisados. De acordo com os resultados, um aumento de um desvio padrão na pontuação total de extroversão diminuiria o risco de o indivíduo se envolver em comportamentos ciberdesviantes/cibercriminosos ($\text{Exp}(B)=0,87$) (Rogers, 2006a). Nenhuma explicação foi avançada para o resultado discordante do estudo realizado anteriormente. Os autores relevam para a dificuldade em extrapolar conclusões quanto ao papel da introversão/extroversão, partindo de um único estudo, não obstante ir de encontro ao esperado.

Tem-se também verificado que os *hackers* possuem maior hostilidade e propensão para exibir qualidades egoístas (Schell & Holt 2010), traduzindo-se isto em níveis mais baixos de agradabilidade. Seigfried-Spellar & Treadway (2014) realizaram um estudo quantitativo recorrendo a inquéritos *online* de autorrelato, aplicados a uma amostra por conveniência de 398 alunos universitários do sul dos Estados Unidos da América, com pelo menos 19 anos. O objetivo do estudo era determinar se existem diferenças individuais entre indivíduos que cometem diferentes formas de ciberdesviância (*i.e.*, *hacking*, escrita de vírus, cyberbullying e roubo de identidade), agrupando os indivíduos de acordo. Analisaram ainda se diferenças a nível da personalidade entre indivíduos ciberdesviantes e indivíduos não- ciberdesviantes, nomeadamente entre *hackers* ($n=170$, da amostra total) e não-*hackers*. Verificou-se que apenas a agradabilidade ($rpb=.11$, $p<.1$) revelava uma relação moderadamente significativa com o *hacking*, indicando que *hackers* possuem menores níveis de agradabilidade, isto é, são mais antagonísticos, em comparação com não-*hackers*. Perante esta relação, foi conduzida uma ANOVA, que sugeriu a existência de diferenças significativas entre grupos para os autorrelatos de *hackers* e não-*hackers*, de acordo com os seus valores em agradabilidade ($F(266)=3.24$, $p=.07$). Baseado nesta análise, foi conduzida uma regressão logística para determinar se a agradabilidade era um preditor significativo de *hacking*, tendo os resultados revelado que baixos níveis de agradabilidade eram um preditor moderadamente significativo de *hacking*. Apesar de ser um comportamento medido à parte, a escrita de vírus é algo que alguns autores inserem no espectro de *hacking* e, neste estudo, apresentou-se significativamente relacionado com agradabilidade ($rpb= -.17$ ($p<.01$)) e conscienciosidade ($rpb= -.17$ ($p<.01$)), demonstrando que indivíduos que escrevem vírus

possuem menores níveis de agradabilidade e de conscienciosidade, em comparação com indivíduos que não cometem este ato ciberdesviante.

Seigfried-Spellar *et al.* (2017) conduziram um estudo quantitativo numa amostra de 235 usuários recrutados da plataforma MTurk, tendo como objetivo explorar as relações entre comportamento cibercriminoso e a psicopatia, o modelo dos cinco fatores da personalidade e outros tipos de comportamento antissocial. Assim, testaram as correlações entre os traços *Big Five* e diversos comportamentos que caem no espectro do *hacking*, nomeadamente acesso não autorizado, escrita de vírus, monitorização de tráfego de rede e desfiguração de *websites*. O neuroticismo revelou-se estatisticamente significativo para a escrita de vírus ($r=.18$, $p<.01$) e desfiguração de *websites* ($r=.16$, $p<.05$); a abertura à experiência revelou-se estatisticamente significativa para a desfiguração de *websites* ($r=-.13$, $p<.05$); e a agradabilidade revelou-se significativamente significativa para o acesso não autorizado ($r=-.15$, $p<.05$), para a monitorização de tráfego de rede ($r=-.13$, $p<.05$) e para a desfiguração de *websites* ($r=-.13$, $p<.05$).

Em suma, os resultados acerca dos traços de personalidade do Modelo *Big Five* mais relacionados com *hacking* têm apresentado alguma divergência. No que toca à extroversão, cuja importância pensada parte da imagem dos *media* destes indivíduos, que desde cedo retratam um jovem introvertido (Karim *et al.*, 2009), os estudos de Rogers (2006, 2006a), conduzidos em momentos diferentes, levaram a conclusões opostas entre si. No que toca à agradabilidade, os achados são mais consistentes, concluindo uma associação entre menores níveis deste traço e a prática de *hacking*. No que ao neuroticismo, conscienciosidade e abertura à experiência diz respeito, os estudos existentes são muito limitados e os resultados alcançados foram apenas para certos comportamentos específicos medidos, no entanto, parecem apontar para maiores níveis de neuroticismo e de conscienciosidade e para menores níveis de abertura à experiência, em *hackers* (Seigfried-Spellar & Treadway, 2017).

3.4.1.1. Diferenças entre *hackers white hat*, *grey hat* e *black hat* a nível do Modelo dos Cinco Fatores da Personalidade

A literatura que procura aplicar o Modelo dos Cinco Fatores aos diferentes tipos de *hackers* é escassa, tendo-se encontrado apenas um estudo, de Matulessy & Humaira (2016), que o procurou fazer. O objetivo deste era determinar os perfis de personalidade destes três tipos de *hacker*, em função dos *Big Five*. Para tal, aplicaram um questionário

a 30 *hackers*, para avaliarem os fatores da personalidade mais associados a cada tipo. Concluíram que para os *black hat*, o traço prevalente é a abertura à experiência, devido a uma predisposição por parte destes indivíduos a novas ideias, manifestando-se de forma negativa, (Matulesy & Humaira, 2016). Verificaram que os *white hat* têm como traço prevalente a agradabilidade, indo de encontro à restante literatura (e.g., Moore, 2015), visto que procuram beneficiar os outros com a sua atividade associada com o seu desejo de proteger os sistemas informáticos e os seus proprietários, sendo motivados por altruísmo. Por fim, os autores concluíram que o traço prevalente nos *grey hat* é o neuroticismo, consubstanciando-se este numa tendência para a emocionalidade (Costa & McCrae, 1992), associado à tendência de variarem entre *hacking white hat* e *black hat*, revelando um grande espectro de emocionalidade (Matulesy & Humaira, 2016).

3.4.2. Traços de Personalidade do Modelo *Dark Triad*

Outro dos modelos de personalidade que se procura abordar neste trabalho, aplicado ao *hacking*, é a *Dark Triad*, proposta por Paulhus e Williams (2002). A *Dark Triad* consiste em traços de personalidade intercorrelacionados e descritos predominantemente, tal como o nome implica, como traços negativos, sendo associados com tendências para participar em comportamentos não éticos e criminais (Jones & Paulhus, 2014; Paulhus & Williams, 2002). Estes traços são frequentemente estudados no que toca ao dano interpessoal, mas não têm sido estudados extensivamente em contexto de cibersegurança (Jones *et al.*, 2021). A *Dark Triad* é, então, um conjunto de traços de personalidade - maquiavelismo, narcisismo e psicopatia -, no espectro negativo das desordens de personalidade (Paulhus & Williams, 2002). Quanto ao maquiavelismo, indivíduos com elevados níveis deste traço veem outras pessoas mais ou menos como objetos para serem manipulados para atingir os seus objetivos. Os maquiavélicos são, portanto, frios, manipulativos e racionais no seu comportamento. São orientados para objetivos e estratégicos, manipuladores até um determinado ponto o que lhes permite atingir os seus objetivos (Jones & Paulhus, 2014) e têm sido descritos como “moralmente flexíveis” (Jonason *et al.*, 2015, p.103). Já o narcisismo descreve alguém que precisa de admiração e a quem falta empatia por outros. Pauta-se também por aspetos como sentimento de grandiosidade e egocentrismo (DSM-5), possuindo estes indivíduos uma crença inflacionada das suas próprias competências e habilidades (Jones & Paulhus, 2014; Paulhus & Williams, 2002) e um sentimento de intitulado, através do qual tiram vantagem de outros (DSM-5). O último traço do modelo consiste na psicopatia. As tendências psicopáticas levam ao desprezo para com consequências a longo prazo. Indivíduos com

altos níveis de psicopatia revelam baixa capacidade para mostrar empatia, remorso e ansiedade, bem como elevados níveis de impulsividade e procura de sensação, associado a atitudes criminais (Paulhus & Williams, 2002).

Esta teoria tem vindo a ser, recentemente, aplicada ao cibercrime, por exemplo, tem-se observado que uma tendência psicopática parece ser um fator preditor de comportamentos como ciberagressão e *ciberstalking*, *trolling* e pirataria digital (Pabian *et al.*, 2015; Lopes & Yu, 2017; Seigfried-Spellar *et al.*, 2017). O modelo da *Dark Triad* tem sido (escassamente) utilizado na compreensão do *hacking*, tendo os traços abordados sido postulados como preditores para interesse neste comportamento (Gaia *et al.*, 2021).

A ligação entre maquiavelismo e *hacking* foi comprovada no estudo de Jabłońska e Zajdel (2020), que aplicaram um questionário *online* numa amostra nascida entre 1980 e 2000, numa amostra não probabilística, consistindo em pessoas entre os 18 e os 38 anos, de seis regiões da Polónia (N=384), com o objetivo de investigar a relação entre a *Dark Triad* e o comportamento *online*. Vários comportamentos foram medidos, numa escala de Likert de 4 pontos, desde discordo fortemente a concordo fortemente, nomeadamente “desejo de cometer *hacking* num *website*”, tendo-se analisado diferenças relativamente aos traços de psicopatia, maquiavelismo e narcisismo. Para todos os traços a prevalência foi “concordo fortemente”. As médias revelaram uma maior relevância do traço de psicopatia e menor relevância do traço de narcisismo. Seigfried-Spellar e Treadway (2017) testaram também no seu estudo o impacto do traço da psicopatia, utilizando uma medida de psicopatia (Elemental Psychopathy Assessment-Short Form, de Lynam *et al.*, 2013) que mede quatro fatores (Antagonismo interpessoal, Estabilidade emocional, Desinibição e Narcisismo) podendo-se produzir uma pontuação total ou pontual cada fator separadamente. Procuraram relacionar o traço “psicopatia” com os restantes que abordam no seu estudo (*e.g.*, traços Big Five) e com comportamentos antissociais, nomeadamente no ciberespaço. Alguns dos comportamentos averiguados encontram-se no espectro do *hacking*, designadamente, acesso não autorizado, web *defacement*, escrita de vírus e monitoring network traffic (Yar, 2006). Os resultados revelaram que a medida compósita EPA (Elemental Psychopathy Assessment) se revelou significativa para todos os tipos de comportamentos medidos no espectro do *hacking*, sendo que as relações se revelaram moderadas, variando entre $r=.31$ e $r=.38$. Especificamente para o fator “narcisismo”, este demonstrou estar significativamente relacionado, de forma fraca, com todos os comportamentos relevantes, variando entre $r=.16$ e $r=.24$. Pesando todos os

traços medidos neste estudo, a psicopatia foi o traço que revelou relações mais fortes para com cibercrime (Seigfried-Spellar & Treadway, 2017).

Em suma, quanto aos estudos centrados no papel dos traços da Dark Triad na prática de *hacking*, cada um dos traços tem tido a sua importância relatada, consoante a investigação realizada.

3.4.2.1. Diferenças entre *hackers white hat*, *grey hat* e *black hat* a nível da *Dark Triad*

Atualmente, apenas um estudo, de Gaia et al. (2021) procurou analisar as diferenças ao nível da *Dark Triad* em *hackers white hat*, *black hat* e *grey hat*. Este estudo quantitativo foi conduzido através da aplicação de questionários a uma amostra de 474 alunos universitários de gestão e de informática nos Estados Unidos da América, com o objetivo de estabelecer diferenças entre os indivíduos que levam ao interesse em *hacking white hat*, *grey hat* e *black hat*, tendo concluído que, a nível da *Dark Triad*: a psicopatia, ($r=.293$, $p<.000$), o maquiavelismo ($r=.301$, $p<.000$) e o narcisismo ($r=.116$, $p<.009$) se revelaram preditores da atração a *hacking white hat*; a psicopatia ($r=.199$, $p<.001$) e o maquiavelismo ($r=.214$, $p<.000$) revelaram-se preditores da atração a *hacking grey hat*; por fim a psicopatia ($r=.227$, $p<.000$) e o maquiavelismo ($r=.345$, $p<.000$) revelaram-se preditores da atração a *hacking black hat*.

As conclusões alcançadas pelos estudos empíricos relatados permitem compreender que o estudo dos indivíduos praticantes de *hacking* está no início do seu desenvolvimento. Até aqui analisámos as teorias e os modelos que têm sido avançados como potenciais sustentos da prática de *hacking* (Chng et al., 2022). Não obstante, não foi ainda efetuada uma análise combinada destas como explicação destes comportamentos, quer na generalidade dos *hackers*, quer nas suas diferentes manifestações. Historicamente, os *hackers* foram vistos como um grupo genérico, algo que Rogers (2006) equipara a agrupar todos os indivíduos criminosos numa só categoria. É, desta forma, necessário também explorar de que forma os fatores individuais retratados anteriormente contribuem para a distinção dentro desta comunidade. Através da junção destas teorias e da sua posterior aplicação aos diferentes tipos de indivíduos praticantes de *hacking*, ambiciona-se, com o presente estudo, o alcance de uma visão mais compreensiva e completa acerca do *hacking* e dos *hackers*.

CAPÍTULO II – ESTUDO EMPÍRICO

Neste capítulo será apresentado o estudo empírico conduzido. Primeiramente, serão explanados os objetivos gerais e específicos, bem como as hipóteses formuladas, a testar. De seguida, será descrita a metodologia utilizada para atingir estes objetivos, designadamente, o tipo de estudo adotado, as técnicas de amostragem e os procedimentos seguidos para a construção do instrumento, recolha de dados e análise dos mesmos.

1. Objetivos do estudo

1.1. Objetivos gerais e específicos

Esta dissertação pretende abordar a temática do *hacking* e terá como principal alvo os indivíduos praticantes deste comportamento, procurando-se aprofundar o conhecimento acerca dos mesmos. Para tal, e no seguimento do exposto no capítulo anterior, o presente estudo terá como objetivos gerais: 1) Analisar e compreender a influência de características individuais na prática de *hacking*, ou seja, perceber quais as variáveis que melhor explicam este tipo de comportamento; 2) Analisar e compreender a influência de características individuais no tipo de *hacking* praticado.

Especificamente, pretende-se: 1) Analisar a influência das variáveis sociodemográficas (*e.g.*, idade, género, escolaridade, setor profissional e setor profissional parental) na prática de *hacking*, através da comparação entre *hackers* e não *hackers*; 2) Estudar a influência do autocontrolo na prática de *hacking*, através da comparação entre *hackers* e não *hackers*; 3) Estudar a influência dos traços de personalidade (*i.e.*, traços que constituem os modelos de personalidade *Big five* e *Dark triad*) na prática de *hacking*, através da comparação entre *hackers* e não-*hackers*; 4) Analisar a preponderância das características sociodemográficas elencadas previamente, autocontrolo, traços de personalidade e motivações em tipos distintos de *hackers* (*i.e.*, *hackers black hat*, *hackers grey hat* e *hackers white hat*).

1.2. Hipóteses de Investigação

Tendo em conta os objetivos do presente estudo, bem como as teorias e literatura científica previamente descritas, foi formulado um conjunto de hipóteses que se pretendem testar.

Quanto à prática de *hacking*, concretamente, colocam-se as seguintes hipóteses: **H1**. Os *hackers* têm um perfil sociodemográfico diferente de não-*hackers*, sendo que, em comparação com estes, os *hackers* são (a) maioritariamente do sexo masculino, (b) encontram-se empregados com maior prevalência no setor tecnológico, (c) possuem

maior prevalência de pais empregados no setor tecnológico e (d) possuem maiores níveis de escolaridade. **H2.** Indivíduos com menores níveis de autocontrolo têm maior propensão para a prática de *hacking*, em comparação com indivíduos com níveis mais elevados de auto-controlo. **H3.** Quanto aos traços de personalidade *Big five*, indivíduos com maiores níveis de (a) abertura à experiência e (b) neuroticismo e menores níveis de (c) extroversão, (d) agradabilidade e (e) conscienciosidade terão maior propensão para serem praticantes de *hacking*. **H4.** Quanto aos traços da *Dark triad*, face aos não-*hackers*, os *hackers* apresentam maiores níveis de maquiavelismo (a), psicopatia (b) e (c) narcisismo.

Quanto à prática de *hacking* de tipo *black hat*, *grey hat* e *white hat*, são delineadas as seguintes hipóteses⁶: **H5.** Existem diferenças a nível sociodemográfico entre *hackers black hat*, *grey hat* e *white hat*. **H6.** Os níveis de autocontrolo são menores em *hackers black hat* e maiores em *hackers white hat*. **H7.** Existe uma relação entre os traços *Big Five* e o tipo de *hacking* praticado. **H8.** Existe uma relação entre os traços da *Dark Triad* e o tipo de *hacking* praticado. **H9.** Existem diferenças a nível de motivação entre os diferentes tipos de *hackers*.

2. Desenho da investigação

A presente investigação procura explorar, destacadamente, as características individuais de indivíduos que praticam *hacking*, investigando a correlação entre estas características e o cometimento de *hacking* e tipo de *hacking*. Designa-se, assim, como estudo quantitativo, tendo em conta a forma como os dados são recolhidos e analisados, e de carácter correlacional, com o intuito de explorar uma correlação entre variáveis, suportado por toda a revisão de estudos científicos realizados neste âmbito. O método correlacional permite estabelecer relações entre variáveis e quantificar essas relações, indo além dos métodos descritivos da realidade, pois não se limita à descrição dos fenómenos, mas ficando aquém dos estudos experimentais, pois não permite atribuir causalidade às relações encontradas entre as variáveis (Freire & Almeida, 2008). Trata-se, também, de um estudo transversal uma vez que os dados são recolhidos num único momento temporal, não havendo manipulação das variáveis independentes (Marôco, 2007). É ainda um estudo retrospectivo, visto que procura obter informações respetivas a acontecimentos prévios, neste caso, a prática de *hacking*, que é medida,

⁶ Devido à existência de bibliografia limitada que averigua a existência de diferenças entre tipos de *hackers* foram construídas hipóteses gerais.

restrospectivamente, no ano prévio à data de aplicação do questionário; e explicativo, uma vez que procura perceber quais as variáveis independentes que podem explicar a dependente, examinando a potencial associação entre a prática de *hacking* e o autocontrole, os traços de personalidade e as motivações (Marôco, 2007).

3. Amostra e Amostragem

A amostra total do estudo é constituída por 593 indivíduos, que responderam ao questionário online, sendo que estes indivíduos foram alcançados por meio de várias formas de divulgação. Em primeiro lugar, o questionário foi divulgado por universidades (públicas e privadas), bem como por escolas profissionais. Procurou incidir-se, sobretudo, em cursos (CTeSP, licenciaturas, mestrados, doutoramentos, pós-graduações) na área tecnológica e informática, acreditando-se ter, a partir destes, uma maior prevalência de indivíduos praticantes de *hacking*. Alguma literatura tem defendido que em amostras de alunos universitários se observam maiores níveis de cibercrime, nomeadamente *hacking* (e.g., Skinner & Fream, 1997), acrescentando que estudantes na área informática têm maior probabilidade de ter a motivação e habilidade para praticarem atividades de *hacking* e terão também maior probabilidade de já terem cometido este tipo de comportamentos (Hu *et al.*, 2013).

Ademais, procurou divulgar-se o questionário por empresas informáticas, obtendo resposta positiva de uma empresa. Perante a baixa amostra e baixa aderência das universidades/escolas nacionais ao pedido de divulgação, foram feitos novos pedidos, nomeadamente interpellando aos diretores dos cursos pretendidos.

Por fim, o estudo foi divulgado em redes sociais, como Facebook e Reddit e, através destes, em fóruns de *hacking*, recorrendo à técnica de amostragem de *snowball*, um método que consiste em pedir a participantes que indiquem outros indivíduos, que se enquadrem nos objetivos do estudo, que possivelmente estariam disponíveis para fazer parte do estudo. Assim, ao longo de todo o processo de recolha de amostra o tipo de amostragem utilizada foi não-probabilística, por conveniência, dada a impossibilidade de garantir a mesma probabilidade de inclusão no questionário. Ainda, é uma amostragem por conveniência sendo os indivíduos selecionados pela sua maior acessibilidade e disponibilidade (Marôco, 2007).

4. Operacionalização das variáveis e construção do questionário

Como mencionado, o estudo foi operacionalizado por meio de um questionário *online* de autorrelato, construído na plataforma LimeSurvey, cujas variáveis medidas e método de construção são elencados de seguida.

4.1. Construção do questionário

Considerando-se a metodologia quantitativa como a mais adequada para responder aos objetivos e hipóteses propostas para este estudo e tendo em conta a natureza do mesmo, daqui derivou a escolha de um questionário *online* de autorrelato. De acordo com Bachmann (2008), os questionários eletrónicos são os mais indicados para este tipo de estudo, uma vez que permitem captar a vasta gama de diferentes tipos de *hackers*. Os estudos que utilizam estas técnicas de medição seriam mais especificamente orientados para os diferentes tipos de *hackers* e produziram resultados pautados por maior pormenor e abrangência, sem excluir sistematicamente qualquer tipo de *hacker*. Deste modo, poderiam dar respostas a questões prementes, como qual é, exatamente, o rácio entre *hackers white hat* e *hackers black hat*, e que fração da comunidade de *hackers* é composta por *hackers* cumpridores da lei (Bachmann, 2008). Para a construção do questionário final, cuja estrutura será descrita em seguida, procedeu-se a uma análise da literatura com objetivos semelhantes. O questionário consiste em sete grupos, tendo estes derivados de medidas e itens presentes na bibliografia empírica considerados indicados para medição das variáveis em estudo e, quando isto se revelava impossível, procedendo-se à sua adaptação ou elaboração das medidas necessárias e adequadas, recorrendo-se a bibliografia, tanto empírica, como não empírica. Assim, a construção do questionário para esta investigação foi um processo realizado por etapas:

1) Uma extensiva recolha bibliográfica sobre instrumentos de medição das variáveis a estudar, que fossem, sobretudo, utilizados e validados na comunidade científica e em Portugal. Aqui, um dos fatores que pesou foi, igualmente, a extensão dos instrumentos, uma vez que várias variáveis são medidas e os questionários mais usados são mais extensos e conduzem a uma grande taxa de desistência, afetando a validade interna;

2) Estabeleceu-se contacto com investigadores da área da cibersegurança, com o propósito de ter um parecer sobre as medidas construídas para efeitos deste estudo (escalas referentes ao hacking), uma vez que não teriam sido validadas previamente;

3) A realização de um pré-teste com uma versão não definitiva do questionário, o que permitiu o seu aperfeiçoamento para este estudo em concreto, sendo o processo detalhado no ponto 5.

Após estas atividades científicas, deu-se por concluída a fase de construção do questionário. Nas próximas linhas, estarão descritos, detalhadamente, os grupos pertencentes ao mesmo, nomeadamente as questões que os compõem, a forma de codificação das variáveis e índices que serão posteriormente analisados.

Consentimento Informado

Ao realizar uma investigação é crucial considerar princípios éticos da investigação científica, bem como esclarecê-los junto dos potenciais participantes. Particularmente na Criminologia é extremamente importante abordar de forma cuidadosa temas como o anonimato e a confidencialidade. Isto porque a investigação criminológica toma como estudo um objeto sensível relacionado com o crime. Todos estes pressupostos mencionados são assegurados por meio do consentimento informado. Este está presente na página inicial e possibilitou ao participante a tomada de decisão acerca da sua participação no estudo. Para uma decisão livre e informada, o formulário de consentimento informado serviu para, detalhadamente, informar o possível participante acerca da natureza e objetivos do estudo. Acentuou, ainda, a natureza voluntária da participação no estudo, em que uma das suas componentes, também assegurada, é a possibilidade de se poder retirar em qualquer fase da investigação e por qualquer motivo, sem prejuízo (Agrawal, 2003). Por fim, foram ainda assegurados o anonimato e confidencialidade dos dados recolhidos, garantindo a sua utilização somente no âmbito académico, sendo isto importante para aumentar a confiança dos participantes em revelar comportamentos criminalmente sancionáveis (Seigfried-Spellar & Treadway, 2014), como seria o caso, em princípio, dos *hackers black hat* e *grey hat*.

Grupo I – Questões sociodemográficas

Neste grupo, procurou-se obter informações que permitissem caracterizar sociodemograficamente os sujeitos, incluindo diversas variáveis que têm sido encontradas pela literatura como estando relacionadas com o cometimento de *hacking* (VD). As variáveis sociodemográficas constituem-se como variáveis independentes neste estudo, englobando: 1) género; 2) idade; 3) habilitações literárias; 4) setor de profissão; 5) setor de profissão parental. Neste grupo colocam-se as questões consideradas menos invasivas, consistindo, no total, em oito questões. As variáveis independentes neste estudo são as características individuais, englobando as variáveis sociodemográficas (*i.e.*, género, idade, habilitações literárias, setor de profissão, setor de profissão parental).

Concretamente, a primeira questão do grupo aborda o género, variável nominal (1=feminino, 2=masculino, 3=outro⁷). Já a segunda questão, aborda a idade do inquirido, variável quantitativa contínua, baseando-se na idade deste (em anos) no momento da

⁷ A categoria “outro” foi utilizada apenas para efeitos de estatística descritiva. Uma vez que poucos indivíduos selecionaram esta categoria (N=11), optou-se por relatar estes como *missing values*.

recolha de dados (Holt *et al.*, 2011; Nodeland & Morris, 2018). A terceira questão deste grupo diz respeito às habilitações literárias (variável ordinal) questionando-se o nível mais elevado de escolaridade “Que habilitações literárias possui (ano mais elevado de escolaridade completo)?”, através de uma lista *dropdown* de 7 opções, desde 1º ciclo (=1) a Doutoramento (=7)⁸. Também a situação profissional, variável nominal, foi questionada aos indivíduos, medida através de 4 categorias (0= estudante; 1= trabalhador; 2= trabalhador-estudante; 4=outro). Em caso de estudante, uma questão-filtro questiona o participante acerca do grau (1=licenciatura, 2=mestrado, 3=doutoramento, outro) e ano (medida quantitativa) que frequentam atualmente, para efeitos de estatística descritiva. Caso se posicionem como estudante, trabalhador-estudante ou trabalhador, uma segunda questão-filtro é utilizada para averiguar se o participante atualmente estuda/trabalha numa área relacionada com o setor informático, através de uma medida dicotómica (0= não; 1= sim). Como visto, Steinmetz (2016) demonstra, através de metodologia qualitativa, que não só os *hackers*, mas também os seus pais possuem frequentemente empregos no setor tecnológico. Não tendo sido encontrados estudos empíricos que operacionalizassem esta variável, foi necessário adaptar estes itens para uma medida quantitativa. Assim, a ocupação parental é medida através da questão “Algum dos seus pais se encontra a trabalhar ou já trabalhou no setor informático/tecnológico?” e operacionalizando através de uma lista *dropdown* (0=nenhum, 1=a minha mãe, 2=o meu pai, 3=ambos)⁹.

Grupo II – Prática de hacking

O grupo II é composto por apenas uma questão, que operacionaliza e mede a primeira variável dependente: a prática de *hacking*. Partindo da delimitação concetual de autores como Holt (2007), Fox e Holt (2021) e Holt e Steinmetz (2020), começou-se por apresentar uma definição de *hacking*: o uso de tecnologia para ganhar acesso a computadores e dados com ou sem a permissão da pessoa proprietária (Fox & Holt, 2021). Esta definição alargada possibilita englobar a utilização de *hacking* para fins tanto lícitos como ilícitos (Fox & Holt, 2021), algo crucial para o presente estudo, devido aos seus objetivos. A prática de *hacking* é medida de forma dicotómica (0=não, 1=sim), questionando os indivíduos se “Tendo por base a definição apresentada, praticou hacking nos últimos 12 meses?”, sendo este item utilizado por vários outros trabalhos na mesma

⁸ Posteriormente, esta questão foi recodificada numa variável dicotómica (0=até ao ensino secundário e 1=a partir do ensino secundário).

⁹ Posteriormente, esta questão foi recodificada numa variável dicotómica (0=nenhum e 1=mãe, pai ou ambos).

linha de investigação (e.g., Holt *et al.*, 2012; Marcum *et al.*, 2014; e Back *et al.*, 2018). Esta abordagem tem a vantagem de permitir aos inquiridos autoidentificar o que consideram ser o *hacking*, sem quaisquer juízos de valor assumidos (Steinmetz, 2015). Além disso, esta definição é coerente com a gama de atividades que podem ser definidas como *hacking*, abrangendo aplicações ilegais e éticas, bem como atividades simples ou mais complexas (Holt, 2007; Jordan & Taylor, 1998). Tanto esta medida de autorrelato como a definição utilizada foram as consideradas mais indicadas e congruentes com os objetivos do estudo, pois permitem um maior alcance das atividades que podem ser definidas como um *hack*, incluindo aplicações e propósitos legítimos, ilegítimos ou criminais (Fox & Holt, 2021). Em caso de resposta negativa, não haverá preenchimento do grupo seguinte e os participantes são direcionados ao grupo V e seguintes (variáveis individuais), devido a uma quota programada para o efeito. Em caso de resposta positiva, os participantes são direcionados para o grupo seguinte, que averigua o tipo de *hacking* que percebem praticar, bem como os comportamentos realizados, nos 12 meses prévios à aplicação do questionário.

Grupo III – Tipo de *Hacking* praticado

Este grupo é composto por duas questões, operacionalizando a segunda variável dependente, referente ao tipo de *hacking* praticado. Ambos os itens foram construídos a partir de literatura previamente descrita. Primeiramente, foi construída uma medida assente na autoperceção dos *hackers*. Esta técnica, empregue também por Matulessy & Humaira (2016), baseia-se no pressuposto de que os sujeitos são mais capazes de se compreenderem a si próprios do que qualquer outra pessoa e que a informação que fornecem sobre si próprios é passível de ser, portanto, exata e fiável (Matulessy & Humaira, 2016). Assim, foram apresentadas definições para cada tipo de hacker, construídas de forma a serem abrangentes para com tanto a concetualização original, de Moore (2015), como para com as concetualizações mais atualizadas. Assim, após uma extensa revisão bibliográfica, foram retirados os conceitos que surgem nas definições de cada artigo/obra com maior incidência, para possibilitar a construção das definições finais, sendo estas: 1) ***Hacker Black Hat*** (=1): Ajo tanto ilegalmente como maliciosamente nas minhas atividades de *hacking*; 2) ***Hacker Grey Hat*** (=2): Procuro descobrir vulnerabilidades, ainda que de forma não autorizada, sem objetivos maliciosos ou, apenas, para obter algum ganho financeiro; 3) ***Hacker White Hat*** (=3): Nas minhas atividades de *hacking* atuo de forma autorizada com o propósito de proteger, isto é, identificar e/ou resolver problemas de segurança em sistemas e redes.

Por outro lado, foi também construída uma medida comportamental, averiguando-se, numa escala de *likert* de 4 pontos, em que 1 corresponde a nunca e 4 a sempre, a frequência dos comportamentos cometidos. Nesta escala foram mensurados 15 comportamentos, divididos igualmente pelos diferentes tipos de *hackers* avaliados, explanada de seguida. Releva dizer que se procurou opiniões de especialistas para constituição dos itens e avaliação da escala final, designadamente indivíduos na área informática e *hackers white hat*.

a) Itens referentes a comportamentos de hacking Black Hat

A constituição dos itens de *hacking black hat* partiu, principalmente, da escala de Skinner e Fream (1997), adaptando-a aos objetivos do estudo. Esta escala, que consiste em seis itens (e.g., “usou alguma forma de *malware* para aceder a um computador que não o seu”), está pensada para *hackers* maliciosos, contudo, uma vez que os comportamentos dos três tipos de *hackers* muitas vezes se sobrepõem, distinguindo-se apenas pela intenção, a escala foi adaptada adicionando a todos os itens a condição de “por malícia ou para ganhos pessoais”, fazendo isto parte da definição de Moore (2015) de *hacker black hat*. Assim, foram criados os seguintes itens: (1) “Adicionei, apaguei, mudei, copiei ou imprimi alguma informação nos ficheiros de computador de outra pessoa sem o seu conhecimento ou permissão, por malícia ou ganhos pessoais.”; (2) “Acedi ao computador, ficheiros, redes ou contas de alheios sem consentimento dos seus proprietários, por malícia ou ganhos pessoais.”, sendo ambos retirados adaptados da escala de Skinner & Fream (1997); (3) “Escrevi, usei ou distribuí *malware* ou partes de *malware* (e.g., cavalos de tróia, emails *Phishing*, vírus, *worms*, etc), por malícia ou ganhos pessoais.”, sendo este item construído através da junção de três itens da escala de Skinner & Fream (1997) (“Usou *software* que destruiria os dados informáticos de outra pessoa”, “Usou alguma forma de *malware* para aceder a um computador que não o seu” e “Escreveu *malware* ou partes de *malware*”) e um item recolhido de um estudo de Bachmann (2008) (“Distribuí algum tipo de *malware*”), adicionando, ainda, exemplos de *malware*; (4) “Já procurei ou consegui roubar informação sensível, pessoal e dados de empresas, por malícia ou ganhos pessoais.”, tendo sido construído a partir da revisão bibliográfica de Jaquet-Chiffelle e Loi (2020); e (5) “Procurei vulnerabilidades para ganhar acesso a informação, para alterar ou distribuir, ou danificar um sistema ou rede, por malícia ou ganhos pessoais.”, retirado do artigo da revista *Red Hat* (2003).

b) Itens referentes a comportamentos de hacking White Hat

Para os itens da escala de *hacking white hat*, foram construídos os seguintes itens: (1) “Acedi de forma autorizada pelo proprietário a sistemas ou redes, para identificar e/ou resolver vulnerabilidades”, retirado e adaptado da definição de Moore (201); (2) “Intervi no sentido de identificar, proteger e/ou combater indivíduos que acedem a sistemas informáticos, com objetivos maliciosos ou por ganhos pessoais, recolhido e adaptado de uma revisão bibliográfica de Yaacoub *et al.* (2021), que retrata as ações de *hackers white hat* como *hacking* ofensivo com o propósito de combater *hackers black hat*; (3) “Forneci programas de segurança para proteger os sistemas de serem ilegalmente e maliciosamente penetrados.”, retirado da definição de Moore (2015); (4) “Realizei atividades em âmbito de emprego numa agência ou empresa, para testar e fortalecer as redes de segurança *online*”, construído a partir de várias revisões bibliográficas (*e.g.*, Barber, 2001; Abeoussi, 2019; Goerzen & Matthews, 2019; Kirsch, 2014; Chang & Whitehead, 2022); e (5) “Examinei *software* lançado, em procura de vulnerabilidades, para submeter a *bug bounty programs* (programas que oferecem recompensas a quem identificar vulnerabilidades e as divulgar ao fabricante).”, construído a partir da definição de Votipka *et al.* (2018), fornecendo ainda a definição de *bug bounty programs*.

c) Itens referentes a comportamentos de hacking Grey Hat

Por fim, a escala de *hacking grey hat* consiste nos seguintes itens: (1) “Ofereci-me para resolver vulnerabilidades descobertas, em troca de valor monetário”, construída a partir da definição de Moore (2015); (2) “Divulguei vulnerabilidades de forma pública, de forma a forçar os proprietários do sistema a resolvê-las.”, construída a partir da revisão bibliográfica de Kirsch (2014); (3) “Participei em atividades de *hacking* tanto legítimas, como ilegítimas, dependendo do necessário para atingir os meus objetivos.” (4) “Procurei descobrir vulnerabilidades para as trazer à atenção do proprietário, mas, encontrando-as, é mais importante para mim notificar o público antes, do que o proprietário do sistema.”, construído a partir das revisões de Franklin *et al.* (2019), Kirsch (2014) e Goerzen & Matthews (2019); e (5) “Não considero que tenha aderido a atividades maliciosas, mas também não me preocupei em seguir leis.”, tendo este item sido retirado do estudo de Matulessy & Humaira (2016). Tendo em conta a escala de Skinner & Fream (1997), optou-se por utilizar, igualmente, uma escala de frequência, recorrendo-se a uma escala tipo *Likert* em que 0=Nunca e 4=Sempre, averiguando a frequência de comportamentos nos 12 meses anteriores à aplicação do questionário.

Grupo IV - Motivações

A questão única deste grupo averigua as motivações para o *hacking*, sendo esta outra das variáveis independentes do estudo. Para medir a importância das motivações para o cometimento de *hacking* relatado, procedeu-se à construção de uma lista de onze motivações, tendo por base as que surgem com maior incidência na literatura relevante, sendo algumas por vezes agrupadas numa única categoria, pela sua semelhança.

As motivações tidas em conta, foram, desta feita, adaptadas e formuladas da seguinte forma: (1) *Aprendizagem*; (2) *Desafio intelectual/curiosidade*, agrupadas numa só motivação, uma vez que Madarie (2017) verificou estarem altamente correlacionadas; (3) *Diversão e Lazer* (e.g., Holt, 2011; Seebruck, 2015), (4) *Ideologia* (e.g., Seebruck, 2015), (5) *Lucro* (e.g., Seebruck, 2015), (6) *Prestígio/Estatuto*, agrupados por Bachmann (2010), (7) *Procura de sensações* (e.g., Gaia et al., 2021), (8) *Provar que sou melhor do que outros* (Turgeman-Goldschmidt, 2005), (9) *Vingança* (e.g., Rogers, 2006), (10) *Proteger e defender* e (11) *Fazer o bem/Ajudar os outros* (HackerOne, 2020). Assim, os indivíduos autorrelataram, numa escala de *Likert*, desde 1 (nada importante) a 4 (muito importante), qual a importância de cada motivação na prática dos seus comportamentos de *hacking*. A escolha desta forma de medição parte da assunção de Seebruck (2015), da importância de olhar para as motivações como algo multidimensional, procurando-se, desta forma, aceder ao conjunto de motivações mais importantes e não apenas da primária.

Grupo V – Medição de Baixo autocontrolo

Relativamente ao Grupo V, este engloba a operacionalização do autocontrolo, utilizando-se a escala de Grasmick et al. (1993). Esta escala contém 24 itens de autocontrolo divididos em 6 dimensões, de acordo com a Teoria Geral do Crime (Gottfredson & Hirschi, 1990): (1) impulsividade (e.g., “ajo frequentemente no calor do momento sem parar para pensar”); (2) tarefas simples (e.g., “frequentemente tento evitar projetos que sei que serão difíceis”); (3) procura de risco (e.g., “excitação e aventura são mais importantes para mim do que segurança”); (4) atividades físicas (e.g., “não gosto de tarefas muito difíceis que levam as minhas habilidades ao limite”); (5) egocentrismo (e.g., “se as coisas que eu faço incomodam outras pessoas, é problema delas, não meu”); e (6) temperamento (e.g., “quando estou com muita raiva é melhor que as outras pessoas fiquem longe de mim”). Cada dimensão possui 4 itens, contendo a escala, ao todo, 24 itens. A operacionalização é alcançada através de uma escala de *likert*, de discordo fortemente (=1) a concordo fortemente (=4), em que a sua soma indica o nível de

autocontrolo do indivíduo. Uma pontuação global mais elevada representará um nível mais baixo de autocontrolo, sendo que cada participante obtém um *score* quantitativo entre 24 e 96 pontos (Bossler & Burruss, 2011).¹⁰ Esta é a medida mais utilizada em estudos criminológicos que procurem estudar o baixo autocontrolo, e tem demonstrado uma boa validade e fiabilidade. Aquando da sua primeira utilização, a escala conjunta dos 24 itens demonstrou um bom índice de consistência interna ($\alpha=.80$) (Grasmick *et al.*, 1993), e tem vindo a apresentar valores de consistência interna elevados ($\alpha>.80$) em várias das suas revisões (*e.g.*, DeLisi *et al.*, 2003; Rand *et al.*, 1998). No estudo de Pinto (2023), que realizou uma comparação entre *hacking* malicioso e não-malicioso, esta escala revelou uma fiabilidade de .90. Face a esta escala, uma versão traduzida e aplicada à população portuguesa era já detida pela Escola de Criminologia, pelo que não foi efetuado pedido de autorização aos respetivos autores.

Grupo VI – Medição de traços de personalidade do Modelo Big Five

Para a medição dos traços de personalidade referentes ao Modelo *Big five* optou-se pelo instrumento NEO-FFI-20. Este instrumento corresponde a uma versão reduzida do Inventário de Personalidade NEO (NEO-PIR), primeiramente construída por Costa & McCrae (1978). Os autores do instrumento NEO-FFI (Bertoquini & Pais-Ribeiro, 2006) afirmam que estudos que integram diversos instrumentos e variáveis, como é o caso do presente estudo, podem causar uma diminuição da adesão dos participantes. A escala original, NEO-PIR, é composta por 240 itens. A sua versão reduzida NEO-FFI, composta por 60 itens, é a mais comumente utilizada em estudos similares. Contudo, apesar de reduzida, continua a verificar-se uma alta taxa de desistência, quando aplicada. Assim, procurando colmatar esta limitação já antecipada devido às variáveis que me propus medir, a escolha deste instrumento decorreu, principalmente, da procura por uma forma de medição mais curta, mas cujas características psicométricas não fossem largamente afetadas por este critério. Assim, os autores (Bertoquini & Pais-Ribeiro, 2006), operacionalizaram este modelo através de uma escala de apenas 20 itens, avaliando-os por meio de uma escala tipo Likert de cinco pontos, desde 0 (=discordo fortemente) a 4 (=concordo fortemente). Seguindo a cotação dos autores, a escala seria dividida de igual forma pelas cinco dimensões, consistindo em 4 itens para cada uma destas: neuroticismo (1+6+11+16), extroversão (2+7+12+17), abertura à experiência (3+8+13+18),

¹⁰ Posteriormente, procede-se à divisão do score pelo número de itens, facilitando o tratamento dos dados recolhidos no inquérito a respeito do autocontrolo.

amabilidade (4+9+14+19) e conscienciosidade (5+10+15+20), atentando a que os itens 1, 3, 11, 13, 14, 18 e 19 são cotados inversamente.

No estudo de Bertoquini e Pais Ribeiro (2005), a escala revelou níveis de consistência interna elevados ($\alpha > .70$) em todas as dimensões: 0,90 em neuroticismo, 0,86 na dimensão de extroversão, 0,81 para abertura à experiência, 0,82 em agradabilidade e, finalmente, 0,87 na dimensão de conscienciosidade.

Previamente à sua utilização, foi efetuado um pedido de autorização ao Professor José Luís Pais Ribeiro, que disponibilizou a escala por e-mail, juntamente com as instruções para o seu uso e cotações necessárias.

Grupo VII – Medição dos traços de Personalidade do Modelo Dark Triad

Pretendendo-se avaliar a variável independente referente aos traços de personalidade que integram a *Dark triad*, esta foi operacionalizada através da escala *Dark Triad Dirty Dozen*, uma medida concisa dos traços, construída originalmente por Jonason e Webster (2010) e adaptada para a população portuguesa por Pechorro e colaboradores (2021). Esta é constituída por três subescalas de 4 itens, para cada um dos traços contendo 12 itens ao todo: maquiavelismo (*e.g.*, “tenho tendência a levar as outras pessoas a fazerem o que eu quero”), psicopatia (*e.g.*, “tenho tendência a não sentir remorsos ou arrependimento”) e narcisismo (*e.g.*, “tenho tendência a querer que as outras pessoas sintam admiração por mim”). Aos respondentes pede-se que classifiquem cada uma das afirmações em função da sua concordância com estas, desde discordo fortemente (=1), a concordo fortemente (=5). As três subescalas têm revelado consistência interna adequada, nomeadamente, num estudo de Whithers (2019), o narcisismo cotou ($\alpha = .79$), a psicopatia ($\alpha = .76$) e o maquiavelismo ($\alpha = 0.83$). Também os autores originais realizaram um teste de validação à sua própria escala, tendo os resultados sido consistentes com os apresentados anteriormente (Jonason & Webster, 2010). Ademais, a escala foi já traduzida e validada numa amostra portuguesa, por Pechorro *et al.* (2021). Para o seu uso, foi efetuado um pedido de autorização ao Professor Doutor Pedro Pechorro, que garantiu a autorização e providenciou informação acerca de onde encontrar a escala.

5. Procedimentos de recolha de dados

Após a construção do instrumento e prévio à sua efetiva aplicação, procedeu-se à realização de um pré-teste. O questionário foi testado num pequeno grupo de sujeitos, representativo da amostra do estudo. Este pré-teste foi efetuado através de 4 indivíduos, de diferentes idades de forma a avaliar a compreensão dos itens (Tyupa, 2011). Foram

pedidas uma leitura atenta e a resposta positiva a perguntas sujeitas a filtros (*e.g.*, consentimento informado e prática de *hacking*), de forma a garantir o ensaio de todas as questões. Straub e Gefan (2004) relevam para a importância de fazer um teste piloto de todos os instrumentos presentes num questionário, para prevenir problemas não antecipados de surgir posteriormente, durante a sua aplicação e para testar o tempo e compreensão. Assim, com este pré-teste, concluiu-se uma média de tempo de cerca de 12,5 minutos para completar todo o questionário. A respeito da compreensão e coerência das questões do questionário, algumas questões foram reformuladas (grau escolar atual) e algumas opções de ‘outro’ foram acrescentadas. Outras questões de formatação gráfica foram levantadas (*e.g.*, referente à caixa de resposta ao item “idade”) e resolvidas, antes da publicação do questionário.

6. Procedimentos estatísticos

Esta secção descreve os procedimentos estatísticos adotados aquando da análise de dados, dividindo-se em: criação da base de dados, *screening*, estatística descritiva e estatística inferencial. O tratamento dos dados foi efetuado com recurso ao *software* IBM SPSS Statistics 29.

6.1. Criação da Base de Dados

O primeiro passo dos procedimentos estatísticos passou pela criação e limpeza da base de dados, de forma a facilitar a gestão da informação recolhida pelo questionário e a futura análise da mesma. Durante este passo, definiram-se e categorizaram-se todas as variáveis em conformidade com a sua natureza e tipo, definindo o seu nome, rótulo e valores, eliminando-se ainda secções como a data de preenchimento do questionário, para possibilitar a visualização e tratamento apenas da informação considerada essencial.

6.2. *Screening*

Neste segundo passo realizou-se um processo de *screening*, cujo objetivo foi não só a uniformização e adequação das variáveis para aquele que seria o tratamento estatístico subsequente, mas também o aproveitamento máximo da informação proveniente de todos os participantes. Neste sentido, procedeu-se à imputação de *missing values*, substituindo os valores em falta por uma constante (“999”), realizando-se este processo para os participantes que completaram, pelo menos, o grupo II (prática de *hacking*). Quando isto não se verificou, optou-se pela remoção destes participantes da amostra. Por outro lado, verificando-se desistência após grupos completos (no caso das variáveis individuais) não se procedeu à imputação de *missing values* para os restantes grupos, apenas perante desistência já após começo de um grupo. Quanto ao item que

media o grau de escolaridade que os participantes estudantes e trabalhadores-estudantes se encontram a frequentar, verificou-se, após ordenação dos dados por ordem decrescente, que alguns participantes colocaram o ano atual (*e.g.*, 2024, 2025), procedendo-se, nestes casos, também à imputação de *missing values*.

Quanto às variáveis com opção “outro”, estas foram observadas caso a caso, havendo algumas mudanças nos seus valores. A título de exemplo, para o item relativo à situação profissional, alguns participantes selecionaram “outro”, explicitando depois “docente”. Assim, os valores da situação profissional foram alterados na base de dados, para refletir o estatuto de “trabalhador” e não de “outro”, procurando evitar o enviesamento dos dados.

Para a escala NEO-FFI-20, foi ainda necessário realizar um processo de recodificação, devido a vários itens de cotação invertida, criando assim itens recodificados (1-5, 2-4, 3-3, 4-2 e 5-1).

Por fim, nesta etapa, procedeu-se à criação de variáveis compostas, com os itens das escalas utilizadas no questionário (*i.e.*, autocontrolo, *big five*, *dark triad* e escala comportamental de *hacking*), de forma a resumir os dados de cada escala numa única variável quantitativa, facilitando o seu tratamento. Estas variáveis compostas foram também divididas pelo número de itens (através da operação N_{Sum}/N_{Valid}), para que a variável final fosse a média em números mais fáceis de trabalhar (*e.g.*, o resultado da medida de autocontrolo, que variaria entre 24 e 96, passou a variar apenas entre 1 e 4).

6.3. Estatística Descritiva

6.3.1. Análise Fatorial

Esta etapa decorreu com base na escala comportamental de *hacking* construída.

O método de análise fatorial permite encontrar e analisar a estrutura de um conjunto de variáveis interrelacionadas para posteriormente construir uma escala de medida para fatores. Ou seja, esta técnica exploratória de dados irá permitir que se encontrem as variáveis que partilham de um fator comum latente. Para tal, recorreu-se ao método de rotação *varimax* com Normalização de Kaiser, para serem válidas as componentes a partir dos itens da estrutura inicial.

Uma vez que a escala já se encontrava construída, foram empregues dois métodos, para comparação: em primeiro lugar, recorreu-se ao método da Análise Fatorial Exploratória, sendo as variáveis agregadas conforme o fator latente, independentemente do número de fatores, tendo este método resultado em 4 fatores distintos; em segundo lugar, efetuou-se uma Análise Fatorial Confirmatória, usada quando já existe uma teoria

ou modelo pré-definido sobre quantos fatores existem e que itens estão associados aos mesmos. A tabela (cf. Anexo V) representa uma matriz de componentes rotativa, resultado da análise fatorial confirmatória. Esta foi obtida através de uma análise de componentes principal, recorrendo ao método de rotação Varimax, que foi utilizada para identificar a estrutura subjacente de um conjunto de 15 itens. Os resultados demonstraram agrupamento em três fatores principais: o Fator 1 consistiu nos itens 1, 2, 3, 4, 5 e 13; o Fator 2 agrupou os itens 6, 7, 8, 9 e 10; e, por fim, o Fator 3 agrupou 11, 12, 13, 14 e 15. À exceção dos itens 11 e 13, todos os itens revelam uma alta carga fatorial ($>.5$). Estes resultados ajudam a validar a estrutura da escala e confirmam que os itens se agrupam, à exceção do item 13, que revela maior ligação (.474) para com o fator 1 (*hacking black hat*) do que para com o fator 3 (*hacking grey hat*) (.449), para o qual foi pensado e formulado. Assim, este item teria de ser repensado ou removido da escala. Ademais, a escala formulada revelou alfas de Cronbach satisfatórios, designadamente: .87 para a escala com os itens *black hat*; .81 para a escala com os itens *white hat*; e .64 para a escala com os itens *grey hat*.

6.3.2. Testes de fiabilidade

Foram realizados testes de fiabilidade, com o intuito de analisar a consistência interna do conjunto de itens que constituem as escalas a usar na presente investigação. Para medir a consistência interna dos itens que integravam cada uma das escalas utilizou-se o índice do alfa (α) de Cronbach. Caso o valor do alfa se situe: entre 0.7 e 0.8 é considerado razoável; entre 0.8 e 0.9 é bom; e se for superior a 0.9 é visto como excelente (Hill & Hill, 1998; Field, 2013).

6.3.3. Estatística univariada

Para a análise univariada foram utilizadas algumas medidas de tendência central. No caso de variáveis quantitativas (e.g., idade, autocontrolo, motivações, traços *big five*, traços *dark triad*) recorreu-se a medidas como a média amostral (M) e o desvio padrão (DP) para verificar qual a dispersão perante o valor médio, apresentando-se ainda os limites mínimos e máximos (Min.; Máx.). Para variáveis de índole qualitativa (e.g., género, habilitações literárias, situação profissional, habilitações a frequentar, estudo/emprego em área informática e emprego parental em área informática, prática de *hacking* e tipo de *hacker*), recorreu-se a frequência (N) e percentagens (Marôco, 2007).

6.3.4. Estatística bivariada

Quanto à escolha dos métodos estatísticos a adotar, esta foi tomada tendo em conta o Teorema Limite Central (Marôco, 2014), que argumenta que perante uma amostra

superior a 30, pode recorrer-se a testes paramétricos. Desta forma, para os testes iniciais, consistindo na amostra total e, num segundo momento, numa comparação entre amostra não-*hacker* e amostra *hacker*, optou-se pelo uso de testes paramétricos, uma vez que a dimensão das amostras a isto possibilita. Por outro lado, perante as comparações entre tipos de *hackers*, optou-se pelo recurso aos métodos não paramétricos, devido à reduzida amostra ($N < 30$) de *hackers black hat* e *grey hat*. Desta forma, de acordo com a tipologia das variáveis utilizaram-se: *testes-t* para amostras independentes, para analisar as diferenças de médias das variáveis quantitativas (idade, autocontrolo e traços de personalidade) entre dois grupos (*hackers* vs. não-*hackers*); testes Kruskal-Wallis, para efeitos de comparações entre mais de dois grupos independentes (*hackers black hat*, *grey hat* e *White hat*) e variáveis quantitativas ou ordinais (idade, autocontrolo, traços de personalidade e motivações), sendo este acompanhado do respetivo teste *post-hoc*; e testes qui-quadrado (X^2) para analisar as associações entre variáveis categóricas (e.g., prática de *hacking*, tipo de *hacker*, género, habilitações, setor profissional, setor profissional parental). No sentido de verificar como as variáveis em estudo se relacionavam entre si, designadamente a intensidade e a direção dessas relações, recorreu-se a medidas de associação e coeficientes de correlação. Para analisar a associação entre duas variáveis dicotómicas, utilizou-se o teste χ^2 de independência, atendendo-se ao coeficiente de *Phi* (ϕ) para verificar a magnitude da associação. Importa ainda referir que nas análises estatísticas efetuadas considerou-se um valor de $p \leq .05$, bilateral, como estatisticamente significativo.

6.4. Estatística Inferencial

Neste estudo foram realizadas análises de regressão logística binárias, no sentido de analisar as variáveis independentes que melhor explicam a prática de *hacking*. Para a realização destas operações, dicotomizaram-se as variáveis nominais (habilitações, género e setor profissional parental) em variáveis *dummy*, da seguinte forma: quanto às habilitações, anteriormente cotadas de 1 (1º ciclo) a 7 (doutoramento), esta variável é agora dicotomizada de forma 0= 1º ciclo até ao ensino secundário e 1=a partir do ensino secundário; para dicotomização do género, foi removida a categoria “outro”, devido à reduzida amostra ($N=11$); finalmente, para o setor da profissão parental, que era categorizado em 0 (Nenhum), 1 (Mãe), 2 (Pai) e 3 (Ambos), este é dicotomizado em 0 (Nenhum) e 1 (Mãe, Pai, Ambos). Uma vez realizada esta preparação, foram criados três modelos, em que o primeiro incluiu as variáveis sociodemográficas, o modelo dois incluiu as variáveis individuais (i.e., autocontrolo e variáveis da personalidade) e, por fim, o

modelo três incluiu todas as variáveis (sociodemográficas e individuais). Para analisar estes modelos, teve-se em conta os valores do R^2 ajustado, bem como os valores de B e *pvalue* ($<.05$ para resultados estatisticamente significativos). Além disso, seguindo a sugestão de Menard (2002), de que o coeficiente de tolerância e VIF são adequados para regressões logísticas binárias, salienta-se o facto de que não se observou a existência de indícios fortes de multicolinearidade, ou seja, as variáveis não estavam altamente correlacionadas entre si. Seguido o diagnóstico de colinearidade do SPSS, os valores de VIF foram todos inferiores a 3. Ainda, Freund e Wilson (2002) defendem que níveis de tolerância menores do que .2 indicam problemas de multicolinearidade, tendo-se observado valores superiores no teste.

CAPÍTULO III – RESULTADOS DO ESTUDO EMPÍRICO

1. Caracterização da amostra

1.1. Caracterização com base nas variáveis sociodemográficas

Originalmente, a amostra foi constituída por 794 indivíduos. No entanto, verificou-se a desistência de alguns participantes durante o preenchimento questionário. Para evitar perda de informação, optou-se por manter os participantes que responderam, pelo menos, até à primeira variável dependente (prática de *hacking*). Assim, a amostra final do estudo é constituída por 593 indivíduos.

Na Tabela 1 apresenta-se a caracterização da amostra segundo o conjunto de variáveis sociodemográficas em análise. Note-se que, aquando da descrição destes resultados, será adicionalmente elucidado como algumas das variáveis foram recodificadas para análises subsequentes.

Tabela 1. Caracterização da amostra segundo as variáveis sociodemográficas

Variáveis	N	%	M	DP	Min.	Máx.
Idade	592		30.55	12.52	18	99
Género	593					
Masculino (0)	364	61.4				
Feminino (1)	218	36.8				
Outro (2)	11	1.9				
Habilitações literárias	593					
1.º ciclo (1)	3	0.5				
2.º ciclo (2)	1	0.2				

3.º ciclo (3)	2	0.3
Ensino Secundário (4)	200	33.7
Licenciatura (5)	209	35.2
Mestrado (6)	126	21.2
Doutoramento (7)	52	8.8
Situação profissional	588	
Estudante (1)	262	44.6
Trabalhador/a (2)	186	31.6
Estudante-Trabalhador/a (3)	131	22.3
Desempregado/a (4)	9	1.5
Grau de escolaridade a frequentar	391	
Licenciatura (1)	181	46.3
Mestrado (2)	145	37.1
Doutoramento (3)	37	9.5
Outro	28	7.2
Estudo/emprego na área informática	573	
Não (0)	211	36.8
Sim (1)	362	63.2
Emprego parental em área informática	593	
Nenhum (0)	516	87
Mãe (1)	12	2
Pai (2)	51	8.6
Ambos (3)	14	2.4

Nota: M = Média; DP = Desvio padrão; Min. = Mínimo; Máx. = Máximo

No que respeita à *idade*, os inquiridos (N=592) têm idades compreendidas entre os 18 e os 99 anos, com uma média de cerca de 31 anos (30.55) e um desvio-padrão de 12.52. Relativamente ao *género*, predomina o masculino comparativamente ao feminino (61.4% e 36.8%, respetivamente), ressaltando que 11 (1.9%) indivíduos se identificaram como ‘outro’. Devido à baixa frequência desta última categoria, optou-se por transformar estes valores em *missing values* devido a posteriores testes a realizar. Assim, a percentagem válida do sexo feminino passou a ser de 37.5% e a do sexo masculino de 62.5%. No que concerne às *habilitações literárias*, constata-se que os três graus concluídos mais

predominantes são a licenciatura (N=209, 35.2%), o ensino secundário (N=200, 33.7%) e o mestrado (N=126, 21.2%). O doutoramento surge também com alguma frequência (N=52, 8.8%) enquanto o 1.º, 2.º e 3.º ciclos são as habilitações com menor frequência (0.5%, 0.2% e 0.3%, respetivamente). Referente à *situação profissional*, constata-se que uma grande parte dos participantes se encontra apenas a estudar (N=262, 44.6%), 31.6% encontra-se a trabalhar (N=186), 22.3% encontra-se em situação de trabalhador-estudante (N=131) e, com menor frequência, 9 indivíduos (1.5%) encontram-se na condição de desempregado. Quanto ao *grau de escolaridade a frequentar*, questionado aos estudantes e trabalhadores-estudantes, verifica-se que 46.3% da amostra (N=181) se encontra a frequentar uma licenciatura, 37.1% um mestrado (N=145) e 9.5% um doutoramento (N=37). Para além desses, 7.2% da amostra (N=28) selecionou ‘outro’, tendo como exemplos ‘CTESP’, ‘Mestrado Integrado’ e ‘Estágio’. Relativamente à variável *estudo/emprego na área informática*, predomina a resposta afirmativa (63.2%) face à resposta negativa (36.8%), ou seja, a maioria dos participantes estudava ou trabalhava na área informática/tecnológica. Finalmente, quanto ao *emprego parental em área informática*, verificou-se que a larga maioria (87%) dos indivíduos da amostra total não possui nenhuma figura parental empregada no setor informático e tecnológico (N=516). Contudo, 8.6% (N=51) afirmou ter o pai a trabalhar, presentemente ou no passado, no setor informático e, com percentagens mais baixas encontram-se os participantes com ambos (N=14, 2.4%), ou apenas a mãe (N=12, 2%), empregados no setor referido.

1.2. Caracterização com base nas variáveis individuais do autocontrolo e traços de personalidade

A Tabela 2 apresenta a estatística descritiva das variáveis individuais.

Tabela 2. Caracterização da amostra segundo as variáveis individuais

Variável		N	M	DP	Min.	Máx.
Autocontrolo ($\alpha=.88$)		448	2.05	.42	1.00	3.83
Big five	Neuroticismo ($\alpha=.69$)	420	3.11	.79	1.00	5.00
	Abertura à Experiência ($\alpha=.77$)	419	3.11	.67	1.25	5.00
	Extroversão ($\alpha=.64$)	419	3.34	.95	1.00	5.00
	Agradabilidade ($\alpha=.74$)	419	3.22	.83	1.00	5.00
	Conscienciosidade ($\alpha=.81$)	419	3.90	.67	1.50	5.00

Dark triad	Psicopatia ($\alpha=.77$)	408	2.64	.85	1.00	5.00
	Maquiavelismo ($\alpha=.75$)	408	2.00	.81	1.00	5.00
	Narcisismo ($\alpha=.79$)	408	2.63	.86	1.00	5.00

Nota: M = Média; DP = Desvio-padrão; Min. = Mínimo; Máx. = Máximo

Focando-nos primeiramente no autocontrole, este apresentou uma consistência interna de .88 e uma média de 2.05 (DP=.42). Quanto aos traços do modelo dos **Big five** verificou-se o seguinte: para a dimensão do *Neuroticismo* obteve-se uma consistência interna de .69 e uma média de 3.11 (DP=.79); o traço de *Abertura à Experiência*, por sua vez, obteve um α de .77 e um valor médio de 3.11 (DP=.67); no que diz respeito à *Extroversão*, esta apresenta uma consistência interna de .64 e uma média de 3.3443 (DP=.95); para a dimensão *Agradabilidade* ($\alpha=.744$) foi encontrado um valor médio de 3.2160 (DP=.83); por fim, a consistência interna do traço de *Conscienciosidade* foi de .807 e este apresentou uma média de 3.90 (DP=.67). Quanto aos traços da **Dark triad**, através da observação da tabela constata-se que a *Psicopatia* se apresentou com uma consistência interna de .77 e uma média de 2.64 (DP=.85). Já para o *Maquiavelismo*, a consistência interna foi de .75 e a média de 2.00 (DP=.81). Por seu turno, o *Narcisismo* apresentou um α de .79 e um valor médio de 2.63 (DP=.86).

Uma vez caracterizada a amostra total, procurou-se, de seguida, atender aos principais objetivos do estudo, nomeadamente, explorar as diferenças entre *hackers* e não-*hackers* e entre tipos de *hackers* (*hackers black hat*, *grey hat* e *white hat*) em função dos conjuntos de variáveis anteriores.

2. Diferenças entre *hackers* e não-*hackers*

Para analisar a existência de diferenças entre *hackers* e não-*hackers*, primeiramente, procurou-se aceder ao número de indivíduos que praticaram *hacking*, recorrendo-se a frequências e percentagens (Tabela 3).

Tabela 3. Caracterização da amostra segundo a prática de *hacking*

Variável	Total	
	N	%
Prática de <i>hacking</i>	593	
Não	472	79.6
Sim	121	20.4

Quanto à prática de *hacking*, a primeira variável dependente do estudo, verificou-se que 79.6% dos indivíduos (N=472) afirmaram não ter praticado *hacking* nos 12 meses prévios à recolha de dados, enquanto 20.4% (N=121) autorrelatou a prática de *hacking*. Posto isto, procurou-se, de seguida, explorar a existência de diferenças, entre ambas as subamostras, com base nas variáveis sociodemográficas e individuais.

2.1.Diferenças sociodemográficas

Seguidamente analisam-se as diferenças sociodemográficas entre *hackers* e não-*hackers*, procedendo-se a diferentes tipos de análise, conforme a natureza das variáveis.

Para a idade, devido à sua natureza quantitativa, recorreu-se a um teste *t* para amostras independentes. Atendendo aos resultados do teste *t* (Tabela 4), conclui-se que não existem diferenças significativas entre os grupos em análise, uma vez que os valores de *p-value* são superiores a .05.

Tabela 4. Comparação de médias de idades entre hackers e não-hackers

Variável	Não-hackers			Hackers			t	p
	n	M	DP	n	M	DP		
Idade	471	30,85	12,515	121	29,37	12,495	1.163	.246

Nota: n = amostra; M = média; DP = Desvio-padrão; p = p-value resultante do teste-t de amostras independentes

Como forma de analisar as diferenças nas restantes variáveis sociodemográficas (de natureza categórica) foram realizados testes de Qui-quadrado (χ^2), um teste de associação, que avalia a existência, ou não, de uma associação entre duas variáveis categóricas.

Para realização destes foi necessário, primeiramente, assegurar três pressupostos base, designadamente: as variáveis são categóricas, há independência de observações e todas as células devem ter contagem esperada superior a 5. Quanto ao último pressuposto, este não se verificou a nível das variáveis “escolaridade” e “setor de emprego parental”, pelo que se optou por colapsar algumas das suas categorias e voltar a executar o procedimento, resultando, de seguida, no preenchimento do pressuposto (Blalock, 1972).

Posteriormente, recorreu-se ao coeficiente de *Phi* (ϕ) para verificar a força da associação, nos casos em que se verificou a rejeição da hipótese nula (H_0 =As variáveis são independentes). Esta medida pode ser interpretada como uma correlação, variando de -1 a +1, em que: valores de |.1 a .29| indica uma correlação fraca; valores de |0.3 a 0.49| indicam uma correlação moderada; e valores de |0.5 a 1| indicam uma correlação forte (Cohen, 1988).

Na Tabela 5 apresentam-se os resultados dos testes Qui-quadrado para analisar as diferenças entre *não-hackers* e *hackers* em função das variáveis sociodemográficas qualitativas.

Tabela 5. Comparação de proporções entre a prática de hacking e as variáveis sociodemográficas categóricas

Variáveis	Total		Não-hackers		Hackers		X ²	p
	n	%	n	%	n	%		
Gênero								
Feminino	218	37.5	194	41.7	24	20.5	17,947	<.001
Masculino	364	62.5	271	58.3	93	79.5		
Habilitações literárias								
Até ensino secundário	206	34.7	165	35.0	41	33.9	.049	.457
A partir de ensino secundário	387	65.3	307	65.0	80	66.1		
Setor de estudo/emprego								
Setor informático	362	63.2	263	57.7	99	15.4	29.047	<.001
Outro	211	36.8	193	42.3	18	84.6		
Setor profissional parental								
Setor informático	77	13.0	57	12.1	20	16.5	1.690	.127
Outro	516	87.0	415	87.9	101	83.5		

Os testes qui-quadrado apresentados são analisados à luz do modelo qui-quadrado de Pearson

No que diz respeito ao género pode-se constatar que a maior parte dos *hackers* é do género masculino. Verificou-se uma associação estatisticamente significativa entre esta variável e a prática de *hacking*, $\chi^2(1) = 17,947$ ($p < .001$). Assim, rejeita-se a hipótese nula (existe independência entre a prática de *hacking* e o género), podendo assumir-se que, portanto, a este nível as diferenças entre *hackers* e *não-hackers* são significativas. Quanto à força da associação, esta revelou ser uma associação fraca ($\phi = .176$, $p < .001$). Quanto às habilitações literárias e ao setor profissional parental, os testes Qui-quadrado não se revelaram significativos ($p = .457$ e $p = .224$, respetivamente). Assim, não é possível afirmar que haja associação entre estas variáveis e a prática de *hacking*. Por fim, quanto ao setor de estudo/emprego dos inquiridos, constata-se uma associação significativa ($\chi^2(1) = 29.0447$ ($p < .001$)) entre ser *hacker* e estudar/trabalhar no setor informático, apesar de ser uma associação fraca ($\phi = .225$, $p < .001$), evidenciando diferenças significativas entre *não-hackers* e *hackers* neste âmbito.

2.2.Diferenças individuais a nível de autocontrolo e traços de personalidade

Para se analisar as diferenças individuais entre *hackers* e não *hackers*, dada a natureza quantitativa das variáveis individuais em causa, recorreu-se a testes de diferenças de médias, mais concretamente, ao teste *t* para amostras independentes. Para a interpretação destes testes, foi primeiramente observado o teste de Levene, o qual testa a hipótese de que as variâncias nos dois grupos são iguais. Verificando-se o teste de Levene como significativo ($p < 0.05$), tal significa que as variâncias são significativamente diferentes e atenta-se ao valor do teste *t* presente na linha “variâncias iguais não assumidas”, caso contrário, atenta-se em “variâncias iguais assumidas”.

Os resultados dos testes anteriormente mencionados encontram-se patenteados na Tabela 6, sendo possível observar-se um conjunto de diferenças estatisticamente significativas.

Tabela 6. Comparações de médias entre hackers e não-hackers ao nível das variáveis individuais de autocontrolo e traços de personalidade

Variáveis	Total		Hackers		Não-hackers		<i>t</i>	<i>p</i> *
	<i>n</i>	<i>M</i> ± <i>DP</i>	<i>n</i>	<i>M</i> ± <i>DP</i>	<i>n</i>	<i>M</i> ± <i>DP</i>		
Baixo autocontrolo	448	2.05 ± .42	73	2.19+.66	375	2.03 ± .34	2.105	.038
<i>Big five</i>								
Neuroticismo	420	3.11±.79	69	3.30±.80	351	3.08±.78	2.137	.033
Extroversão	419	3.11±.67	69	3.15±.72	350	3.10±.66	.550	.583
Abertura à Experiência	419	3.34±.95	69	3.37±1.00	350	3.34±.94	.277	.782
Agradabilidade	419	3.22±.83	69	2.79±.85	350	3.30±.80	-4.767	<.001
Conscienciosidade	419	3.90±.67	69	3.97±.76	350	3.89±.66	.963	.336
<i>Dark triad</i>								
Psicopatia	408	2.64±.85	64	2.96±1.01	344	2.58±.80	2.861	<.001
Maquiavelismo	408	2.00±.81	64	2.58±.98	344	1.90±.73	5.288	<.001
Narcisismo	408	2.63±.86	64	2.59±1.00	344	2.64±.83	-.386	.701

Nota: *M* ± *DP* = Média ± Desvio-padrão; **p* value correspondente ao teste *t* para amostras independentes

Em primeiro lugar, considerando a variável baixo autocontrolo, podemos observar, pelos resultados do teste *t*, a existência de diferenças significativas entre as médias dos grupos em análise ($p=.038$). O grupo dos *hackers* obteve uma média significativamente superior na escala de baixo autocontrolo ($M=2.19\pm.66$),

comparativamente ao grupo dos não-*hackers* ($M=2.03\pm.34$). Assim, pode concluir-se que os *hackers* possuem níveis mais elevados do que os não-*hackers* ($t(79,726) = 2,105$; $p=.038$) na escala de baixo autocontrolo, isto é, revelam ter menor autocontrolo.

No que concerne aos traços do *Big five*, os testes de comparação de médias evidenciaram diferenças significativas apenas ao nível do neuroticismo e da agradabilidade. Quanto ao neuroticismo o teste t revelou-se significativo ($p<.033$), em que os *hackers* possuem valores de neuroticismo mais elevados ($M=3.30$) comparativamente aos não-*hackers* ($M=3,08$) ($t(418) = 2.137$; $p<.033$). Para a agradabilidade, o teste t revelou-se igualmente significativo ($p<.001$), verificando-se que os *hackers* possuem menos agradabilidade ($M=2.79$) comparativamente aos não-*hackers* ($M=3.30$), ($t(417) = -4.767$; $p<.001$). Para os restantes traços que compõem o modelo *Big five*, verifica-se que os *hackers* possuem uma pontuação mais elevada em todos estes, comparativamente aos não-*hackers*, designadamente, na extroversão ($M=3.15$ e $M=3.10$, respetivamente), abertura à experiência ($M=3.37$ e $M=3.34$, respetivamente) e conscienciosidade ($M=3.97$ e $M=3.89$, respetivamente). No entanto, estas diferenças não se revelaram estatisticamente significativas.

Quanto aos traços da *Dark triad*, os testes de comparação de médias demonstraram a existência de diferenças significativas a nível da psicopatia e do maquiavelismo. Para a psicopatia, observam-se níveis significativamente mais elevados de psicopatia por parte do grupo de *hackers* ($M=2.96$) comparativamente ao grupo de não-*hackers* ($M=2.58$), ($t(78,419) = 2.861$; $p<.001$). Também para o traço do maquiavelismo constata-se que o grupo de *hackers* possui um valor significativamente mais elevado deste traço ($M=2.58$) comparativamente aos não-*hackers* ($M=1.90$), ($t(76,373) = 5.288$; $p<.001$). Finalmente, quanto ao narcisismo, embora se observe um nível mais baixo deste traço no grupo de *hackers* ($M=2.59$) comparativamente ao grupo de não-*hackers* ($M=2.64$), esta diferença não é estatisticamente significativa.

3. Motivações dos *hackers*

A Tabela 7 apresenta a caracterização da subamostra de *hackers* segundo as motivações para o *hacking*. Recorda-se que a escala de resposta utilizada variou 1 (nada importante) a 4 (muito importante), como forma de avaliar a importância das motivações presentes na lista e, desta forma, uma média mais elevada expressa uma maior importância dada a determinada motivação pelo conjunto de *hackers*.

Tabela 7. Caracterização da subamostra de *hackers* segundo as motivações para o *hacking* ($N=77$)

Motivações	M	DP	Min.	Máx.
Aprendizagem	3.57	.733	1	4
Desafio intelectual/curiosidade	3.61	.610	2	4
Diversão e Lazer	3.08	.970	1	4
Ideologia	2.30	1.065	1	4
Lucro	2.21	1.092	1	4
Prestígio/Estatuto	2.10	1.033	1	4
Procura de sensações	2.18	1.109	1	4
Provar que sou melhor do que os outros	1.73	.955	1	4
Vingança	1.42	.848	1	4
Proteger e Defender	2.92	1.097	1	4
Fazer o bem/ajudar os outros	3.01	.977	1	4

Nota: M = Média; DP = Desvio-padrão; Min. = Mínimo; Máx. = Máximo

Pela análise da Tabela 7, é possível concluir que “Desafio intelectual/curiosidade” é a motivação mais frequente em *hackers* (M=3.61), seguida de “Aprendizagem” (M=3.57) e “Diversão e Lazer” (M=3.08). Relativamente à motivação “Desafio intelectual/curiosidade”, é de notar que esta varia de 2 a 4, isto é, nenhum dos *hackers* (N=77) selecionou “nada importante” no que toca a esta. Como motivações que surgem como tendo menor importância para os *hackers* temos “Vingança” (M=1.42), “Provar que sou melhor do que os outros” (M=1.73) e “Prestígio/Estatuto” (M=2.10).

4. Regressões logísticas

De modo a perceber que variáveis predizem o *hacking*, foram realizadas regressões logísticas. Foram elaborados dois modelos parcelares (contendo o primeiro as variáveis sociodemográficas; e o segundo as variáveis individuais) e um modelo final (onde foram incluídas todas as variáveis previamente utilizadas nos modelos parcelares).

Devido à natureza binária da variável dependente, prática de *hacking* (0=não, 1=sim), optou-se pela regressão logística binária, utilizada para estimar a probabilidade de um evento (*i.e.*, prática de *hacking*) ocorrer.

4.1. Modelo 1: Características sociodemográficas

No primeiro modelo parcelar (cf. Anexo III) apenas foram incluídas as variáveis sociodemográficas como potenciais preditores do *hacking*. Através da sua análise é possível verificar que o modelo se mostrou significativo ($\chi^2(5) = 46.977, p < .001.$), resultado também comprovado pelo teste de Hosmer e Lemeshow (não apresentado na tabela), que não se demonstra estatisticamente significativo ($p = 0,796$), indicando que o

modelo não está mal ajustado. Ademais, verifica-se que 12,4% (Nagelkerke $R^2=.124$) da variância total na prática de *hacking* é explicada pelas variáveis independentes. Do conjunto das variáveis sociodemográficas presentes no modelo, destacam-se o gênero ($p=.003$), a idade ($p=.010$) e estudar/trabalhar na área informática ($p<.001$), como tendo um efeito significativo sobre a prática de *hacking*. Relativamente ao gênero, os resultados indicam que ao aumentar uma unidade nesta variável independente (ou seja, ser homem) aumenta a probabilidade de praticar *hacking*. Mais concretamente, os indivíduos do gênero masculino têm uma chance 2.279 vezes maior de praticar *hacking* do que para indivíduos do gênero feminino ($p=.003$). Já para a idade, verifica-se um valor inferior a 1 ($OR=.971, p=.010$), indicando uma diminuição da probabilidade com um aumento de uma unidade da variável independente. Para maior clareza, o rácio de probabilidade pode ser invertido ($1/.971=1.03$), indicando que, para cada unidade de redução na variável independente, idade, a probabilidade de praticar *hacking* aumenta por um fator de 1.03. Por fim, estudar/trabalhar na área informática revelou-se também um preditor da prática de *hacking*. Mais concretamente, os resultados indicam que os indivíduos que estudam/trabalham na área informática têm 3.016 vezes mais chances de praticar *hacking* do que os indivíduos que não trabalham nessa área ($p<.001$). Quanto às habilitações literárias e ao emprego parental na área informática, verifica-se que não se mostraram preditores da prática de *hacking* ($p=.058$ e $p=.722$, respetivamente).

4.2.Modelo 2: Características individuais com base no autocontrolo e traços de personalidade

Quanto ao segundo modelo parcelar (cf. Anexo IV), este abrangeu as variáveis individuais (autocontrolo e traços de personalidade). Através da sua análise é possível verificar que o modelo preditivo do *hacking* com base nas variáveis individuais se mostrou significativo ($\chi^2(9)=45.269, p<.001$) e adequadamente ajustado, como comprovado pelo teste de Hosmer e Lemeshow ($p=0.561$). É possível constatar que 18,1% (Nagelkerke $R^2=.181$) da variância total na prática de *hacking* é explicada por este modelo. Do conjunto das variáveis individuais incluídas no modelo, apenas o maquiavelismo ($p<.001$) revelou ter um efeito significativo sobre a prática de *hacking*. Concretamente, os indivíduos com níveis mais elevados de maquiavelismo são mais propensos a praticar *hacking* do que os indivíduos com níveis mais baixos deste traço de personalidade ($OR=2.184$).

4.3. Modelo 3: Modelo final

O modelo final, que se pode observar na Tabela 8, inclui todas as variáveis independentes utilizadas nos modelos parcelares prévios. O modelo revelou-se significativo ($p < .001$) e com qualidade de ajuste, como evidenciado pelo teste de Hosmer e Lemeshow ($p = .783$), e explica 29.3% da variância na prática de *hacking*.

Demonstraram-se preditores da prática de *hacking* a variável “estudar/trabalhar na área informático” e os traços de personalidade “neuroticismo” e “maquiavelismo”, cujos efeitos são detalhados de seguida.

Tabela 8. Modelo explicativo final da prática de *hacking*

Variáveis	Modelo 3			
	B	SE	OR	p
Género (0=feminino)	.685	.416	1.985	.099
Idade	-.025	.016	.975	.123
Habilitações literárias (0=até ensino secundário)	.695	.380	2.005	.067
Estudar/trabalhar na área informática (0=não)	1.531	.441	4.622	<.001
Área informática (pais) (0=nenhum dos pais trabalha na área informática)	.217	.469	1.243	.643
Autocontrolo	-.209	.501	.812	.677
Neuroticismo	.804	.275	2.235	.004
Extroversão	.476	.281	1.609	.090
Abertura à Experiência	.215	.173	1.239	.216
Agradabilidade	-.291	.234	.747	.214
Conscienciosidade	.238	.261	1.268	.362
Psicopatia	.160	.233	1.173	.494
Maquiavelismo	.639	.232	1.895	.006
Narcisismo	-.307	.220	.736	.163
X² + p	72.986; $p < .001$			
-2. Log Likelihood	266.292			
Nagelkerke R²	.293			

Nota: B= coeficientes não estandardizado; SE= erro padrão; OR = *odds ratio*

Relativamente a trabalhar/estudar no setor informático, os resultados indicam que a chance de praticar *hacking* é 4.622 vezes maior para indivíduos que trabalham e/ou estudam neste setor do que para indivíduos que não o fazem ($p < .001$). Já para o neuroticismo os resultados indicam que os indivíduos com níveis mais altos deste traço têm uma chance 2.235 maior de praticar *hacking* do que os indivíduos com níveis mais baixos do mesmo ($p = .004$). Finalmente, para o maquiavelismo, é possível constatar que os indivíduos com níveis mais altos de maquiavelismo têm uma chance quase duas vezes superior ($OR = 1.895$) de praticar *hacking* do que os indivíduos com níveis mais baixo do mesmo ($p = .006$). Em essência, os resultados sugerem que indivíduos envolvidos no setor tecnológico, mais neuróticos e maquiavélicos apresentam uma probabilidade acrescida de se envolverem na prática de *hacking*.

5. Diferenças entre grupos de *hackers* (*black hat*, *grey hat*, *white hat*)

Para analisar a existência de diferenças entre os tipos de *hackers*, primeiramente, procurou-se aceder ao número de indivíduos que praticam cada tipo de *hacking*, recorrendo-se a frequências e percentagens (Tabela 9).

Tabela 9. Caracterização da subamostra de *hackers* com base no tipo de *hacking* que praticam

Variável	Total	
	N	%
Tipo de <i>hacking</i> praticado	86	
<i>Hacking Black Hat</i> (=1)	15	17.44%
<i>Hacking Grey Hat</i> (=2)	21	24.42%
<i>Hacking White Hat</i> (=3)	50	58.14%

Nos seguintes pontos, optou-se por seguir a abordagem não paramétrica, devido às reduzidas subamostras de *hackers black hat* ($N=15$) e *grey hat* ($N=21$). Note-se que os testes não paramétricos não comparam médias entre dois ou mais grupos amostrais. No entanto, nas subsecções seguintes, apresentar-se-ão as médias (nas tabelas e no texto) dos diferentes grupos amostrais nas variáveis em análise para uma melhor ilustração dos resultados.

5.1. Diferenças sociodemográficas

Na Tabela 10 estão presentes as distribuições das pontuações da idade pelos diferentes grupos. A *mean rank* da idade foi de 57.30 para os *black hat*, de 35.67 para os *grey hat* e de 42.65 para *white hat* e, como se pode observar na tabela, verifica-se a existência de uma diferença estatisticamente significativa nas idades entre os diferentes

grupos ($H(2) = 6.731$, $p = .035$). Assim, pode rejeitar-se a hipótese nula (H_0), concluindo-se que, pelo menos dois dos grupos, apresentam diferenças significativas a nível de idades.

Tabela 10. Comparações a nível da variável idade entre os tipos de *hackers*

Variável	<i>Hackers Grey hat</i>	<i>Hackers White hat</i>	<i>Hackers Black hat</i>	Comparações entre grupos: H*
<i>Idade</i>				
<i>N</i>	15	21	50	
<i>M ± DP</i>	34±16.74	26±8.59	28.2±12.38	6.731 ^a ($p = .035$) ^a

Nota: M = Média; DP = Desvio-padrão; *Teste Kruskal-Wallis; ^a Valor de significância ajustado pela correção Bonferroni

Para determinar quais dos grupos são responsáveis pelas diferenças estatisticamente significativas encontradas no teste prévio, foram efetuadas comparações *Post-hoc* recorrendo-se ao método de Dunn com uma correção de Bonferroni para testes múltiplos. As comparações par a par com correção de Bonferroni indicaram que os *hackers grey hat* diferem significativamente dos *black hat* (p ajustado = .031), no sentido em que a *mean rank* da idade do grupo *black hat* foi significativamente maior do que a do grupo *grey hat*. No entanto, não houve diferenças significativas entre as *mean ranks* de idade dos grupos *White hat* e *Grey hat* ($p=.844$) ou entre *White hat* e *Black hat* ($p = .138$).

Para as variáveis sociodemográficas categóricas recorreu-se, mais uma vez, a testes Qui-quadrado de independência. No entanto, devido ao tamanho reduzido das subamostras de *hackers black hat* e *grey hat*, não foi possível assegurar o pressuposto que dita que todas as células devem ter contagem esperada superior a 5 no caso das variáveis género, trabalhar/estudar no setor informático e pais trabalharem no setor informático. Assim, nestes casos optou-se por realizar o teste exato de Fisher, sendo esta abordagem recomendada quando a dimensão da amostra é pequena (ou seja, quando a frequência esperada de uma ou mais células é inferior a cinco) (Blalock, 1972). No caso das habilitações em que a contagem de células esperadas foi superior a 5, recorreu-se ao teste Qui-quadrado de Independência de Pearson.

Posteriormente, nos casos em que houve a rejeição da hipótese nula (H_0 =As variáveis são independentes), recorreu-se a uma medida para verificar a força da associação. Uma vez que a medida de *Phi* é adequada apenas em tabulações cruzadas 2x2, recorreu-se, então, à medida *V* de Cramer. O *V* de Cramer varia entre 0 e 1, em que 0 indica nenhuma associação e 1 indica uma associação perfeita, pelo que Cohen (1988)

sugeriu a seguinte diretriz para interpretar o V de Cramer: a partir de .1 é uma relação baixa; a partir de .3 é moderada; e a partir de .5 é elevada.

De seguida, na Tabela 11, apresentam-se os testes Qui-quadrado para as variáveis sociodemográficas qualitativas em função do tipo de *hacker*.

Tabela 11. Comparação de proporções entre os tipos de *hackers* e as variáveis sociodemográficas categóricas

Variáveis		<i>Black hat</i>		<i>Grey hat</i>		<i>White hat</i>		X ²	p
		N	%	N	%	N	%		
Género (N=83)									
Feminino		2	15.4	5	25	9	18	.665 ^a	.729
Masculino		11	84.6	15	75	41	82		
Escolaridade (N=86)									
Até ensino secundário		4	26,7	7	33,3	19	38	.682 ^b	.705
A partir de ensino secundário		11	73,3	14	66,7	31	62		
Estudar/trabalhar na área informática (N=83)									
Setor informático		8	61,5	19	90,5	46	93,9	8.114 ^a	.009
Outro		5	38,5	2	9,5	3	6,1		
Pais trabalham na área informática (N=86)									
Algum ou ambos		6	40.0	4	19	6	12	5.516 ^a	.057
Nenhum		9	60.0	17	81	44	88		

^a Teste exato de Fisher

^b Qui-quadrado de Pearson

Como se pode observar na tabela, apenas a variável “estudar/trabalhar no setor informático” se revelou significativa ($X^2(2) = 8.114$, $p=.009$). A maioria dos *hackers grey hat* e *white hat* estão no setor informático (90.5% e 93.9%, respetivamente), face a uma menor proporção de *hackers black hat* (61.5%). Assim, verifica-se uma associação significativa entre estudar/trabalhar na área informática e o tipo de *hacker*. Quanto à força da associação, atentando à medida V de Cramer, este teve o valor de .352 ($p=.010$), indicando uma relação moderada (Cohen, 1988). Quanto ao emprego parental no setor informático, o valor de p é 0.057, estando, assim, no limiar da significância estatística, o que sugere uma possível tendência para haver uma associação entre o tipo de *hacking* praticado e a ocupação parental, sendo que a proporção de *hackers black hat* com pelo menos um dos pais no setor informático demonstra ser a mais elevada, face aos restantes tipos. Por fim, para o género e para as habilitações, os testes não se revelaram estatisticamente significativos.

5.2.Diferenças individuais a nível de autocontrolo e traços de personalidade

A nível das diferenças individuais entre *hackers black hat*, *grey hat* e *white hat*, recorrendo ao teste Kruskal-Wallis foram efetuadas comparações em função das variáveis individuais em estudo, as quais podem ser observadas na Tabela 12.

Tabela 12. Comparações a nível de autocontrolo e traços de personalidade entre tipos de *hackers*

Variável	Hackers Black hat	Hackers Grey hat	Hackers White hat	Comparações entre grupos: H*
<i>Baixo Autocontrolo</i>				
N	15	18	40	
M ± DP	2.68±.65	2.25±.71	1.98±.54	15.483 ^a (p<.001) ^a
<i>Big five</i>				
N	13	17	39	
<i>Neuroticismo</i>				
M ± DP	3.42±.90	3.60±.86	3.12±.72	4.566 (p=.102) ^a
<i>Extroversão</i>				
M ± DP	2.87±.77	2.94±.74	3.3333±.65	4.797 (p = .091) ^a
<i>Abertura à Experiência</i>				
M ± DP	4.21±.71	3.26±.84	3.1410±1.02	11.927 (p=.003) ^a
<i>Agradabilidade</i>				
M ± DP	2.06±.98	2.78±.74	3.0449±.71	12.288 (p=.002) ^a
<i>Conscienciosidade</i>				
M ± DP	3.96±.66	3.97±.85	3.9746±.76	.141(p=.932) ^a
<i>Dark triad</i>				
N	13	15	36	
<i>Psicopatia</i>				
M ± DP	3.19±1.09	2.98±.1.12	2.88±.94	1.596 (p=.450) ^a
<i>Maquiavelismo</i>				

M ± DP	2.98±.93	2.97±1.00	2.27±.90	8.619 (p=.013) ^a
Narcisismo				
M ± DP	1.88±.96	2.78±.93	2.76±.95	8.100 (p=.017) ^a

Nota: M±DP = Média±Desvio-Padrão; Valor de significância ajustado pela correção Bonferroni

No que toca às variáveis individuais, é possível constatar, através da observação da Tabela 14, que para o autocontrole se verificaram diferenças significativas entre os três tipos de *hackers* ($H(2) = 15.483, p < .001$). Os *hackers black hat* obtiveram uma *mean rank* de 54.50, os *grey hat* de 39.19 e os *white hat* de 29.45, sendo que uma *mean rank* mais elevada significa menores níveis de autocontrole. Recorrendo ao teste *post-hoc* de Dunn, verificaram-se diferenças significativas entre os grupos *white hat* e *black hat* (p e p ajustado $< .001$), mas não entre o grupo *grey hat* e qualquer combinação com este.

Já para os traços *Big five*, foram encontradas diferenças significativas para os traços de Abertura à Experiência e Agradabilidade. No caso da Abertura à Experiência, as *mean ranks* foram de 52.15, 32.47 e 30.38, para os *hackers black hat*, *grey hat* e *white hat*, respetivamente, demonstrando que, entre os grupos, os *black hat* revelam valores mais elevados deste traço, enquanto os *white hat* possuem os valores mais baixos. As diferenças significativas encontradas foram averiguadas com maior detalhe através do *post-hoc* Dunn, verificando-se existirem a nível dos grupos *white hat* e *black hat* ($p = .001$; p ajustado = .002) e entre *grey hat* e *black hat* ($p = .008$, p ajustado = .023). Para a agradabilidade, as *mean ranks* foram de 18.42 para os *hackers black hat*, 34.32 para os *grey hat* e 40.82 para os *white hat*, demonstrando estes últimos valores mais elevados do traço de agradabilidade, ao passo que os *black hat* demonstraram possuir os valores mais baixos. Ainda, verificaram-se diferenças entre *hackers black hat* e *grey hat*, quando a significância não foi ajustada ($p=.031$), e entre os *hackers black hat* e *grey hat* ($<.001$).

Por fim, para os traços da *Dark triad*, o maquiavelismo e o narcisismo revelaram diferenças significativas. A nível do maquiavelismo, as *mean ranks* para os tipos de *hackers* foram de 40.31 para os *black hat*, 40.13 para os *grey hat* e 26.5 para os *white hat*, demonstrando que os *hackers black hat* e *grey hat* são mais maquiavélicos do que os *white hat*. Tal como anteriormente, recorreu-se ao teste de Dunn, encontrando-se diferenças entre os *white hat* e *grey hat* ($p=.017$; p ajustado=.050) e entre os *hackers white hat* e *black hat* ($p=.021$; p ajustado=.064). Finalmente, a nível do narcisismo, as *mean ranks* foram de 19.42 (*black hat*), 35.74 (*white hat*) e 36.07 (*grey hat*), demonstrando uma tendência para os *grey hat* serem os mais narcisistas, seguidos dos *white hat* e, por fim,

os *black hat* revelam-se como os menos narcisistas. A este nível, o teste de Dunn revelou diferenças significativas entre os grupos *black hat-white hat* ($p=.007$; p ajustado $=.020$) e *black hat-grey hat* ($p=.018$; p ajustado $=.054$).

5.3.Diferenças a nível de motivações

Foram, ainda, realizados testes Kruskal-Wallis para determinar a existência de diferenças a nível das motivações medidas entre os diferentes grupos de hackers: “*black hat*” ($n = 15$), “*grey hat*” ($n = 20$) e “*white hat*” ($n = 42$). A Tabela 13 apresenta os resultados destes testes.

Tabela 13. Comparações entre tipos de *hackers* a nível das motivações

Variável	Hackers Black hat	Hackers Grey hat	Hackers White hat	Comparações entre grupos: H*
<i>Motivações</i>				
<i>N</i>	15	20	42	
<i>Aprendizagem</i>				
M $\pm$ DP	3.80 $\pm$.414	3.45 $\pm$.605	3.55 $\pm$.861	3.488 ^a ($p = .175$) ^a
Desafio intelectual/curiosidade				
M $\pm$ DP	3.60 $\pm$.737	3.60 $\pm$.598	3.62 $\pm$.582	.100 ($p=.951$)
Diversão e Lazer				
M $\pm$ DP	3.33 $\pm$ 1.047	3.30 $\pm$.801	2.88 $\pm$.153	4.681 ($p=.096$)
Ideologia				
M $\pm$ DP	1.80 $\pm$.941	2.30 $\pm$.923	2.48 $\pm$ 1.131	4.467 ($p=.107$)
Lucro				
M $\pm$ DP	2.40 $\pm$ 1.121	2.25 $\pm$ 1.118	2.12 $\pm$ 1.087	.828 ($p=.661$)
Prestígio/Estatuto				
M $\pm$ DP	1.73 $\pm$.961	2.05 $\pm$ 1.050	2.26 $\pm$ 1.037	3.170 ($p=.205$)
Procura de sensações				
M $\pm$ DP	3.13 $\pm$ 1.060	2.00 $\pm$ 1.026	1.93 $\pm$.997	12.394 ($p=.002$)

Provar que sou melhor do que os outros				
M ± DP	1.87±.834	1.85±1.137	1.62±.909	1.570 (p=.456)
Vingança				
M ± DP	1.33±.816	1.70±.979	1.31±.780	4.072 (p=.131)
Proteger e Defender				
M ± DP	1.87±1.125	2.65±.988	3.43±.801	21.861 (p<.001)
Fazer o bem/ajudar os outros				
M ± DP	2.00±1.069	2.85±.813	3.45±.739	21.906 (p<.001)

Como se verifica na Tabela 13, existem diferenças estatisticamente significativas para apenas três das motivações: “Procura de sensações” ($H(2) = 12.394$, $p=.002$); “Proteger e Defender” ($H(2) = 21.861$, $p<.001$) e; “Fazer o bem/ajudar os outros” ($H(2) = 21.906$, $p<.001$). Para a motivação de “Procura de sensações” verificou-se que as *mean ranks* dos hackers *black hat*, de *grey hat* e de *white hat* foram, respetivamente, 56.47, 35.75 e 34.31, revelando ser uma motivação de maior importância para os *hackers black hat* e menor para os *white hat*. Já para “Proteger e Defender”, as *mean ranks* foram de 20,33 (*black hat*), 32,75 (*grey hat*) e 48,64 (*white hat*). Finalmente, quanto a “Fazer o bem/ajudar os outros” verificaram-se as *mean ranks* de 19,73 para *black hat*, de 33,73 para *grey hat* e de 48,39 para *hackers white hat*. Assim, ambas as anteriores são motivações que desempenham um papel maior na prática de *hacking white hat* e menor em *black hat*.

Posteriormente, foram efetuadas comparações entre pares utilizando o procedimento de Dunn (1964) com uma correção de Bonferroni para comparações múltiplas. Esta análise *post-hoc* revelou diferenças estatisticamente significativas nas pontuações da motivação “Procura de sensações” entre os grupos *white hat-black hat* ($p=.002$) e *grey hat-black hat* ($p=.014$), mas não entre os grupos *grey hat-white hat*. Quanto à motivação “Proteger e Defender” verificaram-se diferenças significativas a nível da comparação entre *black hat-white hat* ($p=<0,001$) e *grey hat-white hat* ($p=.018$). Por fim, a motivação “Fazer o bem/ajudar os outros” revelou diferenças significativas a nível dos grupos *black hat-white hat* ($p=<.001$) e *grey hat-white hat* ($p=.032$).

CAPÍTULO IV – DISCUSSÃO

A presente dissertação procurou relacionar um conjunto de fatores individuais com duas variáveis dependentes: por um lado, a prática de *hacking* e, por outro, o tipo de *hacking* praticado. Para tal recorreu-se: 1) à Teoria Geral do Crime (Gottfredson & Hirschi, 1990), medindo o autocontrolo; ao Modelo *Big five*, de Costa e McCrae (1992), medindo os traços neuroticismo, extroversão, abertura à experiência, conscienciosidade e agradabilidade; e ao Modelo *Dark Triad*, proposto por Paulhus e Williams (2002), constituído, por sua vez, por psicopatia, maquiavelismo e narcisismo. Por fim, analisaram-se diferenças a nível das motivações no tipo de *hacking* praticado. Com estes objetivos em consideração, foi aplicado um questionário *online* a uma amostra de 593 indivíduos. Apresenta-se, de seguida, a discussão dos resultados alcançados, tecendo considerações acerca da sua conformidade, ou não, com as hipóteses levantadas.

a) Diferenças entre *hackers* e não-*hackers*

No presente estudo, 20.4% dos participantes afirmou ter praticado *hacking* nos 12 meses prévios à aplicação do questionário, sendo valores relativamente superiores aos que têm sido obtidos na comunidade científica (*e.g.*, 5.4% no estudo de Holt *et al.*, 2020 e entre 7% a 14% no estudo de Marcum *et al.*, 2014), podendo tal dever-se à incidência num ambiente relacionado com as áreas informáticas, para constituição da amostra.

Perante a análise dos resultados, verifica-se que a primeira hipótese – *Os hackers têm um perfil sociodemográfico diferente de não-hackers, sendo que os hackers apresentam (a) maior proporção do sexo masculino, (b) menor média de idades, (c) maior prevalência no setor tecnológico, (d) maior prevalência de pais no setor tecnológico e (e) maiores níveis de escolaridade* - se verifica parcialmente. A análise revela uma prevalência significativa do género masculino (79.5%) na prática de *hacking*, similar a outros estudos, como Fox e Holt (2021) e Hutchings e Chua (2016) (74.6% e 78.6%, respetivamente). Taylor (1999) e Steinmetz (2016) propõem como possível justificação a socialização do género masculino para a tecnologia, desde a adolescência. Aliado a isto, verifica-se maior prevalência de estudantes masculinos em cursos da área de informática, levando à aquisição de conhecimentos para a prática de *hacking* (Hutchings & Chua, 2016; Gerstenfeld, 2023). Ainda, as mulheres *hackers* são vistas com baixa consideração e observa-se uma falta de apoio pela comunidade *hacker* (Chantler, 1995; Taylor, 1999; Hutchings & Chua, 2016), algo que também pode influenciar este *gender-gap*. Verificou-se, ainda, que indivíduos do sexo masculino têm uma probabilidade duas vezes maior de praticar *hacking*, resultado similar aos estudos de Fox

& Holt (2021) (OR=3.01) e de Udris (2016) (OR variou entre 2.70 e 3.21). A relação positiva com a área informática foi também confirmada, revelando-se o fator mais explicativo da prática de *hacking* (OR=4.6). Steinmetz (2016) e HackerOne (2021) concluem que muitos dos participantes em conferências de *hacking* encontram-se empregados na área. Ainda, estudantes da área informática têm maior probabilidade de ter a motivação e habilidade para atividades de *hacking*, além de serem mais propensos a já as terem praticado (Hu *et al.*, 2013), uma tendência reconhecida na comunidade científica, que frequentemente estuda o *hacking* em amostras estudantis (e.g., Pinto, 2023; Gaia *et al.*, 2021) e de profissionais da área (e.g., Happe, 2023). A frequência de cursos em áreas tecnológicas permite, por um lado, a aquisição das competências necessárias e, por outro, oportunidades de emprego em empresas, como *programadores* (Grispos, 2019; Gerstenfeld, 2023), podendo isto estar refletido na percentagem acentuada de indivíduos *white hat* no estudo.

Para a variável idade, estimou-se que os *hackers* fossem mais novos do que não-*hackers*. Verificou-se que os resultados encontrados foram de encontro ao esperado, contudo, estes não se verificaram significativos para as comparações de médias. Isto não é um resultado completamente inesperado, visto que a literatura tem demonstrado idades variadas (Steinmetz, 2015; Turgeman-Goldschmidt, 2005), muitas vezes não se apresentando como fator significativo (e.g., Fox & Holt, 2021). Não obstante, revelou-se significativa no primeiro modelo explicativo, demonstrando uma maior probabilidade de prática de *hacking* consoante o decréscimo da idade, indo de encontro a estudos que demonstram que *hackers* tendem a ser mais novos do que não-*hackers* (Bachmann, 2010; Fox & Holt, 2021; HackerOne, 2020, 2021). Tal pode ser explicado por uma maior proficiência tecnológica, associada a indivíduos mais jovens (Gaia *et al.*, 2021), visto que facilita a aprendizagem e realização do tipo de comportamentos que integram o *hacking*.

No que concerne às habilitações, os resultados não foram significativos, podendo ter sido enviesados pela estratégia de amostragem, que incidiu em instituições de ensino superior. Igualmente, o setor de emprego parental não se revelou significativo, não se confirmando a hipótese. Esta foi uma hipótese de nível exploratório, havendo apenas um estudo de carácter qualitativo que aborda esta associação, sendo que o próprio autor (Steinmetz, 2016) concordou que a relação entre as ocupações parentais dos entrevistados e a prática de *hacking* não era perfeita.

Concluindo, face ao perfil sociodemográfico que se procurou estabelecer, confirmou-se o previsto quanto ao género, idade e relação com a área tecnológica.

Na vertente das variáveis individuais, primeiramente testou-se a hipótese (2), de que “*Indivíduos com menor autocontrole têm maior propensão para a prática de hacking, em comparação com indivíduos com maior autocontrole*”. Os resultados em análise levam à confirmação desta hipótese, constatando-se diferenças de médias com significância estatística, havendo superior BAC nos *hackers*¹¹. Kim *et al.* (2022), Fox & Holt (2021) e Udris (2016), que utilizaram a mesma forma de operacionalização da prática de *hacking*, chegaram às mesmas conclusões. Indivíduos com BAC são caracterizados como impulsivos, insensíveis, arriscados e atraídos por tarefas simples, sendo ainda incapazes de ver as consequências das suas ações (Gottfredson & Hirschi, 1990) devido às “*dimensões do autocontrole [que são] fatores que afetam o cálculo das consequências dos nossos atos. A pessoa impulsiva (...) não considera as consequências negativas ou dolorosas dos seus atos; a pessoa insensível tem menos consequências negativas a considerar*” (Gottfredson e Hirschi 1990, p. 95). Para os autores da TGC, o crime é atrativo pois fornece benefícios imediatos, levando à desconsideração de impactos a longo-termo. Marcum *et al.* (2014) aplicam o pressuposto anterior aos *hackers*, tomando-os como indivíduos que não conseguem antecipar a quebra de confiança ao praticar *hacking*, nem consideram a possibilidade de ser detetados ou de sofrer sanções. Isto é, ainda, facilitado pelo carácter anónimo do ciberespaço (Holt *et al.*, 2011), levando à perceção de uma baixa probabilidade de serem detetados e efetivamente punidos (Young *et al.*, 2007). A preferência por tarefas simples e físicas têm sido dimensões discutidas, uma vez que alguns autores apontam persistência e paciência como características de um *hacker* com sucesso (Holt, 2007; Steinmetz, 2015). Por exemplo, Holt e Kilger (2008) sugerem que indivíduos com BAC seriam demasiado impulsivos para dedicar tempo às tarefas mentais exigidas a um *hacker*. Fox & Holt (2021) relembram que, embora a prática de *hacking* possa começar devido a BAC, um estudo transversal, como o presente estudo, não permite determinar se os jovens alcançados são os que persistem no *hacking*, ou se são os que possuem um BAC que os impulsionará para a desistência, pois mede a prática de *hacking*, pontualmente, no último ano. Ademais, comportamentos mais simples requerem menos autocontrole para aprender, comparativamente a outros mais sofisticados (Holt, 2007; Steinmetz, 2015; Bossler & Burruss, 2011). É ainda possível que a população de *hackers* tenha um menor

¹¹ Nos modelos de predição o BAC não se destacou, demonstrando uma perda de capacidade explicativa do *hacking*, ao pesar outras variáveis.

autocontrolo face à população em geral, mas maior do que outros grupos (ciber)desviantes, sendo necessária mais investigação neste sentido.

A nível dos traços de personalidade do Modelo *Big five*, formulou-se para o teste de hipóteses que (3) “*Indivíduos com maiores níveis de (a) abertura à experiência e (b) neuroticismo e menores níveis de (c) extroversão, (d) agradabilidade e (e) conscienciosidade terão maior propensão para a prática de hacking*”. Esta hipótese foi parcialmente confirmada, apesar de algumas das diferenças encontradas não irem ao encontro à literatura existente, explanado de seguida. Importa referir que a literatura existente acerca deste tópico é limitada e inconsistente, sendo um tema exploratório e, desta forma, resultados diferenciados não são completamente inesperados.

No que toca à extroversão, esta revelou, contrariamente ao esperado, uma maior média em *hackers*, ainda que não se demonstre significativa. Alguns estudos (Rogers, 2006; Rogers, 2006a) têm colocado como hipótese a existência de menores níveis de extroversão em *hackers*, devido ao seu retrato por parte dos *media*. Contudo, Holt (2020) defende que, pese embora os *media* retratem os *hackers* como socialmente isolados, estes frequentemente aprendem através de uma rede de pares com interesses semelhantes, tanto *online* como *offline* (Bossler & Burruss 2011; Holt et al. 2009; Skinner & Fream, 1997), podendo isto explicar os resultados de extroversão encontrados. Seigfried-Spellar & Treadway (2014) encontraram, de igual forma ao presente estudo, evidências de maior (mas não significativa) extroversão em *hackers*, avançando com a possibilidade de, devido à globalização da tecnologia, a subcultura *hacker* poder estar a mudar para incluir indivíduos para além do estereótipo, especificamente a nível de extroversão.

Já o traço de abertura à experiência não revelou uma diferença de médias significativa, entre *hackers* e não-*hackers*, um resultado que vai, novamente, contra a hipótese inicialmente formulada, uma vez que seria congruente com a definição original de “*hacker*”, um indivíduo que procurava descobrir e dar usos diferentes e inovadores à tecnologia (Levy, 2010). No entanto, perante a evolução da tecnologia e diferentes usos dados pela população em geral, pode já não se tratar de um traço distintivo (Seigfried-Spellar & Treadway, 2014).

No que concerne à agradabilidade, este demonstrou-se significativa, na direção estimada, na comparação de médias entre *hackers* e não-*hackers*, resultado que vai de encontro aos estudos de Seigfried-Spellar *et al.* (2017) e Seigfried-Spellar e Treadway (2014). Autores como Woo *et al.* (2004) associam o antagonismo à noção de uso indevido da tecnologia, através de atividades cometidas tendo por base sentimentos negativos,

como raiva, vingança ou motivos de “*hacktivism*”. Assim, menor agradabilidade apresenta-se relacionada com comportamentos de *hacking* criminal. A agradabilidade associa-se, nomeadamente, a altruísmo e preocupação com outros (Costa & McCrae, 1992) encontrando-se, desta forma, também relacionada com o autocontrolo, que envolve dimensões como autocentração (Kranenbarg *et al.*, 2023). Uma baixa agradabilidade leva a maior egoísmo e agressividade, refletindo-se em comportamentos de *hacking* malicioso ou motivado por vingança (Schell & Holt, 2002).

O neuroticismo foi o único traço que se revelou significativo tanto a nível de comparação de médias como, posteriormente, no modelo final, variando na direção esperada. Os estudos têm apontado para maior neuroticismo em diferentes tipos de comportamentos no espectro de *hacking* (Seigfried-Spellar & Treadway, 2014). Por exemplo, Seigfried-Spellar *et al.*, (2017), medindo a estabilidade emocional (oposto de neuroticismo, que consiste numa tendência para a emocionalidade), concluem uma relação negativa entre estabilidade emocional e comportamentos relacionados com cibercrime. Ainda, Miller e Pilkonis (2006) retratam o neuroticismo como predisposição para estados afetivos negativos, tais como depressão, ansiedade e raiva, algo que vai de encontro ao estudo de Schell & Holt (2002), que identificaram nos *hackers* estados frequentes de depressão e ansiedade. A concentração e dedicação necessária para a prática *hacking* complexo pode atrair indivíduos que já possuem predisposição para maior neuroticismo ou, tratando-se de atividades que podem envolver uma elevada pressão, podem exacerbar as tendências neuróticas. Aliado à elevada pressão, o estilo de vida de *hackers* retratado, por exemplo, pelos *media*, designadamente horários de sono disfuncionais e falta de atividade física (Rogers, 2006), bem como o envolvimento em atividades de risco, pode também justificar a associação a este traço.

Por fim, apesar de não significativo, não servindo para corroborar a hipótese formulada, os *hackers* revelaram maior conscienciosidade. Apesar de estudos empíricos (*e.g.*, Seigfried-Spellar *et al.*, 2017) revelarem menor conscienciosidade, algumas características, podendo contribuir para este achado contraditório. Happe (2023) conduziu entrevistas em *hackers*, descobrindo que, por um lado, *pen-testers* revelam preocupados com a qualidade do seu trabalho bem como uma necessidade de eficiência e gestão de tempo (Happe, 2023). Apesar de não ser algo diretamente relacionado com a conscienciosidade, vai de encontro à descrição do traço, por Costa e McCrae (1992).

De seguida, foi colocado como hipótese que (4) “quanto aos traços da Dark Triad, face aos não-hackers, os hackers apresentam maiores níveis em todos os traços”. Esta hipótese foi confirmada parcialmente, para a psicopatia e maquiavelismo.

Referente à psicopatia, esta tem sido elencada como um fator preditivo de cibercrime em geral e, especificamente, de *hacking* (e.g., Seigfried-Spellar *et al.*, 2017). Este é um preditor da criminalidade comum e parece ser transversal a ciberoofensores. As características a este traço associadas, designadamente, comportamento impulsivo, desrespeito pelos direitos e pela privacidade dos outros e a falta de empatia podem contribuir para que o cibercrime seja visto como uma alternativa válida para atingir os seus objetivos. Salienta-se, ainda, o papel importante das seguintes características do ciberespaço que favorecem a prática de infrações: anonimato, ausência de sinais não verbais, assincronia e pouca clareza das normas (Selzer & Oelrich, 2021). Vários estudos mostram que estas características facilitam a expressão de características psicopáticas, como menor empatia, falta de remorsos, desrespeito pelas normas éticas e legais (Wright *et al.*, 2019) e pouco controlo de impulsos (Davis *et al.*, 2002). Ainda, podem ter o efeito de “distanciamento psicológico”, levando a que percebam outros utilizadores da *Internet* como seres abstratos (Trobe & Liberman, 2010). Este efeito parece também refletir outras características psicopáticas, como a reduzida capacidade de empatia e de adotar o ponto de vista de outras pessoas, potenciando o uso de manipulação e exploração dessas mesmas pessoas para os seus próprios fins. Indivíduos que exibem traços mais elevados de psicopatia, demonstram também maior impulsividade e têm maior tendência para procura de sensações (Djubina, 2024), estando assim a psicopatia muito associada ao baixo autocontrolo (Seigfried-Spellar & Treadwy, 2017). Desta forma, a existência de maiores níveis de psicopatia em *hackers*, demonstrada pelas diferenças significativas de médias, já era esperada, uma vez que também o baixo autocontrolo flutuou na mesma direção.

Quanto ao maquiavelismo¹², esta dimensão tem sido demonstrada como positivamente relacionada com o *hacking*. Jones e Paulhus (2014) associam-no a características como racionalidade, perspicácia, orientação para objetivos e planeamento estratégico, características já em si valorizadas pela subcultura *hacker* e que podem auxiliar na prática de *hacking*, nomeadamente, na manipulação de outras pessoas ou redes (Selzer & Oelrich, 2021), podendo assim ser utilizado para obtenção de informação sobre potenciais vítimas, designadamente através de um processo de *social engineering*, cada

¹² No presente estudo revelou um OR de aproximadamente 2, tanto no modelo preditivo com as variáveis individuais quanto no modelo preditivo final.

vez mais utilizado como forma de *hacking*. Ainda, indivíduos maquiavélicos demonstram uma postura ética flexível (Jonason *et al.*, 2015), o que vai ao encontro ao carácter ambíguo de muitos *hackers* (Zhang *et al.*, 2011), que muitas vezes operam numa área cinzenta e fazem uso de racionalizações para justificar as suas ações (Turgemann-Goldschmidt, 2005). Ademais, esta flexibilidade moral é ainda demonstrada na mentalidade de vários *hackers*, em que frequentemente os fins justificam os meios (Chiffelle & Loi, 2020), levando à desconsideração de fatores como a legalidade e moralidade.

Finalmente, o narcisismo não se revelou significativo. Selzer e Oelrich (2021) apresentam como possível explicação o facto de o cibercrime e o *hacking* poderem não proporcionar a mesma valorização e validação que as formas tradicionais de crime. No entanto, isto pode ser diferente para diferentes formas de crime ciberdependente, por exemplo, *hacking* que envolve atenção ou um reconhecimento por parte das vítimas (*e.g.*, *hacktivismo*), que não foi diretamente medido neste estudo, poderia levar a resultados diferentes. Assim, podem existir cibercrimes menos atrativos para indivíduos mais narcisistas, uma vez que a atenção (da vítima ou público), pode não ser manifesta. Uma vez que Holt *et al.* (2011) apontam o anonimato oferecido pela *Internet* como possível motivo de atração da ciberdesviância, esta pode ser, igualmente, uma possível explicação para o resultado encontrado.

b) Diferenças entre *hackers black hat*, *grey hat* e *white hat*

Ao nível de diferenças sociodemográficas, foi colocada a hipótese (5) de que “Existem diferenças a nível das características sociodemográficas entre *hackers black hat*, *grey hat* e *white hat*”. Verificou-se que quanto ao género e habilitações não foram encontradas quaisquer diferenças significativas. Em relação à idade, esta revelou diferenças significativas, no sentido em que *hackers black hat* revelaram uma *mean rank* mais elevada, enquanto *hackers white hat* revelaram uma *mean rank* mais reduzida. Este resultado vai contra as conclusões de estudos anteriores (*e.g.*, Holt & Kilger, 2008, Nodeland & Morris, 2018; Djubina, 2024) que afirmam também que indivíduos mais jovens, passam mais tempo a utilizar tecnologias e constituem também, tradicionalmente, a população mais propensa ao crime. Este resultado inesperado pode, contudo, dever-se ao aumento de oportunidades a *hackers white hat*, sendo que a indústria da cibersegurança tem tido um crescimento acentuado nos últimos anos, havendo um maior reconhecimento do valor de *hackers* éticos, oferecendo oportunidades de educação formal e carreira

legítimas e bem pagas (Bachmann & Corzine, 2010; Tanczer, 2019), atraindo jovens saídos de cursos da área informática para o *hacking white hat*. Outras atividades que atraem jovens informáticos (e.g., *hackathons* e *bug bounty programs*) também podem ser responsáveis por encorajar o desenvolvimento de competências no ambiente ético e para propósitos legais. Quanto ao nível de estudo/emprego no setor informático, verificou-se significância, em que *hackers white hat* e *grey hat* demonstraram uma grande percentagem neste setor contrariamente aos *hackers black hat*. Este dado vai contra os resultados do estudo de Pinto (2023) que observou que os *hackers* maliciosos (*hackers black hat*) têm tendência a maior presença nas áreas TIC. Não obstante, dada a entrada cada vez mais crescente de *hackers white hat* em empresas, em função de *programadores* e *pen-testers*, não é surpreendente. Quanto à empregabilidade dos pais no setor informático, apesar de não ser significativo, estabeleceu-se no limite da significância, sendo bastante superior no caso dos *black hat* e verificando-se nos *white hat* uma menor propensão para ter pelo menos um pai empregado neste setor. Apesar de nenhum estudo, do nosso melhor conhecimento, abordar esta hipótese, alguns têm demonstrado uma associação entre *hacking* criminoso ou desviante (e.g., Marcum *et al.*, 2014) e um contacto mais precoce com a tecnologia, ao passo que Steinmetz (2016) justificou a ligação entre ocupação parental no setor informático e a prática de *hacking* através de fatores como apoio parental e aceitação das atividades. Assim, uma possível explicação poderia unir ambas as anteriores, em que a ligação dos pais a atividades tecnológicas possibilita um contacto mais precoce com a tecnologia, que por sua vez pode levar a maior propensão de *hacking* criminoso ou desviante.

De seguida, confirmou-se que (6) “*Os níveis de autocontrolo são menores em hackers black hat e maiores em hackers white hat*”. Tal como discutido anteriormente e revisitando a TGC de Gottfredson & Hirschi (1990), esta é uma teoria explicativa do crime, que associa o BAC à prática de crime sendo, assim, coerente, que o grupo de *hackers* criminoso, os *black hat*, teria níveis mais reduzidos de autocontrolo, ao passo que o grupo menos criminoso e caracterizado pela conformidade com a lei, os *white hat*, teriam os níveis mais elevados, entre os três grupos analisados. Este resultado vai ao encontro do estudo de Pinto (2023), em que *hackers* maliciosos revelaram, igualmente, níveis mais baixos de autocontrolo, comparativamente à amostra que integrou os *hackers* não-maliciosos. Holt & Kilger (2008) defendem que diferentes níveis de autocontrolo podem levar à prática de diferentes tipos de *hacking*, nomeadamente, um baixo nível de autocontrolo pode levar os indivíduos a não ter em conta os fatores legais associados aos

seus comportamentos, algo congruente com *hackers black hat*, explicando os seus níveis mais reduzidos de autocontrolo. No estudo de Silic e Lowry (2019)¹³, vários *hackers* não reconheciam os seus atos digitais como tão importantes como crimes físicos, recorrendo a técnicas de negação do dano (Sykes & Matza, 1957), iludindo-se, assim, na questão de que os riscos de apreensão também seriam diminutos (Silic e Lowry, 2019). Contrariamente, *hackers* com níveis mais elevados de autocontrolo podem, por sua vez, ter a paciência necessária para desenvolver uma compreensão mais abrangente da tecnologia, da ética e das ramificações das suas ações (Holt & Kilger, 2008), acabando a situar-se na legalidade do *hacking*, tal como os *white hat*. Por esta lógica, um nível intermédio entre ambos de autocontrolo verifica-se nos *grey hat* que, de acordo com a literatura, se situa entre ambos no espectro da legalidade e da ética (Chiffelle & Loi, 2020). Por fim, compatível com a conclusão de um menor autocontrolo em *hackers black hat*, Gaia et al. (2021) identificam uma relação positiva entre procura de risco (uma das componentes do autocontrolo, identificada pela TGC) e *hacking black hat*, associação não encontrada para os restantes tipos de *hackers*.

No que respeita à personalidade, verificaram-se diferenças significativas em ambos os modelos. Primeiramente, a hipótese 7 postula que “*Existem diferenças significativas entre os traços Big Five e o tipo de hacking praticado*”. No presente estudo, estas identificaram-se para com os traços de abertura à experiência e agradabilidade, tendo as diferenças ocorrido nas direções esperadas. Isto é, face ao traço de abertura à experiência, esperava-se que este fosse mais prevalente nos *hackers black hat*, uma vez que teriam predisposição para novas ideias que se manifestam de forma negativa e estariam mais abertos a explorar o lado ilegal do *hacking* (Matulessy & Humaira, 2016). Já no caso dos *white hat* verifica-se uma menor *mean rank* deste traço, possivelmente explicada por serem mais conformistas. Já para a agradabilidade, verifica-se o oposto, com a *mean rank* mais elevada por parte dos *white hat* e a mais reduzida por parte dos *black hat*. Os *white hat* caracterizam-se por serem altruístas e agirem de acordo com princípios éticos, tendo como propósito proteger os sistemas e resolver vulnerabilidades (Moore, 2015), estando o seu altruísmo alinhado com o traço de agradabilidade (Costa & McCrae, 1992). Já os *black hat* caracterizam-se pela prática de *hacking* com motivos maliciosos ou de beneficiação pessoal (Moore, 2015), contrariamente ao traço de

¹³ Os autores conduziram entrevistas com *hackers* criminosos procurando compreender como lidam com o possível stress de praticar este tipo de comportamentos.

agradabilidade (Costa & McCrae, 1992). Quanto aos restantes traços, não foram reveladas diferenças significativas.

Quanto à hipótese 8, foi testado se “*Existem diferenças significativas entre os traços Dark Triad e o tipo de hacking praticado*”, sendo esta confirmada a nível do traço maquiavelismo e narcisismo. Quanto ao traço do maquiavelismo, verificaram-se na direção esperada, isto é, o traço revelou uma *mean rank* superior em *hackers black hat* e menor em *white hat*, tal como previamente demonstrado pelo estudo de Gaia et al. (2021). Como mencionado anteriormente, o maquiavelismo está altamente relacionado com o uso de comportamentos manipuladores e de decepção para alcançar objetivos pessoais, bem como a uma atitude de desprezo pelas consequências negativas que recaem sobre os outros perante estas ações (Scilhavy & King, 2009). Este tem sido um traço também estudado a nível de profissionais de IT e, designadamente, Scilhavy e King (2009) testam a sua relação com comportamentos éticos e morais, concluindo a existência de uma relação negativa ($\beta = -0.27$), ressaltando ainda para o facto de que os efeitos do maquiavelismo incrementam em cenários com dilemas morais significativos, algo mais provável em *hackers black hat*, mas também *grey hat*, que realizam, por vezes, comportamentos ilegais e/ou imorais.

No que concerne ao narcisismo, verificou-se que a *mean rank* é superior em *hackers grey hat* e inferior em *hackers black hat*, de forma significativa. Este é um efeito inesperado, uma vez que Gaia et al. (2021) concluem no seu estudo que o narcisismo está relacionado apenas com o tipo de *hacking white hat*, no entanto, verifica-se que a *mean rank* dos *hackers white hat* é similar à dos *hackers grey hat*. Várias explicações podem ser apontadas para este achado. Em primeiro lugar, estando os *black hat* associados a comportamentos criminosos, estes tendem a aproveitar-se do anonimato possibilitado pelo uso de tecnologias, sendo esperado que tivessem menores níveis de narcisismo, querendo, em princípio, evitar as atenções da população em geral (Selzer & Oelrich, 2021), uma vez que poderia conduzir à sua deteção. Por sua vez, para explicar os resultados encontrados a nível dos *hackers white hat* e dos *grey hat* surgem diferentes explicações. Seebruck (2015) defende que os *hackers white hat* praticam os seus comportamentos por um desejo de prestígio, estando este relacionado com o narcisismo, nomeadamente, fazendo parte de um item da escala *Dirty Dozen*, utilizada para mensurar este traço. O autor associa as atividades dos *hackers* bons ao desejo de notoriedade e reconhecimento. Desta feita, o narcisismo pode estar a potenciar várias das suas ações, nomeadamente podendo ser uma explicação para o envolvimento frequente dos *hackers*

white hat em competições, como *bug bounty programs*, que conferem reconhecimento aos vencedores (Votipka *et al.*, 2018). O relatório da *HackerOne* (2021) demonstra também que os *hackers* procuram avançar na sua carreira informática e, sendo uma área extremamente competitiva, o desejo de atenção e de expor os seus feitos seria algo inerente. Por fim, os resultados elevados na *mean rank* dos *hackers grey hat* podem dever-se à prática de determinados comportamentos relacionados com *hacktivismo* (Gaia *et al.*, 2021) que exigem atenção pública ou, de acordo com a definição de *grey hat*, devido ao comportamento de interpelar a proprietários de sistemas, procurando a sua atenção para que resolvam os problemas para os quais alertaram (Kirsch, 2014; Franklin *et al.*, 2019).

Quanto à psicopatia não foram encontradas diferenças significativas, mas verificou-se uma *mean rank* superior para *hackers black hat*, congruente com os resultados já discutidos acerca de um menor autocontrolo nestes, tendo inclinações impulsivas e de propensão para o risco e para a procura de sensação (Gaia *et al.*, 2021; Taylor *et al.*, 2014), altamente relacionado com o traço psicopático.

Por fim, quanto à hipótese final (9), foi postulado que “*Existem diferenças a nível das motivações entre hackers black hat, grey hat e white hat*”. Esta hipótese foi confirmada, concluindo-se diferenças ao nível da “procura de sensação”, “proteger e defender” e “fazer o bem/ajudar os outros”. No caso da procura de sensação, a *mean rank* foi mais elevada, com significância estatística, nos *hackers black hat*. Este achado é congruente com estudos anteriores, que afirmam uma procura de excitação e adrenalina (Gordon, 1994), por parte destes indivíduos, indo também de encontro aos resultados encontrados no que toca aos valores do BAC nestes. A literatura afirma que os *hackers* são indivíduos que procuram emoções, que obtêm prazer e excitação da sua atividade, da superação de barreiras e do acesso a outros sistemas (Levy, 1984; Yar, 2005). Esta característica aplica-se particularmente aos *hackers black hat*, pessoas que não subscrevem a qualquer ética de *hacker* (Levy, 1984), mas que usam as suas capacidades para entrar em sistemas sem o consentimento do proprietário. Envolvem-se em atividades ilícitas, o que introduz maiores riscos, potenciando a excitação e a obtenção da sensação que desejam (Bachmann, 2010). Por fim, quanto às motivações “proteger e defender” e “fazer o bem/ajudar os outros”, estas variaram também no sentido previsto, demonstrando uma *mean rank* superior nos *hackers white hat*. No relatório da *HackerOne* (2020), estas são motivações frequentemente elencadas, que vão de encontro à visão alargada do que é um *hacker white hat*, sendo alguém cujo propósito é proteger redes e sistemas e ajudarem

outros, ao descobrirem vulnerabilidades e alertarem para estas de forma ética e legal (Moore, 2015; Kumar, 2018; Chang & Whitehead, 2022).

6. Limitações e Linhas de Investigação Futuras

O *hacking* ganha cada vez mais relevância na atualidade, sendo que os custos a este associados (tanto económicos como sociais) têm aumentado exponencialmente nos últimos anos (Chang & Whitehead, 2022), justificando a pertinência de estudos como este. A análise das variáveis individuais de *hackers* tem sido escassamente realizada. Concretamente, em contexto português, existe apenas um estudo (Pinto, 2023) que segue uma linha de investigação similar. O presente estudo realça a importância de reconhecer as diferenças individuais na compreensão do fenómeno, focando-se em alguns pontos ainda não considerados no contexto português e pouco estudados a nível internacional, designadamente, a questão da personalidade e da diferenciação entre três tipos de *hackers*. Ademais, procurou-se ainda formular uma escala que pudesse medir os comportamentos associados aos diferentes tipos de *hacking*, uma vez que esta não existe ainda na literatura. Assim, considera-se uma investigação inovadora, no sentido em que procura uma nova abordagem para um objeto de estudo ainda pouco aprofundado. Ao compreender a interação dos fatores estudados com o comportamento dos *hackers*, através de uma perspetiva criminológica, os resultados alcançados contribuem para preencher lacunas críticas na literatura, no que diz respeito aos *hackers* e ao seu *modus operandi*. Além disso, delinear as distinções entre os tipos de *hackers* permite uma maior compreensão das diferentes formas de manifestação do *hacking*, e serve também para informar a prevenção e as intervenções que visam a cibersegurança e a ética digital.

Não obstante, o estudo realizado não se encontra imune a algumas limitações. Primeiramente, será de notar o facto de se basear numa amostra selecionada por conveniência, não probabilística, o que limita a generalização dos resultados obtidos para a população-alvo. Em investigações futuras, deverá procurar obter-se uma amostra recorrendo a amostragem probabilística, visando a potenciação da generalização dos resultados. Ainda em relação à amostra utilizada, outras limitações podem ser apontadas, nomeadamente por ser composta por (1) uma grande percentagem de estudantes universitários, podendo a taxa de resposta ser baixa; (2) *hackers*, uma população de difícil colaboração, devido à natureza dos comportamentos questionados (legalmente tipificados como crime) e acesso, devido ao seu anonimato; e (3) trabalhadores de empresas tecnológicas, podendo os resultados obtidos junto destes conter enviesamento (Dodou &

Winter, 2014), devido a desejabilidade social. Foram utilizados alguns métodos que ajudam a reduzir o enviesamento por desejabilidade social, como o uso de itens de escolha forçada e o facto de ser um questionário autoadministrado (Nederhof, 1985), contudo, estes podem apenas atenuar o efeito. Quanto à metodologia utilizada, este estudo assenta numa metodologia quantitativa, contudo, outros métodos de recolha de dados poderiam permitir uma análise mais aprofundada, nomeadamente complementando, por exemplo, com a aplicação de entrevistas. Isto é particularmente relevante para as questões referentes aos comportamentos dos *hackers*, uma vez que há críticas apontadas à classificação utilizada neste estudo, pois o comportamento não é algo óbvio, o que é “grey” para uma pessoa pode ser “black” para outra (Fitch, 2004), sendo que as entrevistas ajudariam a aprofundar este tópico. Uma tentativa de colmatar isto foi a construção de uma escala comportamental para o *hacking*, contudo, optou-se por se utilizar a medida de autoperceção para classificação dos *hackers*, podendo ser benéfico, em futuras investigações, o uso de ambas, bem como uma comparação entre os resultados obtidos através de cada uma, para averiguar a coerência entre a autoperceção do tipo de *hacking* praticado e os comportamentos efetivamente adotados. Por fim, o questionário final é bastante longo, o que se consubstanciou como uma limitação para o presente estudo, causando uma grande taxa de desistência, pelo que seria benéfico ser abreviado.

Elencam-se, agora, algumas sugestões para investigações futuras. Primeiramente, seria relevante analisar o papel de cada uma das dimensões individuais do autocontrolo na prática de *hacking* para aprofundar as críticas relacionadas com as dimensões de preferência por tarefas simples e físicas (e.g., Holt, 2007). Ademais, semelhante ao estudo de Pinto (2023), seria interessante abordar a mediação entre o BAC, a personalidade e a prática de *hacking*, ainda não analisada. Algumas relações encontradas neste estudo poderiam ser também aprofundadas através de um estudo longitudinal que averigue as variáveis individuais e mudanças nestas de acordo com a prática de *hacking*. Por fim, verificou-se que as variáveis em estudo explicam, no seu conjunto, cerca de 29% da prática de *hacking*, sendo necessário explorar outros aspetos que possam contribuir para uma explicação mais completa, tais como fatores de índole social ou contextual.

Referências Bibliográficas

Abeoussi, J. M. D. (2019). *Black Hat and White Hat Hacking - The thin line of ethics*. EC-Council University.

American Psychiatric Association. (2013). *Diagnostic and statistical manual of mental disorders* (5th ed.).

- Bachmann, M. (2008). *What makes them Click? Applying the Rational Choice Perspective to the Hacking Underground*. University of Central Florida.
- Bachmann, M. (2010). The Risk Propensity Computer Hackers and Rationality. *International Journal of Cyber Criminology*, 4(1), 643-656.
- Bachmann, M. & Corzine, J. (2010). Insights into the Hacking Underground. In T. Finnie, T. Petee, & J. Jarvis (Eds.), *Future Challenges of Cybercrime*. Volume 5: Proceedings of the Futures Working Group (pp. 65-75).
- Back, S., Soor, S., & LaPrade, J. (2018). Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory. *The International Journal of Cybersecurity Intelligence and Cybercrime*, 1(1), 40–55.
- Barber, R. (2001). Hackers Profiled — Who Are They and What Are Their Motivations? *Computer Fraud and Security*, 2001(2), 14–17.
- Beltrán, H. (2022). “Hacking, Computing Expertise, and Difference.” Just Tech. Social Science Research Council.
- Bossler, A. M., & Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers? In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 38-67). Rutland, VT: IGI Global.
- Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38, 227-236.
- Brooks, T. (2022). The Professionalization of the Hacker Industry. *International Journal of Computer Science and Information Technology*, 14(03), 87–99.
- Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press on Demand.
- Chang, L. Y. C., & Whitehead, J. (2022). What the Hack: Reconsidering Responses to Hacking. *Asian Journal of Criminology*, 17, 113-126.
- Chantler, A. N. (1995) ‘Risk: The profile of the computer hacker’, unpublished thesis, Curtin University.
- Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, 5, 100167.
- Chowdappa, K. B., Lakshmi, S. S. & Kumar, P.N.V.S. P. (2014). Ethical Hacking Techniques with Penetration Testing. *International Journal of Computer Science and Information Technologies*, 5(3), 3389-3393.
- Chua, Y., & Holt, T. J. (2016). A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors. *Victims & Offenders*, 11(4), 534-555.
- Clark, L. A., & Watson, D. (1999). Temperament: A new paradigm for trait psychology. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (pp. 399–423). New York: Guilford Press
- Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, 8(3), 255–277.
- Costa, P. T., & McCrae, R. R. (1992). The five-factor model of personality and its relevance to personality disorders. *Journal of Personality Disorders*, 6(4), 343–359.

Crossler, R. E., Johnston, A. C, Lowry, PB, Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Comput Secur*, 32, 90–101.

Cybersecurity Ventures. (2020). Cybercrime to cost the world \$10.5 trillion annually by 2025. *Cybercrime Magazine*. Retrieved from <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>.

DataReportal. (2024). <https://datareportal.com/reports/digital-2024-global-overview-report>

Delisi, M., Hochstetler, A., & Murphy, D. S. (2003). Self-control behind bars: A validation study of the Grasmick et al. scale. *Justice Quarterly*, 20(2), 241–263.

Djubina, J. (2024). The Genesis of the Criminal's Personality in the Digital Age. *Proceedings of the International Scientific and Practical Conference*, 4, 79–82.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. (5th Ed.) Sage edge: London.

Fitch, C. (2004). *Crime and Punishment: The Psychology of Hacking in the New Millennium*, Bethesda, MD.: *SANS Institute*, 1, 1-17.

Fox, B., & Holt, T. J. (2021). Use of a Multitheoretic Model to Understand and Classify Juvenile Computer Hacking Behavior. *Criminal Justice and Behavior*, 48(7), 943–963.

Föttinger, Christian and Wolfgang Ziegler. (1993). “Understanding a Hacker’s Mind: A Psychological Insight into the Hijacking of Identities.” RSA Security. Retrieved from <http://www.donau-uni.ac.at/de/departament/gpa/Informatik/DanubeUniversityHackersStudy.pdf>.

Franklin P, Adams R, Henry C. (2019). What the hack is a hacker?

Freire, T. & Almeida, L. (2008). *Metodologia de Investigação em Psicologia e Educação*. Lisboa: Psiquilibrios.

Furnell, S. M. (2001). Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare*, 1(2), 35-44.

Furnell, S. (2002). Cybercrime: Vandalizing the Information Society. *Proceedings of the 2003 International Conference on Web Engineering*.

Gaia, J., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. W. (2021). Dark Traits and Hacking Potential. *Journal of Organizational Psychology*, 21(3), 23-46.

Gordon, S. (1994). The generic virus writer. *Proceedings of the International Virus Bulletin Conference*. Jersey, Channel Islands, pp.121-138.

Gerstenfeld, J. (2023). Understanding the Connection Between Hackers and Their Hacks: Analyzing USDOJ Reports for Hacker Profiles. *International Journal of Cybersecurity Intelligence & Cybercrime*, 6(1), 59–76.

Gordon, S. (2001). Virus Writers: The end of the Innocence? *IBM*, 1-20.

Goerzen, M., & Matthews, J. (2019). Black hat trolling, white hat trolling, and hacking the attention landscape. In *Proceedings of the world wide web conference (WWW ‘19)* (pp.523–528). Association for Computing Machinery.

Goode, S., & Cruise, S. (2006). What Motivates Software Crackers? *Journal of Business Ethics*, 65(2), 173–201.

Grasmick, H. G., Tittle, C. R., Bursik Jr, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, 30(1), 5-29.

Grispos, G. (2019). Criminals: Cybercriminals. *Encyclopedia of Security and Emergency Management*, 1–7.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford University Press.

HackerOne. (2020). *The 2020 Hacker Report*. Available at: <https://www.hackerone.com/resources/reporting/the-2020-hacker-report>

HackerOne. (2021). *The 2021 Hacker Report*. Available at: <https://www.hackerone.com/resources/reporting/the-2021-hacker-report>

Hollinger, R. C., & Lanza-Kaduce, L. O. N. N. (1988). The process of criminalization: The case of computer crime laws. *Criminology*, 26(1), 101–126.

Hollinger, R. (1988). Computer hackers follow a Guttman-Like Progression. *Phrack Inc.*, 2(22).

Holt, T. J. (2007). Subcultural Evolution? Examining the Influence of On and Offline Experiences on Deviant Subcultures. *Deviant Behavior*, 28, 171-198.

Holt, T. J. (2020). Computer Hacking and the Hacker Subculture. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 725–742). Palgrave Macmillan.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. *Journal of Crime and Justice*, 33(2), 31–6.

Holt, T. J., Bossler, A. M., & May, D. (2011). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice*, 37(3), 1-18.

Holt, T. J., & Kilger, M. (2008). Techcrafters and makers: A comparison of two populations of hackers. *Proceedings of the IEEE: WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, 67-78.

Holt, T. J., Navarro, J. N., & Clevenger, S. (2020). Exploring the moderating role of gender in juvenile hacking behaviors. *Crime & Delinquency*, 66(11), 1533-1555.

Holt, T. J., & Steinmetz, K. F. (2021). Examining the Role of Power-Control Theory and Self-Control to Account for Computer Hacking. *Crime & Delinquency*, 67(10), 1491-1512.

Hutchings, A., & Chua, Y. T. (2016). Gendering cybercrime. In T. J. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 167–188). London: Routledge.

Jabłońska, M. R., & Zajdel, R. (2020). The *Dark triad* Traits and Problematic Internet Use: Their Structure and Relations. *Polish Sociological Review*, 4, 477–496.

Jaquet-Chiffelle, D. O., Loi, M. (2020): Ethical and unethical *hacking*. In: Christen, M., Gordijn, B., Loi, M. (eds.) *The Ethics of Cybersecurity*. pp. 179–204. Springer: Cham.

Jonason, P. K., & Webster, G. D. (2010). The dirty dozen: A concise measure of the dark triad. *Psychological Assessment*, 22(2), 420–432.

- Jonason, P. K., Strosser, G. L., Kroll, C. H., Duineveld, J. J., & Baruffi, S. A. (2015). Valuing myself over others: The Dark triad traits and moral and social values. *Personality and Individual Differences*, 81, 102–106.
- Jones, D. N., & Paulhus, D. L. (2014). Introducing the Short Dark triad (SD3): A brief measure of dark personality traits. *Assessment*, 21(1), 28–41.
- Jones, D. N., Padilla, E., Curtis, S. R., & Kiekintveld, C. (2021). Network discovery and scanning strategies and the Dark Triad. *Computers in Human Behavior*, 122, 1-10.
- Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, 46(4), 757–780.
- Karim, N. S. A., Zamzuri, N. H. A., & Nor, Y. M. (2009). Exploring the relationship between Internet ethics in university students and the big five model of personality. *Computers & Education*, 53(1), 86–93.
- Kim, J., Leban, L., & Lee, Y. (2022). Theoretical Explanations of the Development of Youth Hacking. *Crime & Delinquency*, 1-22.
- Kirsch, C. (2014). The *Grey Hat Hacker*: Reconciling cyberspace reality and the law. *Northern Kentucky Law Review*, 41(3), pp. 383-403.
- Koops, B. J. (2011). The Internet and its Opportunities for Cybercrime. SSRN Electronic Journal.
- Landreth, B., & Rheingold, H. (1985). *Out of the inner circle: a hacker's guide to computer security*. Microsoft Press.
- Levy, S. (2010). *Hackers: Heroes of the computer revolution*. Farnham: O'Reilly
- Loch, K. D., & Conger, S. (1996). Evaluating Ethical Decision Making and Computer Use. *Commun. ACM*, 39(7), 74–83.
- Lopes, B., & Yu, H. (2017). Who do you troll and Why: An investigation into the relationship between the *Dark triad* Personalities and online trolling behaviours towards popular and less popular Facebook profiles. *Computers in Human Behavior*, 77, 69–76.
- Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory Of Motivational Types Of Values In A Sample Of Hackers. *International Journal of Cyber Criminology*, 11(1), 78-97.
- Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in High School: Cybercrime Perpetration by Juveniles. *Deviant Behavior*, 35(7), 581–591.
- Marôco, J. (2007). *Análise estatística com SPSS Statistic*. Lisboa: Edições Sílabo.
- Matta, H., Gupta, R., & Agarwal, S.K. (2020). Search Engine optimization in Digital Marketing: Present Scenario and Future Scope. *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, 530-534.
- Matulessy, A., & Humaira, N. H. (2016). Hacker Personality Profiles Reviewed in Terms of the Big five Personality Traits. *Psychology and Behavioral Sciences*, 5(6), 137-142.
- Maxfield, M. G., & Babbie, E. R. (2014). *Research methods for criminal justice and criminology*. Cengage Learning.
- McCrae, R. R. (1996). Social consequences of experiential openness. *Psychological Bulletin*, 120(3), 323–337.
- McGuire, M., & Dowling, S. (2013). “Cybercrime: A Review of the Evidence” *Research Report 75*. Home Office.

Meyers, C. A., Powers, S. S., & Faissol, D. M. (2009). Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. *Lawrence Livermore National Lab*, 1-22.

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice*, 38(4), 767-772.

Moore, R. (2015). *Cybercrime: Investigating high-technology computer crime*. Routledge.

Nederhof, A. J. (1985). Methods of coping with social desirability bias: A review. *European Journal of Social Psychology*, 15(3), 263–280.

Nodeland, B., & Morris, R. (2020). A test of social learning theory and self-control on cyber offending. *Deviant Behavior*, 41(1), 41–56.

Nye, J.S. (2010). *Cyber power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University.

Oliver, D., & Randolph, Adriane. B. (2022). Hacker Definitions in Information Systems Research. *Journal of Computer Information Systems*, 62(2), 397–409.

Pabian, S., De Backer, C. J. S., & Vandebosch, H. (2015). Dark triad personality traits and adolescent cyber-aggression. *Personality and Individual Differences*, 75, 41-46.

Paulhus, D. L., & Williams, K. M. (2002). The Dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, 36(6), 556–563.

Pechorro, P., DeLisi, M., Gonçalves, R. A., Braga, T., & Maroco, J. (2022). Dark Triad Personalities, Self-control, and Antisocial/Criminal Outcomes in Youth. *Journal of Forensic Psychology Research and Practice*, 22(5), 427–443.

Pechorro, P., Jonason, P. K., Raposo, V., & Maroco, J. (2021). Dirty dozen: A concise measure of dark triad traits among at-risk youths. *Current Psychology*, 40(7), 3522–3531.

Rand, D. L., Stein, J. A., & Rand, S. T. (1998). Reliability and Validity of a SelfcontrolMeasure: Rejoinder. *Criminology*, 36(1), 175–182.

RASI (2023). *Relatório de Segurança Interna – Ano 2023*. Available at: <https://www.portugal.gov.pt/pt/gc24/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2023>

Rogers, M. (1999). *Psychology of hackers: Steps toward a new taxonomy*. Retrieved from <http://www.infowar.com>.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, 3(2), 97–102.

Rogers, M., Smoak, N. D., & Liu, J. (2006). Self-reported Deviant Computer Behavior: A Big-5, Moral Choice, and Manipulative Exploitive Behavior Analysis. *Deviant Behavior*, 27(3), 245–268.

Rogers, M. K., Seigfried, K., and Tidke, K. (2006a) Self-Reported Computer Criminal Behavior: A Psychological Analysis. *Digital Investigation*, 3, 116-120.

Rogers, M. K. (2010). The psyche of cybercriminals: A psycho-social perspective. In S. Ghosh & E. Turrini (Eds.), *Cybercrimes: A multidisciplinary analysis* (pp. 217–235). Springer Berlin Heidelberg.

Schell, B., & Dodge, J. (2002). *The Hacking of America: Who's Doing It, Why, and How*. Westport, CT: Greenwood Publishing Group.

Schell, B. H., & Holt, T. J. (2010). A profile of the demographics, psychological predispositions, and social/behavioral patterns of computer *hacker* insiders and outsiders. In T. J. Holt & B. H. Schell (eds.) *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 144-168). Hershey, PA: IGI Global.

Scilhavy, R. A. M., & King, R. C. (2009). *The Virtuous and the Vicious: The Effects of Professionalism and Machiavellianism on Ethical IT Decision Making*.

Seebruck, R. (2015). A typology of *hackers*: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, 14, 36–45.

Seigfried-Spellar, K. C., & Treadway, K. N. (2014). Differentiating *Hackers*, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences. *Deviant Behavior*, 35(10), 782–803.24

Seigfried-Spellar, K. C., Villacís-Vukadinović, N., & Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice*, 51, 67–73.

Silic, M., & Lowry, P. B. (2021). Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes. *Information Systems Frontiers*, 23(2), 329–341.

Skinner, W. F., & Fream, A. M. (1997). A Social Learning Theory Analysis of Computer Crime Among College Students. *Journal of Research in Crime and Delinquency*, 34(4), 495-518.

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime*. New York University Press.

Straub, D., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems*, 13.

Summers, T. C. (2015). *How hackers think: A mixed method study of mental models and cognitive patterns of high-tech wizards*. Thesis.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, 22(6), 664-670.

Szpor, G., & Gryszczyńska, A. (2022). Hacking in the (cyber)space. *GIS Odyssey Journal*, 2(1), 141–152.

Tanczer, L. M. (2020). 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. *Contemporary Security Policy*, 41(1), 108–128.

Taylor, P. A. (1999). *Hackers: Crime and the digital sublime*. Routledge.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

Thomas, D. (2002). *Hacker culture*. U of Minnesota Press.

Thomas, D., & Loader, B. (2000). *Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge.

Turgeman-Goldschmidt, O. (2005). Hackers' Accounts: Hacking as a Social Entertainment. *Social Science Computer Review*, 23(1), 8–23.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, 2, 382-396.

Udris, R. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: A cross-national study. *International Journal of Cyber Criminology*, 10(2), 127– 146.

Votipka, D., Stevens, R., Redmiles, E.M., Hu, J., & Mazurek, M.L. (2018). Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes. *2018 IEEE Symposium on Security and Privacy (SP)*, 374-391.

Wall, D. S. (2001). *Cybercrime and the Internet*. Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity.

Woo, H. (2003). The Hacker Mentality: Exploring the Relationship Between Psychological Variables and Hacking Activities. [Tese de Doutorado, Graduate Faculty of The University of Georgia]

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, 56(4), 64–74.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A Survey on Ethical Hacking: Issues and Challenges

Yar, M. (2006). *Cybercrime and society*. London, Thousand Oaks, New Delhi: Sage Publications.

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cyber crimes. *Security and Communication Networks*, 5(4), 422–437.

ANEXOS

Anexo I: Questionário

Características Individuais associadas a Comportamentos Online

Existem 16 perguntas neste questionário.

Consentimento Informado

Este questionário procura a recolha de dados para a realização de uma tese no âmbito do Mestrado em Criminologia, pela Faculdade de Direito da Universidade do Porto. Os dados recolhidos destinam-se única e exclusivamente para **fins de investigação académica e científica** e serão **tratados e analisados de forma agregada**, tornando impossível a identificação de situações individuais nos seus resultados.

O **objetivo desta investigação** é estudar a relação entre características individuais e comportamentos efetuados online (e.g., hacking).

Para responder a este questionário tem de ter, pelo menos, **18 anos**.

A sua participação é livre e voluntária, podendo desistir a qualquer momento do questionário, sem quaisquer repercussões.

As respostas dadas serão **anónimas**, uma vez que nenhuma informação que possa identificá-lo será pedida ou recolhida em momento algum, e **confidenciais**, uma vez que os dados recolhidos serão utilizados apenas no âmbito deste estudo.

Não existem respostas certas, nem erradas, por isso, solicita-se a sua honestidade e espontaneidade na resposta, escolhendo a que melhor se adequa a si.

O preenchimento do questionário tem uma duração aproximada de **15 minutos**.

Agradecemos a sua colaboração e disponibilidade.

Em caso de dúvidas, contacte: up201809564@direito.up.pt

Declaro que tomei conhecimento dos objetivos do presente estudo e que consinto em participar no mesmo.

*

Por favor, selecione **apenas uma** das seguintes opções:

☐ Sim

☐ Não

Grupo I - Características Sociodemográficas

Por favor responda às seguintes questões:

Género *

Escolha uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

☐ Feminino

☐ Masculino

☐ Outro

Idade *

Neste campo apenas pode ser introduzido um valor inteiro.

Por favor, escreva aqui a sua resposta:

Que habilitações literárias possui (ano mais elevado de escolaridade completo)? *

Escolha uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ☐ 1º ciclo
- ☐ 2º ciclo
- ☐ 3º ciclo
- ☐ Ensino Secundário
- ☐ Licenciatura
- ☐ Mestrado
- ☐ Doutoramento

Atualmente, qual a sua situação profissional? *

Escolha uma das seguintes respostas

Se selecionar a opção 'Outro. Qual?', por favor especifique a sua escolha utilizando o respetivo campo de texto.

Por favor, selecione **apenas uma** das seguintes opções:

- ☐ Estudante
- ☐ Trabalhador/a
- ☐ Estudante-trabalhador/a
- ☐ Desempregado/a

☐ Outro

Qual das seguintes opções se encontra de momento a frequentar? *

Responda a esta pergunta apenas se as seguintes condições são verdadeiras:

A resposta for 'Estudante' ou 'Estudante-trabalhador/a' na pergunta ' [G01Q04]'
(Atualmente, qual a sua situação profissional?)

Escolha uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

☐ Licenciatura

☐ Mestrado

☐ Doutoramento

☐ Outro

Que ano escolar se encontra a frequentar? *

Responda a esta pergunta apenas se as seguintes condições são verdadeiras:

A resposta for 'Estudante' ou 'Estudante-trabalhador/a' na pergunta ' [G01Q04]'
(Atualmente, qual a sua situação profissional?)

Neste campo só é possível introduzir números.

Por favor, escreva aqui a sua resposta:

Atualmente estuda e/ou trabalha numa área relacionada com o setor informático/tecnológico? *

Responda a esta pergunta apenas se as seguintes condições são verdadeiras:

A resposta for 'Estudante' ou 'Trabalhador/a' ou 'Estudante-trabalhador/a' na pergunta '[G01Q04]' (Atualmente, qual a sua situação profissional?)

Por favor, selecione **apenas uma** das seguintes opções:

- ☐ Sim
- ☐ Não

Algun dos seus pais se encontra a trabalhar ou já trabalhou no setor informático/tecnológico? *

Escolha uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ☐ Nenhum
- ☐ A minha mãe
- ☐ O meu pai
- ☐ Ambos

Grupo II - Comportamentos Online

Responda à questão que se segue tendo em conta a seguinte definição de hacking:

Hacking é o uso de **tecnologia para ganhar acesso** a computadores e/ou dados **com ou sem a permissão** da pessoa proprietária.

Tendo por base a definição apresentada, indique se cometeu hacking nos últimos 12 meses. *

Por favor, selecione **apenas uma** das seguintes opções:

- ☐ Sim
- ☐ Não

Grupo II - Comportamentos Online

De entre as frases apresentadas, escolha aquela que melhor se adequa a si e às suas atividades. *

Responda a esta pergunta apenas se as seguintes condições são verdadeiras:

A resposta for 'Sim' na pergunta ' [G05Q08]' (Tendo por base a definição apresentada, indique se cometeu hacking nos últimos 12 meses.)

Escolha uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ☐ Ajo tanto ilegalmente como maliciosamente nas minhas atividades de hacking.
- ☐ Procuro descobrir vulnerabilidades, ainda que de forma não autorizada, sem objetivos maliciosos ou, apenas, para obter algum ganho financeiro.
- ☐ Nas minhas atividades de hacking atuo de forma autorizada com o propósito de proteger, isto é, identificar e/ou resolver problemas de segurança em sistemas e redes.

Indique o grau de frequência com que realizou, no último ano, cada uma das seguintes atividades. *

Responda a esta pergunta apenas se as seguintes condições são verdadeiras:

A resposta for 'Sim' na pergunta ' [G05Q08]' (Tendo por base a definição apresentada,

indique se cometeu hacking nos últimos 12 meses.)

Por favor, selecione a posição apropriada para cada elemento:

	Nunca	Algumas vezes	Muitas vezes	Sempre
Escrevi, usei ou distribuí malware ou partes de malware (e.g., cavalos de tróia, emails Phishing, vírus, worms, etc), por malícia ou ganhos pessoais.	☐	☐	☐	☐
Adicionei, apaguei, mudei, copiei ou imprimi alguma informação nos ficheiros de computador de outra pessoa sem o seu conhecimento ou permissão, por malícia ou ganhos pessoais.	☐	☐	☐	☐
Acedi ao computador, ficheiros, redes ou contas de alheios sem consentimento dos seus proprietários, por malícia ou ganhos pessoais.	☐	☐	☐	☐
Já procurei ou consegui roubar informação sensível, pessoal e dados de empresas, por malícia ou ganhos pessoais.	☐	☐	☐	☐

Procurei				
----------	--	--	--	--

vulnerabilidades para ganhar acesso a informação, para alterar ou distribuir, ou danificar um sistema ou rede, por malícia ou ganhos pessoais.	☐	☐	☐	☐
Acedi de forma autorizada pelo proprietário a sistemas ou redes, para identificar e/ou resolver vulnerabilidades.	☐	☐	☐	☐
Intevi no sentido de identificar, proteger e/ou combater indivíduos que acedem a sistemas informáticos, com objetivos maliciosos ou por ganhos pessoais.	☐	☐	☐	☐
Forneci programas de segurança para proteger os sistemas de serem ilegalmente e maliciosamente penetrados.	☐	☐	☐	☐
Realizei atividades em âmbito de emprego numa agência ou empresa, para testar e fortalecer as redes de segurança online.	☐	☐	☐	☐

Examinei software lançado, em procura de vulnerabilidades, para				
--	--	--	--	--

submeter a bug bounty programs (programas que oferecem recompensas a quem identificar vulnerabilidades e as divulgar ao fabricante).	☐	☐	☐	☐
Ofereci-me para resolver vulnerabilidades descobertas, em troca de valor monetário.	☐	☐	☐	☐
Divulguei vulnerabilidades de forma pública, de forma a forçar os proprietários do sistema a resolvê-las.	☐	☐	☐	☐
Participei em atividades de hacking tanto legítimas, como ilegítimas, dependendo do necessário para atingir os meus objetivos.	☐	☐	☐	☐
Procurei descobrir vulnerabilidades para as trazer à atenção do proprietário, mas, encontrando-as, é mais importante para mim notificar o público antes, do que o proprietário do sistema.	☐	☐	☐	☐

Não considero que tenha aderido a				
-----------------------------------	--	--	--	--

atividades maliciosas, mas também não me preocupei em seguir leis.	☐	☐	☐	☐
--	-----------------------	-----------------------	-----------------------	-----------------------

Grupo III - Motivações para Comportamentos Online

Tendo em conta as motivações apresentadas assinala, de 1 (nada importante) a 4 (muito importante), o grau de importância que atribui a cada uma, quando comete hacking.

*

Responda a esta pergunta apenas se as seguintes condições são verdadeiras:
A resposta for 'Sim' na pergunta ' [G05Q08]' (Tendo por base a definição apresentada, indique se cometeu hacking nos últimos 12 meses.)

Por favor, selecione a posição apropriada para cada elemento:

	Nada importante	Pouco importante	Algo importante	Muito importante
Aprendizagem	☐	☐	☐	☐
Desafio intelectual/curiosidade	☐	☐	☐	☐
Diversão e Lazer	☐	☐	☐	☐
Ideologia	☐	☐	☐	☐
Lucro	☐	☐	☐	☐
Prestígio/Estatuto	☐	☐	☐	☐

Procura de sensações	☐	☐	☐	☐
Provar que sou melhor do que os outros	☐	☐	☐	☐
Vingança	☐	☐	☐	☐
Proteger e Defender	☐	☐	☐	☐
Fazer o bem/ajudar os outros	☐	☐	☐	☐

Grupo IV - Características Individuais

Leia cuidadosamente cada uma das afirmações que se seguem e assinale, desde discordo totalmente a concordo totalmente, a resposta que melhor se adequa a si.

*

Por favor, selecione a posição apropriada para cada elemento:

	Discordo Totalmente	Discordo	Concordo	Concordo Totalmente
Muitas vezes faço coisas no calor do momento sem parar para pensar.	☐	☐	☐	☐
Não me esforço muito a preparar o futuro, nem penso muito nisso.	☐	☐	☐	☐
Costumo fazer aquilo que me dá prazer no				

momento, mesmo se isso prejudicar um objetivo futuro.	☐	☐	☐	☐
---	-----------------------	-----------------------	-----------------------	-----------------------

Estou mais preocupado com o que se passa comigo no presente do que com o que me possa acontecer no futuro.	☐	☐	☐	☐
Geralmente procuro evitar atividades que eu sei que serão difíceis.	☐	☐	☐	☐
Quando as coisas se complicam, costumo desistir e afastar-me.	☐	☐	☐	☐
Na vida, as coisas que são mais fáceis são aquelas que me dão mais prazer.	☐	☐	☐	☐
Não gosto de tarefas tão difíceis que levem as minhas capacidades até ao limite.	☐	☐	☐	☐
De vez em quando, gosto de me pôr à prova fazendo coisas um pouco arriscadas.	☐	☐	☐	☐
Por vezes corro riscos só pelo divertimento que dão.	☐	☐	☐	☐
Por vezes, acho excitante fazer coisas que me podem causar problemas.	☐	☐	☐	☐

Excitação e aventura são mais importantes para mim do que me sentir seguro/a.	☐	☐	☐	☐
Se eu pudesse escolher, preferia geralmente fazer atividades físicas do que atividades mentais.	☐	☐	☐	☐
Geralmente sinto-me melhor quando estou em movimento do que quando estou sentado/a e a pensar.	☐	☐	☐	☐
Gosto mais de sair e de fazer coisas do que de ler e pensar.	☐	☐	☐	☐
Eu sinto que tenho mais energia e mais necessidade de actividade do que a maioria das pessoas da minha idade.	☐	☐	☐	☐
Eu tento pensar primeiro em mim, mesmo se isso tornar as coisas mais difíceis para os outros.	☐	☐	☐	☐
Eu não sou muito compreensivo/a com as pessoas quando elas estão com problemas.	☐	☐	☐	☐
Se o que eu faço desagrada às outras pessoas, o problema é	☐	☐	☐	☐

delas e não meu.				
-------------------------	--	--	--	--

Procurarei atingir os meus objetivos mesmo que possa causar problemas aos outros.	☐	☐	☐	☐
"Perco a cabeça" com muita facilidade.	☐	☐	☐	☐
Muitas vezes, quando me zango com as pessoas, sinto que tenho mais vontade de as magoar do que de falar com elas sobre o assunto.	☐	☐	☐	☐
Quando estou mesmo zangado/a é melhor que as pessoas se afastem de mim.	☐	☐	☐	☐
Quando discordo seriamente de alguém, é geralmente difícil para mim falar calmamente sobre isso sem me aborrecer.	☐	☐	☐	☐

Grupo IV - Características Individuais

Leia cuidadosamente cada uma das afirmações que se seguem e assinale, desde discordo fortemente a concordo fortemente, a resposta que melhor se adequa a si.

*

	Discordo fortemente	Discordo	Nem concordo, nem discordo	Concordo	Concordo fortemente
Raramente estou triste ou deprimido(a).	☐	☐	☐	☐	☐
Sou uma pessoa alegre e bem-disposta.	☐	☐	☐	☐	☐
A poesia pouco ou nada me diz.	☐	☐	☐	☐	☐
Tendo a pensar o melhor acerca das pessoas.	☐	☐	☐	☐	☐
Sou eficiente e eficaz no meu trabalho.	☐	☐	☐	☐	☐
Sinto-me, muitas vezes, desamparado(a), desejando que alguém resolva os meus problemas por mim.	☐	☐	☐	☐	☐
Muitas vezes, sinto-me a rebentar de energia.	☐	☐	☐	☐	☐
Às vezes ao ler poesia e ao olhar para uma obra de arte sinto um arrepio ou uma onda de emoção.	☐	☐	☐	☐	☐
A minha primeira reação é confiar nas pessoas.	☐	☐	☐	☐	☐
Sou uma pessoa muito competente.	☐	☐	☐	☐	☐

Raramente me sinto só ou abatido(a).	☐	☐	☐	☐	☐
Sou uma pessoa muito ativa.	☐	☐	☐	☐	☐
Acho as discussões filosóficas aborrecidas.	☐	☐	☐	☐	☐
Algumas pessoas consideram-me frio(a) e calculista.	☐	☐	☐	☐	☐
Esforço-me por ser excelente em tudo o que faço.	☐	☐	☐	☐	☐
Houve alturas em que experimentei ressentimento e amargura.	☐	☐	☐	☐	☐
Sou dominador(a), cheio(a) de força e combativo(a).	☐	☐	☐	☐	☐
Não dou grande importância às coisas da arte e da beleza.	☐	☐	☐	☐	☐
Tendo a ser descrente ou a duvidar das boas intenções dos outros.	☐	☐	☐	☐	☐
Sou uma pessoa aplicada, conseguindo sempre realizar o meu trabalho.	☐	☐	☐	☐	☐

certificado encontro ciência 20

Leia cuidadosamente cada uma das afirmações que se seguem e assinale, de discordo fortemente a concordo fortemente, o seu grau de concordância com elas. *

Por favor, selecione a posição apropriada para cada elemento:

	Discordo fortemente	Discordo	Nem concordo, nem discordo	Concordo	Concordo fortemente
Tenho tendência a levar as outras pessoas a fazerem o que eu quero.	☐	☐	☐	☐	☐
Já enganei ou menti para obter o que eu queria.	☐	☐	☐	☐	☐
Já elogiei (engraxeiei) pessoas para obter o que eu queria.	☐	☐	☐	☐	☐
Tenho tendência a usar as outras pessoas em meu benefício pessoal.	☐	☐	☐	☐	☐
Tenho tendência a não sentir remorsos ou arrependimento.	☐	☐	☐	☐	☐
Tenho tendência a não me preocupar com o que é certo ou errado.	☐	☐	☐	☐	☐
Tenho tendência a ser uma pessoa insensível ou fria.	☐	☐	☐	☐	☐

Tenho tendência a não me importar com as regras e normas sociais.	☐	☐	☐	☐	☐
Tenho tendência a querer que as outras pessoas sintam admiração por mim.	☐	☐	☐	☐	☐
Tenho tendência a querer que as outras pessoas me prestem atenção.	☐	☐	☐	☐	☐
Tenho tendência a querer ter prestígio ou estatuto social alto.	☐	☐	☐	☐	☐
Tenho tendência a esperar que os outros me façam favores especiais.	☐	☐	☐	☐	☐

Anexo II: Codificação das variáveis

VARIÁVEIS	
Variáveis sociodemográficas	Codificação
Género	
	Feminino (1)
	Masculino (2)
	Outro (3)
Idade	
	Medida contínua
Habilitações Literárias	
	1º ciclo (1) a doutoramento (7)
Habilitações Literárias a Frequentar	
	Nenhuma (0) a doutoramento (9)
Situação Profissional	
	Estudante (0)
	Trabalhador (1)

Trabalhador-estudante (2)
Outro (3)

Grau a frequentar

Licenciatura (1)
Mestrado (2)
Doutoramento (3)
Outro (4)

Ano que encontra a frequentar

Resposta aberta

Estuda/trabalha no setor informático

Não (0)

Sim (1)

Pais trabalham no setor informático

Nenhum (0)

Mãe (1)

Pai (2)

Ambos (3)

Prática de *hacking*

Codificação

Não (0)

Sim (1)

Tipo de <i>hacking</i> praticado	Codificação
Autopercepção	<i>Hacking black hat</i> (1) <i>Hacking grey hat</i> (2) <i>Hacking white hat</i> (3)

Hacking black hat

- | | |
|---|--|
| (1) Adicionei, apaguei, mudei, copiei ou imprimir alguma informação nos ficheiros de computador de outra pessoa sem o seu conhecimento ou permissão, por malícia ou ganhos pessoais. | Nunca (1)
Algumas vezes (2)
Muitas vezes (3)
Sempre (4) |
| (2) Acedi ao computador, ficheiros, redes ou contas de alheios sem consentimento dos seus proprietários, por malícia ou ganhos pessoais. | |
| (3) Escrevi, usei ou distribuí <i>malware</i> ou partes de <i>malware</i> (e.g., cavalos de tróia, emails <i>Phishing</i> , vírus, <i>worms</i> , etc), por malícia ou ganhos pessoais. | |
| (4) Já procurei ou consegui roubar informação sensível, pessoal e dados de empresas, por malícia ou ganhos pessoais. | |
| (5) Procurei vulnerabilidades para ganhar acesso a informação, para alterar ou distribuir, ou danificar um sistema ou rede, por malícia ou ganhos pessoais. | |

Hacking grey hat

- | | |
|--|--|
| (1) Ofereci-me para resolver vulnerabilidades descobertas, em troca de valor monetário. | Nunca (1)
Algumas vezes (2)
Muitas vezes (3)
Sempre (4) |
| (2) Divulguei vulnerabilidades de forma pública, de forma a forçar os proprietários do sistema a resolvê-las. | |
| (3) Participei em atividades de <i>hacking</i> tanto legítimas, como ilegítimas, dependendo do necessário para atingir os meus objetivos. | |
| (4) Procurei descobrir vulnerabilidades para as trazer à atenção do proprietário, mas, encontrando-as, é mais importante para mim notificar o público antes, do que o proprietário do sistema. | |
| (5) Não considero que tenha aderido a atividades maliciosas, mas também não me preocupei em seguir leis. | |

Hacking white hat

- | | |
|---|--|
| (1) Acedi de forma autorizada pelo proprietário a sistemas ou redes, para | Nunca (1)
Algumas vezes (2)
Muitas vezes (3)
Sempre (4) |
|---|--|

- identificar e/ou resolver vulnerabilidades.
- (2) Intervim no sentido de identificar, proteger e/ou combater indivíduos que acedem a sistemas informáticos, com objetivos maliciosos ou por ganhos pessoais.
 - (3) Forneci programas de segurança para proteger os sistemas de serem ilegalmente e maliciosamente penetrados.
 - (4) Realizei atividades em âmbito de emprego numa agência ou empresa, para testar e fortalecer as redes de segurança *online*.
 - (5) Examinei *software* lançado, em procura de vulnerabilidades, para submeter a *bug bounty programs* (programas que oferecem recompensas a quem identificar vulnerabilidades e as divulgar ao fabricante).

Motivações

- (1) Aprendizagem
- (2) Desafio intelectual/curiosidade
- (3) Diversão e Lazer
- (4) Ideologia
- (5) Lucro
- (6) Prestígio/Estatuto
- (7) Procura de sensações
- (8) Provar que sou melhor do que os outros
- (9) Vingança
- (10) Proteger e Defender
- (11) Fazer o bem/ajudar os outros

Codificação

- Nada importante (1)
 Pouco importante (2)
 Algo importante (3)
 Muito importante (4)

Baixo Autocontrolo

- (1) *Muitas vezes faço coisas no calor do momento sem parar para pensar;*
- (2) *Não me esforço muito a preparar o futuro, nem penso muito nisso;*

Codificação

- Discordo totalmente (1)
 Discordo (2)
 Concordo (3)
 Concordo totalmente (4)

- (3) *Costumo fazer aquilo que me dá prazer no momento, mesmo se isso me prejudicar um objetivo futuro;*
- (4) *Estou mais preocupado com o que se passa comigo no presente do que com o que me possa acontecer no futuro;*
- (5) *Geralmente procuro evitar atividades que eu sei que serão difíceis;*
- (6) *Quando as coisas complicam, costumo desistir e afastar-me;*
- (7) *Na vida, as coisas que são mais fáceis são aquelas que me dão mais prazer;*
- (8) *Não gosto de tarefas tão difíceis que levem as minhas capacidades até ao limite;*
- (9) *De vez em quando, gosto de me pôr à prova fazendo coisas um pouco arriscadas;*
- (10) *Por vezes corro riscos só pelo divertimento que me dão;*
- (11) *Por vezes, acho excitante fazer coisas que me podem causar problemas;*
- (12) *Excitação e aventura são mais importantes para mim do que me sentir seguro;*
- (13) *Se eu pudesse escolher preferia geralmente fazer atividades físicas do que atividades mentais;*
- (14) *Geralmente sinto-me melhor quando estou em movimento do que quando estou sentado e a pensar;*
- (15) *Gosto mais de sair e de fazer coisas do que ler e pensar;*
- (16) *Eu sinto que tenho mais energia e mais decessidade de atividade do que a maioria das pessoas da minha idade;*
- (17) *Eu tento pensar primeiro em mim, mesmo se isso tornar as coisas mais difíceis para os outros;*
- (18) *Eu não sou muito compreensivo com as pessoas quando elas estão com problemas.*
- (19) *Se o que eu faço desagrada às outras pessoas, o problema é delas e não meu.*
- (20) *Procurarei atingir os meus objetivos mesmo que possa causar problemas aos outros.*
- (21) *"Perco a cabeça" com muita facilidade.*
- (22) *Muitas vezes, quando me zango com as pessoas, sinto que tenho mais vontade de as*

magoar do que de falar com elas sobre o assunto.

(23) Quando estou mesmo zangado é melhor que as pessoas se afastem de mim

(24) Quando discordo seriamente de alguém é geralmente difícil para mim falar calmamente sobre isso sem me aborrecer.

NEO-FFI-20

Codificação

- | | |
|--|--------------------------------|
| (1) <i>Raramente estou triste ou deprimido.</i> | Discordo fortemente (1) |
| (2) <i>Sou uma pessoa alegre e bem-disposta.</i> | Discordo (2) |
| (3) <i>A poesia pouco ou nada me diz.</i> | Nem concordo, nem discordo (3) |
| (4) <i>Tendo a pensar o melhor acerca das pessoas.</i> | Concordo (4) |
| (5) <i>Sou eficiente e eficaz no meu trabalho.</i> | Concordo fortemente (5) |
| (6) <i>Sinto-me, muitas vezes, desamparado, desejando que alguém resolva os meus problemas por mim.</i> | |
| (7) <i>Muitas vezes, sinto-me a rebentar de energia.</i> | |
| (8) <i>Às vezes ao ler poesia e ao olhar para uma obra de arte sinto um arrepio ou uma onda de emoção.</i> | |
| (9) <i>A minha primeira reação é confiar nas pessoas.</i> | |
| (10) <i>Sou uma pessoa muito competente.</i> | |
| (11) <i>Raramente me sinto só ou abatido.</i> | |
| (12) <i>Sou uma pessoa muito ativa</i> | |
| (13) <i>Acho as discussões filosóficas aborrecidas.</i> | |
| (14) <i>Algumas pessoas consideram-me frio e calculista.</i> | |
| (15) <i>Esforço-me por ser excelente em tudo o que faço.</i> | |
| (16) <i>Houve alturas em que experimentei ressentimento e amargura.</i> | |
| (17) <i>Sou dominador, cheio de força e combativo.</i> | |
| (18) <i>Não dou grande importância às coisas da arte e da beleza.</i> | |
| (19) <i>Tendo a ser descrente ou a duvidar das boas intenções dos outros.</i> | |
| (20) <i>Sou uma pessoa aplicada, conseguindo sempre realizar o meu trabalho.</i> | |

Dirty Dozen

Codificação

- | | |
|--|--------------------------------|
| (1) Tenho tendência a levar as outras pessoas a fazerem o que eu quero. | Discordo fortemente (0) |
| (2) Já enganei ou menti para obter o que queria. | Discordo (1) |
| (3) Já elogiei (engraxei) pessoas para obter o que eu queria. | Nem concordo, nem discordo (2) |
| (4) Tenho tendência a usar as outras pessoas em meu benefício pessoal. | Concordo (3) |
| (5) Tenho tendência a não sentir remorsos ou arrependimento. | Concordo fortemente (4) |
| (6) Tenho tendência a não me preocupar com o que é certo ou errado. | |
| (7) Tenho tendência a ser uma pessoa insensível ou fria. | |
| (8) Tenho tendência a não me importar com as regras e normas sociais. | |
| (9) Tenho tendência a querer que as outras pessoas sintam admiração por mim. | |
| (10) Tenho tendência a querer que as outras pessoas me prestem atenção. | |
| (11) Tenho tendência a querer prestígio ou estatuto social alto. | |
| (12) Tenho tendência a esperar que os outros me façam favores especiais. | |

Anexo III – Modelo explicativo da prática de hacking com base nas variáveis sociodemográficas

Variáveis	Modelo 1			
	B	SE	OR	p
Género(0 = feminino)	.824	.274	2.279	.003
Idade	.566	.194	.949	.010
Habilitações (0=até ao ensino secundário)	.180	.147	1.626	.058
Área informática (0= não estuda/trabalha na área informática)	.014	.065	3.016	<.001
Área informática (Pais) (0= nenhum dos pais trabalha na área informática)	-.084	.038	1.116	.722
X² + p	46.977; p<.001			
-2. Log Likelihood	521.336			
Nagelkerke R²	.124			

B= coeficientes não standardizados; SE= erro padrão; OR= odds ratio

Anexo IV – Modelo explicativo da prática de hacking com base nas variáveis individuais – autocontrolo e traços de personalidade

Variáveis	Modelo 2			
	B	SE	OR	p
Autocontrolo	-.488	.444	.614	.272
Neuroticismo	.432	.238	1.540	.070
Extroversão	.323	.261	1.381	.216
Abertura à Experiência	.151	.156	1.163	.333
Agradabilidade	-.354	.218	.702	.104
Conscienciosidade	.082	.237	1.086	.729
Psicopatia	.167	.215	1.182	.437
Maquiavelismo	.781	.211	2.184	<.001
Narcisismo	-.179	.193	.844	.377
X² + p	45.269; p<.001			
-2. Log Likelihood	309.226			
Nagelkerke R²	.181			

B= coeficientes não standardizados; SE= erro padrão; OR= odds ratio

Anexo V – Matriz rotativa

Comportamentos	Componente		
	1	2	3
Escrevi, usei ou distribui malware ou partes de malware (e.g., cavalos de troia, emails phishing, vírus, worms, etc.), por malícia ou ganhos pessoais.	.721		
Adicionei, apaguei, mudei, copieie ou imprimi alguma informação nos ficheiros de computador de outra pessoa sem o seu conhecimento ou permissão, por malícia ou ganhos pessoais	.813		
Acedi ao computado, ficheiros, redes ou contas alheios sem consentimento dos seus proprietários, por malícia ou ganhos pessoais.	.843		

Já procurei ou consegui roubar informação sensível, pessoal e dados de empresas, por malícia ou ganhos pessoais.	.819		
Procurei vulnerabilidades para ganhar acesso a informação, para alterar ou distribuir, ou danificar um sistema ou rede, por malícia ou ganhos pessoais.	.829		
Acedi de forma autorizada pelo proprietário a sistemas ou redes, para identificar e/ou resolver vulnerabilidades.		.784	
Intervi no sentido de identificar, proteger e/ou combater indivíduos que acedem a sistemas informáticos, com objetivos maliciosos ou por ganhos pessoais.		.754	
Forneçi programas de segurança para proteger os sistemas de serem ilegalmente e maliciosamente penetrados.		.789	
Realizei atividades em âmbito de emprego numa agência ou empresa, para testar e fortalecer as redes de segurança online.		.829	
Examinei software lançado, em procura de vulnerabilidades, para submeter a <i>bug bounty programs</i> (programas que oferecem recompensas a quem identificar vulnerabilidades e as divulgar ao fabricante).		.544	
Ofereci-me para resolver vulnerabilidades descobertas, em troco de valor monetário.			.483
Divulguei vulnerabilidades de forma pública, de forma a forçar os proprietários do sistema a resolvê-las.			.615
Participei em atividades de hacking tanto legítimas, como ilegítimas, dependendo do necessário para atingir os meus objetivos.	.474		.449

Procurei descobrir vulnerabilidades para as trazer à atenção do proprietário, mas, encontrando-as, é mais importante para mim notificar o público antes, do que o proprietário do sistema.			.755
Não considero que tenha aderido a atividades maliciosas, mas também não me preocupei em seguir as leis.			.707

Nota: 1 – 5: comportamentos *hacking black hat*; 6 – 10: comportamentos de *hacking white hat*; 11 – 15: comportamentos de *hacking grey hat*