U.PORTO

SEGUNDO CICLO DE ESTUDOS

CRIMINOLOGIA

HACKING MALICIOSO: ANÁLISE DO PAPEL DA TEORIA GERAL DO CRIME E DA TEORIA DA APRENDIZAGEM SOCIAL NA EXPLICAÇÃO DOS COMPORTAMENTOS

Ana Carolina Roque Pinto

M

2023

Dissertação apresentada à Faculdade de Direito da Universidade do Porto para obtenção do grau de Mestre em Criminologia, realizada sob orientação da Professora Doutora Inês Guedes e do Professor Doutor Samuel Moreira

RESUMO

Nas últimas décadas, a disseminação do uso da *internet* e dos computadores modificou profundamente o comportamento humano e as dinâmicas societais. Com estas alterações, os recursos tecnológicos evoluem, e consequentemente, comportamentos criminais começam a ser realizados no ciberespaço (Maimon & Louderback, 2019). Um dos ilícitos que mais tem crescido é o *hacking* malicioso, descrito como o *"acesso não autorizado a computadores e redes informáticas*" (Chang & Whitehead, 2022, p. 113). Este fenómeno tem vitimado diversos indivíduos e empresas, sem que o seu perpetuador necessite de compartilhar o mesmo espaço físico que as suas vítimas (Bossler & Burruss, 2011). Todavia, perante o seu caráter problemático e danoso, os avanços criminológicos são diminutos, no qual o conhecimento sobre os seus preditores encontra-se subdesenvolvido, especialmente no contexto português. Nisto, o presente estudo tem como objetivo geral examinar a aplicabilidade da Teoria Geral do Crime (Gottfredson & Hirschi, 1990) e da Teoria da Aprendizagem Social (Akers, 1998) na explicação da prática de *hacking* malicioso. Para tal, foi administrado um questionário *online* a uma amostra de 680 pessoas (38.8% sexo feminino), com uma média de idades de 28 anos. No total, 60.4% dos participantes reportou ter praticado pelo menos um comportamento de *hacking* malicioso durante a sua vida, e 23.2% nos últimos 12 meses. Foi encontrada uma relação entre o baixo autocontrolo e a execução dos comportamentos de *hacking* malicioso, significando que os *hackers* maliciosos apresentam níveis mais baixos de autocontrolo do que *hackers* não maliciosos. Ademais, os *hackers* maliciosos detêm mais amigos que se envolvem nestes comportamentos e são mais reforçados a agir de forma ilegal aquando do uso de um computador. Foram conduzidas regressões logísticas para explorar o papel explicativo das variáveis independentes no *hacking* malicioso. Os resultados e as suas implicações serão explorados.

Palavras-Chave: aprendizagem social; autocontrolo; cibercrime; *hackers*; *hacking*; teorias criminológicas.

ABSTRACT

In the last decades, the spread of internet and computer use has profoundly changed human behavior and societal dynamics. With these changes, technological resources evolve, and consequently, criminal behaviors begin to be performed in the cyberspace (Maimon & Louderback, 2019). One of the fastest growing crimes is malicious hacking, described as *"unauthorized access to computers and computer networks"* (Chang & Whitehead, 2022, p. 113). This phenomenon has victimized several individuals and corporations, without its perpetrator needing to share the same physical space as its victims (Bossler & Burruss, 2011). However, regarding its problematic and harmful character, criminological advances are scarce, in which knowledge about its predictors is underdeveloped, especially in the Portuguese context. In this regard, the present study aims to examine the applicability of the General Theory of Crime (Gottfredson & Hirschi, 1990) and the Social Learning Theory (Akers, 1998) in explaining the practice of malicious hacking. To achieve this, an online survey was administered to a sample of 680 people (38.8% female), with an average age of 28 years. In total, 60.4% of participants reported having practiced at least one malicious hacking behavior during their lifetime, and 23.2% in the last 12 months. A relationship was found between low self-control and the execution of malicious hacking behaviors, meaning that malicious hackers have lower levels of self-control than non-malicious hackers. In addition, malicious hackers have more friends who engage in these behaviors and are more reinforced to act illegally when using a computer. Logistic regressions were conducted to explore the explicative role of the independent variables on malicious hacking. The results and their implications will be explored.

Keywords: social learning; self-control; cybercrime; hackers; hacking; criminological theories.

AGRADECIMENTOS

Em primeiro lugar, um enorme agradecimento aos meus orientadores, a Professora Doutora Inês Guedes e o Professor Doutor Samuel Moreira, que me acompanharam nesta fase tão importante do meu percurso. Tanto ao longo deste ano, como na licenciatura, mostraram sempre a sua disponibilidade e apoio, partilhando comigo os seus conhecimentos, tais que permitiram a minha evolução em termos académicos e pessoais. Obrigada por acreditarem nas minhas capacidades e ajudarem-me a dar o passo seguinte. Nada disto seria possível sem vocês.

Em segundo lugar, quero agradecer às pessoas próximas de mim, aquelas que ocupam um lugar especial no meu coração. As vossas palavras de amor e orgulho aqueceram-me por dentro, deram-me ainda mais motivação para continuar.

Por fim, um obrigada a todas as pessoas que tiraram uns minutos do seu dia a participar no estudo, que mesmo no anonimato contribuíram tanto para o meu trabalho.

Palavras não chegam, mas a todos um sincero e sentido obrigada.

LISTA DE ABREVIATURAS E ACRÓNIMOS

- **AC** – Autocontrolo
- **ARPANET** – *Advanced Research Projects Agency Network*
- **AS** – Aprendizagem Social
- **DDoS** – *Distributed Denial of Service*
- **CCC** – *Chaos Comunication Congress*
- **LC** – Lei do Cibercrime
- **MIT** – *Massachusetts Institute of Technology*
- **SPS**– *Signals and Power Subcommittee*
- **TAS** – Teoria da Aprendizagem Social
- **TIC** – Tecnologias da Informação e Comunicação
- **TGC** – Teoria Geral do Crime
- **TMRC** – *Tech Model Railroad Club*

ÍNDICE GERAL

ÍNDICE DE TABELAS

INTRODUÇÃO

Nas últimas décadas, face ao aparecimento e desenvolvimento do ciberespaço, a sociedade tem sofrido mudanças significativas em diversas áreas (*e.g.,* comércio, comunicação, entretenimento), na medida em que a *internet* e os avanços informáticos passaram a permitir uma ligação contínua entre as pessoas sem necessitarem de compartilhar o mesmo espaço (Mbanaso & Dandaura, 2015). A disseminação e acessibilidade global das componentes das TIC redefiniu os crimes tradicionais existentes (*e.g., bullying*) adicionando-lhes uma faceta *online* (*e.g., cyberbullying*), e possibilitou a criação de novos ilícitos criminais, somente realizados mediante recurso a estes dispositivos (Furnell, 2001; Wall, 2007). Um destes exemplos é o *Hacking*, que pela análise efetuada das tendências da cibercriminalidade, constata-se que é um dos crimes informáticos que foi alvo de um rápido crescimento nos últimos anos (Maimon & Louderback, 2019). Deste feito, estes comportamentos começam a assumir um papel central nas preocupações públicas sociais e governamentais, todavia sem o auxílio de dados estatísticos significativos que reflitam este fenómeno e permitam elaborar medidas de ação (Payne, 2020).

Em 2022, formas de *hacking* (*e.g.,* negação de acesso a um serviço; distribuição de *malware* e *ransomware*) foram responsáveis por mais de metade (52%) das violações de dados existentes (Hiscox, 2022), no qual cerca das 65 mil vulnerabilidades informáticas descobertas foram resultado destes comportamentos (HackerOne, 2022). Relativamente ao contexto português, a mesma propensão é observada, verificando-se em 2022 um aumento de 60.1% do crime 'acesso/interceção ilegítima' face ao ano anterior, tornando-se o ilícito criminal informático com mais frequência nesse ano (RASI, 2022) e sendo considerado um agente de ameaça relevante à cibersegurança portuguesa nos anos referidos (CNCS, 2022). Dado que os *hackers* maliciosos têm aproveitado explorar as vulnerabilidades tecnológicas das instâncias governamentais, das empresas e dos indivíduos singulares (World Economic Forum, 2023), estas práticas resultam em danos sociais, nomeadamente ao nível do custo económico, que no último ano rondou os 4.35 milhões de dólares (IBM Security and Ponemon Institute, 2022).

Embora o *hacking* malicioso seja um fenómeno criminal crescente e com um caráter danoso, a realização de investigações empíricas em torno destes comportamentos é diminuta e marcada por diversas inconsistências (*e.g.,* concetualização e operacionalização não consensuais do *hacking*), comparativamente a outras áreas temáticas inerentes à Criminologia (Holt, 2020). Este facto é ainda mais predominante em Portugal, dado que neste contexto o conhecimento que se detêm é exíguo, existindo uma necessidade de se começar a investigar o

hacking e produzir saber sobre os aspetos inerentes a este fenómeno. Face a isto, a presente investigação tem o propósito, por um lado, de explorar a prática de comportamentos de *hacking* malicioso pela vertente do ofensor e, por outro, de analisar quais os preditos explicativos destes atos, nomeadamente o papel do autocontrolo da Teoria Geral do Crime de Gottfredson e Hirschi (1990) e das componentes da Teoria da Aprendizagem Social de Akers (1998).

Desta forma, passa-se a enumerar os capítulos do estudo. No capítulo I apresentar-se-á um breve enquadramento teórico quanto ao cibercrime, incluindo o papel da *internet* e a concetualização e tipologias do cibercrime. Seguidamente, o capítulo II alude ao *hacking*, onde será elencada a evolução histórica e a caraterização dos principais termos (*hacking, hack e hacker*). Relacionado com este ponto, no capítulo III constará a fundamentação teórica e empírica dos comportamentos de *hacking* malicioso, referindo com mais enfoque os contributos explicativos da TGC e da TAS. Neste ponto, integrar-se-ão estudos empíricos, de modo a apresentar o que tem sido descoberto na comunidade científica e o que suporta a presente investigação. Posteriormente, o capítulo IV será alusivo aos aspetos que consagram o estudo empírico, como os objetivos gerais e específicos, as hipóteses e o método utilizado. Por sua vez, o capítulo V será dedicado à análise estatística e à apresentação dos resultados obtidos advindos da aplicação de um questionário *online*. Por fim, constará uma discussão onde será abordado um ponto de vista crítico quanto aos resultados, as suas implicações e direções futuras.

CAPÍTULO I – CIBERCRIME

1.1. Surgimento do Cibercrime – o papel da *Internet*

O surgimento e evolução histórica do termo cibercrime, ou cibercriminalidade, remete para o aparecimento da *internet*, dado que sem a mesma, esta multiplicidade nova de crimes não existiria (Yar, 2006). A *internet* foi criada, originalmente, no seio do desenvolvimento de estratégias de defesa dos exércitos no período da Guerra Fria, nomeadamente no decorrer dos projetos de investigação ARPANET. Esta era uma ferramenta utilizada para fins militares, desenhada para facilitar a circulação de informação neste meio (Castells, 2002; Choi *et al.*, 2020; Yar, 2006). Desta forma, entende-se que a *internet* estava destinada somente a uma comunidade específica dotada de conhecimento científico e militar. Contudo, em meados dos anos 90, este caráter reservado da *internet* começa a ser substituído pela disseminação e comercialização da mesma, originando um crescimento exponencial nos países que a detinham (Castells, 2002; Choi *et al.*, 2020). A título de exemplo, recorrendo aos dados elencados pela pesquisa do *International Telecommunication Union* e do *Internet World Stats* é possível traçar

uma evolução do uso da *internet* a nível mundial. No ano de 1990, o número de indivíduos que utilizava a *internet* era unicamente de .049%, uma percentagem que cresceu exponencialmente para 69% no ano de 2022.

Antes de abordar as consequências da propagação e utilização em massa da *internet*, é decisivo analisar a sua concetualização. Esta foi sendo alvo de dedicação constante por parte de equipas de investigadores que atuavam no sentido de compreender melhor a *internet*, os seus utilizadores e gerar uma definição (Choi *et al.*, 2020). De acordo com a visão de Snyder (2001), a *internet* não apresenta somente uma forma definitiva ou generalizada, mas antes um conjunto de práticas sociais e pessoais, na medida em que assume determinada configuração consoante o uso que os indivíduos lhe atribuem. Por outro lado, Castells (2002) aborda uma perspetiva com base na comunicação, afirmando que a *internet* é uma "*network of networks"* (p. 11), potencializando a troca de informação entre os cidadãos, tornando-se o 'quê' e o 'como' da atividade executada *online*.

Assim, a incontestável difusão mundial do uso deste utensílio tecnológico inaugura um novo marco, conduzindo a mudanças profundas em diversas áreas da vida em sociedade (MacFarlane & Bocij, 2003; Yar, 2006). A *internet* criou oportunidades incomparáveis em todas as áreas do mundo social, designadamente, no comércio global, na educação, no entretenimento, na investigação científica, no discurso público e na comunicação, aproximando os diversos países e melhorando a sua qualidade de vida (MacFarlane & Bocij, 2003).

De facto, é inegável que a *internet* seja considerada uma janela para o mundo, contribuindo para a consagração de uma sociedade digital nos tempos modernos (Britz, 2013; Dias, 2012). Porém, este desenvolvimento tecnológico acarretou alguns pontos negativos, sobre os quais Britz (2013) expõe que *"as vantagens que tornam a internet (...) tão atraente, costumam ser as mesmas que representam o maior risco"* (p. 2). Ou seja, pelas palavras do autor, considera-se que a *internet* foi o primeiro passo para a criação de um terreno fértil no surgimento de novas atividades e comportamentos ilícitos, que no seu conjunto são comummente intitulados de Cibercrime (Britz, 2013).

1.2. Concetualização e Tipologias do Cibercrime

A denominação do termo Cibercrime, apesar de amplamente utilizada, não contém em si uma visão única e unânime, suscitando várias formas de interpretação. Diversas entidades têm unido esforços no sentido de concetualizar este fenómeno, especialmente a comunidade científica e as instituições legais (Payne, 2020).

Quanto à comunidade científica, de forma simplista, o conceito cibercrime tem sido associado a todos os comportamentos prejudiciais que acontecem no ciberespaço, sendo este último, o *"caminho para transferir informação de uma localização para outra"* (Payne, 2020, p.11). Na perspetiva de Yar (2006), o cibercrime não deve ser descrito como um único comportamento, mas um espetro de atividades ilícitas que detêm como denominador comum a presença nas redes e tecnologias de informação. Na mesma linha de pensamento, Wall (2007) afirma que é a *"ocorrência de um comportamento nocivo, estando relacionado com um computador"* (p. 2). Nasution e colegas (2018) apresentam uma visão mais afunilada, no qual o cibercrime é o *"ataque contra o conteúdo, o sistema de computador e o sistema de comunicação de propriedade, de outras pessoas, ou em geral, no ciberespaço"* (p. 1589).

Relativamente ao sentido que as entidades legais associam ao cibercrime, este varia consoante a consagração legal de cada país, o que dificulta o encontro de um aspeto paralelo (Payne, 2020; Yar, 2006). De modo geral, os países não elencam uma definição isolada, mas classificações de comportamentos criminais que podem ter lugar no ciberespaço (Amador, 2012), indo ao encontro da perspetiva de Yar (2006) apresentada previamente. No caso português, o cibercrime aparece contemplado na Lei do Cibercrime (LC) – Lei n.º 109/2009, de 15 de setembro, onde estão tipificados múltiplos ilícitos penais advindos da criminalidade informática (*e.g.,* falsidade informática). Esta lei segue as direções da Convenção do Cibercrime do Conselho de Europa (2001) pela Resolução da Assembleia da República n.º 88/2009, na qual divide o cibercrime em quatro categorias: 1) infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos; 2) infrações relacionadas com computadores; 3) infrações relacionadas com o conteúdo; 4) infrações respeitantes a violações do direito de autor e direitos conexos[1].

Esta divisão encontra fundamento em tipologias propostas pela comunidade científica, que face à multiplicidade de condutas que o cibercrime abrange, o ato de classificar permite facilitar a sua análise (Wall & Williams, 2007). Furnell (2001) e Furnell e colegas (2015) propõem duas classificações: 1) crimes auxiliados por um computador, ou crimes cibernéticos, sendo atividades que pré-datam a era da *internet* e adquirem um novo formato com o ciberespaço; 2) crimes focados no computador ou crimes ciber-dependentes, dado que agregam novas formas de crime que não existiam antes da *internet*, podendo ser apenas cometidas pelo uso de computadores ou tecnologias.

[1] A visão apresentada nos documentos legais segue uma definição de cibercrime em sentido restrito.

Semelhante a esta classificação, Wall (2007) distingue entre três tipos de ilícitos que a cibercriminalidade pode conter, designadamente: 1) *computer-assisted offenses*, vistos como a reelaboração das ofensas tradicionais no ciberespaço, incluindo formas de roubo e fraude; 2) *computer content crimes*, caraterizados pela comunicação e representação prejudicial para a sociedade e circulação de imagens obscenas e violentas; 3) *computer integrity crimes*, sendo ofensas relacionadas com a integridade dos sistemas. Neste último o ponto, inclui as condutas de *cybertrespass*, retratando a passagem não autorizada dos limites nos sistemas computacionais, ou seja, o *hacking* (Wall, 2001).

Considerando as ideias suprarreferidas, a análise do cibercrime deve ser ponderada e multifacetada, abarcando em si a complexidade do fenómeno (Dias, 2012). Este trouxe impactos drásticos nas sociedades modernas, uma vez que a sua exteriorização se carateriza por uma dimensão global e transnacional, uma deslocação veloz e indecifrável na *internet*, pelo anonimato das condutas criminosas e pela diversidade de ordens e punições jurídicas (Dias, 2012; Wall, 2007). Estas são as caraterísticas que tornam o cibercrime um fenómeno nocivo para a sociedade.

CAPÍTULO II – *HACKING*

Exposta a concetualização e classificação do cibercrime, segue-se para o principal enfoque desta investigação: o *Hacking*. Neste capítulo, expõem-se as principais configurações que permitem caraterizar e compreender aprofundadamente este fenómeno, designadamente, os detalhes da sua evolução histórica, a concetualização e caraterização dos principais termos e a figura do *hacker*, o cibercriminoso. Recordando, o *hacking* malicioso é um comportamento inserido na classe de crimes focados no computador, proposta por Furnell (2001) e nos atos de *cybertrespass* elencados por Wall (2001).

2.1. Evolução Histórica

Relativamente ao aparecimento dos comportamentos de *hacking*, Steinmetz (2016) afirma que os mesmos existem desde que os indivíduos dispõem do contacto, envolvimento e conhecimento especializado inerente à área das TIC. McLeod (2014) partilha da mesma presunção, apresentando o acontecimento de 1903 onde Marconi tentava promover a sua patente de rádio, marcada pelo envio de mensagens confidenciais. Contudo, na sua demonstração, a mensagem recebida não foi a de Marconi, mas a de Maskelyne, que invadiu e

exibiu a fragilidade do sistema do seu autor. Segundo McLeod (2014) e Steinmetz (2016), este ato da altura pode ser visto atualmente como um ato de *hacking*.

Embora seja evidente que existem certos comportamentos que podem ser situados nos primórdios tecnológicos, a generalidade da comunidade científica identifica a década de 50 do século XX como a origem das condutas de *hacking*, mais especificamente associadas aos membros do TMRC (Levy, 1984). Este era um clube pertencente ao MIT, constituído por alunos de engenharia que dedicavam o seu tempo livre a duas tarefas. Por um lado, a construir réplicas de comboios que se assemelhassem à escala real, e por outro, a debruçarem-se nos circuitos de ligação e funcionamento dos mesmos. Neste seguimento, surge um subgrupo intitulado de SPS, dedicado única e exclusivamente ao sistema de tecnologia e controlo dos comboios. Derivado desta aproximação e ligação pessoal dos membros, o comité fortificou-se e começou a criar jargões para as tarefas tecnológicas que executava (Levy, 1984, 2001). É neste terreno que o termo *hacking* emerge primeiramente, sendo a referência a "*brincadeiras com os sistemas elétricos dos sistemas e os equipamentos por diversão"* (Holt, 2020, p. 728).

Neste período inicial, os recursos tecnológicos (*e.g.,* computadores) eram subdesenvolvidos e limitados em termos de processamento e de memória, não se encontrando ligados entre si de nenhuma forma. Assim, este comité começou a delinear e criar estratégias tecnológicas que melhorassem estas capacidades (Jaquet-Chiffelle & Loi, 2020). Ou seja, os seus membros arranjavam soluções benéficas para as funções dos sistemas, sendo intitulado pelos mesmos como *hack* (Levy, 2001). Partindo dos objetivos e ações do clube TMRC e, em concreto, do comité SPS, a arte de 'hackear' ganha força e reconhecimento, (Levy, 1984), iniciando a constituição de uma comunidade ou subcultura marcada por ideais, expressões e comportamentos específicos (Jaquet-Chiffelle & Loi, 2020; Steinmetz, 2016). Posto isto, esta primeira aproximação ao *hacking* e às suas condutas assentava em larga escala num propósito de diversão, colaboração e entusiasmo pelo ambiente digital e tecnológico, onde o principal objetivo era *"partilhar informação, duvidar das autoridades centralizadas e usar os computadores para criar um mundo melhor"* (Jaquet-Chiffelle & Loi, 2020, p. 181). Esta conjetura de ideais ficou denominada de *Hacker Ethic,* sendo estes indivíduos conhecidos como *True Hackers*, uma vez que representa fielmente o espírito e as intenções primordiais do *hacking* (Jaquet-Chiffelle & Loi, 2020).

A partir do final dos anos 80, a perceção social destes comportamentos sofre uma mudança, totalmente persuadida pelas alterações que se faziam sentir na vida social (Holt, 2020; Yar, 2006). Nesta época, a *internet* começa a ser disseminada, e com ela todo o envio e receção

de informação, tal como advogava a *Hacker Ethic*. A adicionar a isto, os computadores e os seus sistemas tecnológicos sofrem uma diminuição, em termos económicos e dimensionais, facilitando a sua detenção para qualquer pessoa (Holt, 2020; Taylor, 1999). Com estes desenvolvimentos, o interesse público e governamental pelo uso de computadores e informação aumenta, iniciando-se os debates e as declarações sobre o direito de privacidade dos cidadãos (Levy, 1984; Yar, 2006). Isto desencadeia uma vaga de novas criminalizações, no qual a lei expande e começa a abranger o acesso não autorizado aos sistemas de computadores e a detenção não autorizada de informação das instituições bancárias e financeiras (Hollinger & Lanza-Kaduce, 1988; Holt, 2020).

Portanto, o rótulo benigno e ético inicialmente atribuído ao *hacking* começa a ser posto em causa, dado que a nova visão geral se aproximava cada vez mais de comportamentos criminais e de má-fé (Holt, 2020). Diversos autores marcam estes acontecimentos como um período fulcral na alteração da imagem do *hacking* e dos *hackers*, no qual os interesses primordiais destes indivíduos foram alvo de especulação e desconfiança, gradualmente associados a um intento malicioso (Holt, 2020; Jaquet-Chiffelle & Loi, 2020; Yar, 2006). Derivado destas ocorrências desencadeia-se uma tensão entre os verdadeiros interesses dos *True Hackers* e as conceções erróneas do público, sendo facilmente entendida pela seguinte citação: *"o aumento na enfâse da aplicação criminal no hacking pelo público, tornou difícil para os jovens, tecnológicos e sofisticados hackers explicarem as suas atividades a outros"* (Holt, 2020, p. 730).

Neste seguimento os *True Hackers* pretendiam alterar o entendimento popular, cristalizando essa intenção com a publicação do *"The Hacker Manifesto"* pelo *The Mentor* em 1986 na *Phrack Magazine*. Este pequeno artigo resumia a paixão pelo *hacking* e pela vontade de deter e partilhar conhecimento, expondo que todas as preocupações sociais para com estes comportamentos eram infundadas e exacerbadas pela falta de entendimento tecnológico por parte do governo e do público. Apesar de bem-intencionada, esta publicação suporta alguns aspetos malignos defendidos pela sociedade, dado que enfatiza que os jovens deviam envolver-se nestas atividades, desafiar as figuras de autoridade e mostrar a verdadeira inteligência e capacidade que detêm, independentemente de ser considerado um ilícito (Holt, 2020; Holt *et al.,* 2022; Wark, 2004).

Nisto, com a passagem para o século XXI e com o progresso ocorrido na sociedade, os computadores e a *internet* passam a ter um lugar central no quotidiano dos cidadãos, especialmente na criação de novas formas de informação e identidade *online* (Jaquet-Chiffelle

& Loi, 2020). Emerge uma nova geração de *hackers* com menos sofisticação e capacidades tecnológicas, todavia, com mais intenções duvidosas. Estes, detendo uma visão puramente económica, rapidamente se aperceberam das vantagens que poderiam obter com a navegação no ciberespaço, perdurando este propósito até aos dias de hoje (Holt, 2020; Taylor, 1999).

Atualmente, a visão do *hacking* mantém-se na conotação maliciosa, sendo perspetivado de forma generalizada e simplista como o *"acesso não autorizado a computadores e redes informáticas*" (Chang & Whitehead, 2022, p. 113). Esta forma foi autonomizada para diversos planos legais, como no caso português com a Lei do Cibercrime (LC) – Lei n.º 109/2009, de 15 de setembro, concretamente no artigo 6º, intitulado de '*Acesso Ilegítimo'*. Porém, frisa-se que na atualidade não é aconselhável abordar o *hacking* como algo unidimensional, dado que envolve manifestações distintas que não devem ser transpostas para uma única concetualização (Holt, 2020; Jaquet-Chiffelle & Loi, 2020).

2.2. Caraterização dos Termos

Traçado o desenvolvimento histórico do *hacking*, de seguida passa-se para a apresentação e caraterização dos principais termos inerentes ao fenómeno em causa: *hacking*, *hack* e *hacker(s)*. O objetivo é dar a conhecer os diversos detalhes dos comportamentos e agentes do *hacking*, para se recriar uma imagem geral.

2.2.1. Hacking

Atualmente, o *hacking* malicioso é um dos fenómenos cibercriminais mais analisado pela comunidade científica internacional, paralelamente situado no centro dos debates e das preocupações públicas sociais (Yar, 2006; Holt, 2020; Payne, 2020). Pela análise histórica deste cibercrime, compreende-se que o *hacking* adquiriu diversas visões ao longo do tempo, resultando num modelo concetual mutável e pouco consensual (Steinmetz, 2016). Thomas (2002) complementa esta ideia, no qual declara que o termo é extremamente difícil de definir, dado que foi aplicado e esticado a diversos grupos e contextos, perdendo-se qualquer precisão concetual que se detinha inicialmente.

Como visto previamente, na origem do termo, o *hacking* era definido como ético, ligado ao fascínio pelas descobertas tecnológicas e à inovação e sofisticação informática (Levy, 1984; Holt, 2020; Jaquet-Chiffelle & Loi, 2020), no qual seria *"uma forma criativa de resolver um problema quando confrontado com a sua complexidade técnica"* (Yar, 2016, p. 6). Porém, esta visão inverteu-se, começando a adquirir o rótulo maligno. Nisto, os *True Hackers* apresentam o termo *cracking* para enfatizar o que seria na realidade essas intenções malignas e condutas

criminais e, deste modo, conseguirem distanciar delas o seu trabalho (Jordan, 2017; Yar, 2006). Moore (2015) apresenta este conceito como o ato que *"viola as proteções dos direitos de autor de um software, e o acesso inadequado a ficheiros e serviços protegidos por palavras-passe"* (p. 19). Embora esta vontade de criar uma distinção fosse notável, a consagração ilícita do *hacking* prevaleceu, consolidando-se até aos dias de hoje (Moore, 2015; Yar, 2006).

Atualmente, a concetualização mais aceite no seio da comunidade científica é a de Taylor (1999, p.viii) – "*acesso não autorizado e consequente uso de sistemas computacionais de outras pessoas"* – na medida em que retrata os contornos do *hacking* de forma simples, mas composta (Holt, 2020). Diversos autores contribuem para a sua corroboração, afirmando que o *hacking* é sinónimo de atividades ilegais associadas à intrusão e manipulação de um computador (Yar, 2006), no qual esta tentativa, seja ou não bem-sucedida, é sempre não autorizada (Sharma, 2007).

Ademais, outra perspetiva emerge na caraterização do *hacking*, sendo a alegação de que este fenómeno é uma subcultura, apelidada de *Hacking Culture* (Holt, 2020). Múltiplos autores (*e.g.,* Holt, 2020; Jordan & Taylor, 1998; Steinmetz, 2016; Thomas, 2002) afirmam que os objetivos e crenças desta cultura convergem em três elementos centrais – tecnologia, conhecimento e secretismo – na qual se mantêm, independentemente de os atos terem uma natureza ética ou maliciosa. Ou seja, esta cultura partilha da paixão pela tecnologia e inovação técnica, no qual o conhecimento sobre esta é reconhecido pelos seus membros. Embora exista a vontade de partilhar as descobertas com o mundo, devido ao crescimento da conotação maliciosa do termo *hacking* e da extensão da aplicação da lei, a comunicação entre os indivíduos passa a ser feita *online* com base no secretismo e na ocultação de identidade (Holt, 2020; Taylor, 1999; Yar, 2006).

Embora o *hacking* assuma diversos contornos na sua caraterização e evolução, conclui-se que a perspetiva dominante é a configuração negativa e criminal, no qual estas alterações concetuais são meramente analisadas pela Criminologia com o intuito de perceber detalhadamente o fenómeno. Constata-se que é um termo socialmente construído, adquirindo a concetualização que a sociedade lhe atribui (Becker, 1963). Esta construção social pode assumir pontos de vista exacerbados, resultando num pânico moral infundado (Wark, 2006), que apenas origina um processo contínuo de rotulagem no comportamento e na identidade do próprio indivíduo (Becker, 1963; Coleman & Golub, 2008). Nisto surge a necessidade de realizar uma análise aprofundada do fenómeno e desconstruir diversos aspetos e termos que o *hacking* envolve.

2.2.2. Hack

Originalmente, o conceito *hack* aparece associado às partidas e brincadeiras que os alunos do MIT realizavam, seja entre eles, seja para com os professores e a universidade (Levy, 1984). Apesar deste primeiro uso mais antigo e tradicional, o termo ganha uma nova vida com os membros do clube TMRC, tal como visto previamente na parte 2.1. Seria considerado um *hack* um procedimento técnico e sofisticado que trouxesse agrado para o seu realizador (Levy, 1984; Steinmetz, 2016). Em termos gerais, a definição apresentada pode ter um certo encaixe na realidade atual, não relacionada diretamente com as tecnologias, mas no qual as pessoas tendem a criar *life hacks* ou truques que facilitem e simplifiquem a forma de se fazer determinada tarefa no seu dia-a-dia. Contudo, este conceito é amplamente conhecido e inserido no meio dos sistemas informáticos, tecnológicos e computacionais, sendo aí que detém o seu destaque (Holt, 2020; Yar, 2006).

O termo em questão, como abordado anteriormente, advém de uma manifestação mais abrangente – o *hacking* – podendo afirmar-se que o *hack* é, assim, um ato de *hacking* ou 'hackear'. Esta perceção é claramente simplista, dado que este comportamento envolve em si múltiplos detalhes e caraterísticas que têm de ser alvo de um aprofundamento (Yar, 2006). De acordo com Holt (2020) o *hack* alia-se a *"métodos mais técnicos e tecnológicos* (...) *envolvendo o uso de programas e ferramentas que facilitem um compromisso."* (p. 727). Derivado disto, este ato abrange duas componentes chave – a vulnerabilidade e a exploração. Segundo o autor, existem inúmeras vulnerabilidades a serem identificadas num dispositivo, no qual esta falha ou erro pode ser utilizado para explorar determinado *software* e/ou *hardware*, e consequentemente ganhar acesso ao sistema de comando e ligações (Holt, 2020).

Perante isto, a realização de *hacks* pode assentar num consenso e consentimento entre indivíduos, sendo uma forma de resolver um problema de forma eficiente (Holt, 2020; Turkle, 1984; Yar, 2006). Contudo, atualmente a visão prevalecente envolve o uso de infraestruturas e/ou ferramentas tecnológicas, direcionado a um propósito criminal e ilegítimo, que segundo Peacock (2013) remete para *"a invasão a um computador com o objetivo específico de roubar informação ou causar dano"* (p. 31).

Diversos autores, em vez de proporem uma concetualização única do termo, passam por elencar algumas caraterísticas do que seria considerado um 'bom *hack*' (Peacock, 2013). Nisto destaca-se a referência a determinadas palavras, designadamente: simplicidade; mestria; e ilicitude. Isto significa que o ato seria simples, mas impressionante; controlado, concretizado a

partir de técnicas sofisticadas; e ilícito, indo contra as regras normativas e legais (Taylor, 1999; Turkle, 1984).

Situados noutro prisma de análise, os escritos de Yar (2006) contribuem em grande medida para a imagem geral que se detém do comportamento. O autor parte da sua conceção de *hacking* e exemplifica múltiplas formas que o ato pode assumir, sendo as seguintes: 1) o furto de informação confidencial ou propriedade; 2) o furto de recursos computacionais; 3) a desfiguração de *sites*; 4) a sabotagem, alteração e/ou destruição de sistemas; 5) a negação de acesso a um serviço; 6) a distribuição de *software* malicioso.

2.2.3. Hacker(s)

O termo *hacker(s)* tem sofrido mutações na sua identidade, derivado das mudanças históricas e tecnológicas que se fizeram sentir na sociedade. Inicialmente, este emerge na década de 60 com uma representação positiva e de enaltecimento, na qual descrevia um indivíduo com competências criativas desenvolvidas, capaz de criar e fornecer soluções que resolvessem problemas computacionais (Levy, 1984, 2001; Yar, 2006). Esta aproximação é descrita por Levy (1984) como a primeira geração de *hackers*, ficando conhecidos como os pioneiros das técnicas de programação e domínio dos computadores.

Ademais, derivado da evolução computacional, nasce a segunda geração, trazendo consigo a vontade de imersão total no saber tecnológico, especialmente no funcionamento de *hardware* e *software*. O objetivo destes *hackers* era devolver esses conhecimentos às grandes empresas, disseminando estas ferramentas (Taylor, 1999). Mais tarde, com o avanço das funcionalidades gráficas dos dispositivos, aparece uma terceira geração, conhecida por *programmers*. Estes dedicavam-se exclusivamente aos jogos de computador e à sua arquitetura, tornando-se vanguardistas na área (Levy, 1984). Por fim, a quarta geração de *hackers* relaciona-se inteiramente com a conotação negativa, sendo alguém que acede de forma ilegítima ao computador de outrem (Taylor, 1999; Holt, 2020). As ideias referidas por Richet (2013) permitem aprofundar esta definição, no qual o autor refere que os *media* utilizam o conceito em questão para se referirem *"a um intruso que entra num sistema de computadores para roubar ou destruir informação"* (p. 54).

Embora seja notável o contributo desta distinção geracional, a análise destes indivíduos não deve ser reduzida à ação que realizam, dado que o comportamento do *hacker* é baseado em diversos objetivos, justificações e intenções, existindo estas em simultâneo (Moeckel, 2019; Rogers, 2010). Nisto, ressalva-se que nem todos os indivíduos que se envolvem nestes atos possuem intenções maliciosas (Rogers *et al.*, 2006). Segundo Richet (2013), seria crucial

utilizar o conceito *hacker(s)* segundo o seu significado original, e o conceito *cracker(s)* para referir os indivíduos que usam as suas competências para criarem e usarem *malwares*, e infiltrarem-se nos sistemas de segurança de forma ilegal e com intenção de causar danos nos mesmos.

Posto isto, uma concetualização mais apropriada seria a de Fox e Holt (2021), que descrevem os *hacker*s como os indivíduos com um interesse profundo na tecnologia, no qual utilizam os seus conhecimentos para aceder aos sistemas informáticos, seja com ou sem permissão do proprietário do sistema. Outros autores adotam esta posição, afirmando que é inadequado representar os *hackers* segundo uma dicotomia de indivíduos benignos ou malignos (Coleman & Golub, 2008), dado que o termo engloba diferentes grupos, intenções e objetivos, logo a visão da literatura científica não deve reduzir estes indivíduos a *"visionários ou diabos sinistros"* (Bossler & Burruss, 2011, p. 65).

2.3. Perfil Sociodemográfico do *Hacker*

Até ao século XX, o *hacker* era visto como um jovem dotado de inteligência tecnológica, obcecado pela procura excessiva de conhecimento, habitando num ambiente misterioso e anónimo (Coleman & Golub, 2008; Nissenbaum, 2004). A tendência era perspetivar o indivíduo como patológico, sinistro e introvertido, que somente conseguia comunicar no ciberespaço (Hollinger, 1991; Peacock, 2013). Atualmente, esta visão altera-se drasticamente, dado que o *hacker* é o realizador do *hack*, ou seja, alguém que se infiltra num sistema de computadores independentemente da sua motivação (Jaquet-Chiffelle & Loi, 2020). Este não aparece relacionado com a introversão e a solidão, apenas marcado pela ocultação da sua identidade (Peacock, 2013; Seebruck, 2015).

Pelos estudos científicos levados a cabo é possível traçar um perfil sociodemográfico do *hacker*, embora sempre comprometido pelo anonimato e pela fraca participação nas investigações (Ferreira & Guedes, 2021; Taylor, 1999). Relativamente a fatores como o género, a etnia e a idade, os resultados obtidos por diversas fontes convergem para um perfil comum, no qual o *hacker* se cinge a ser alguém do sexo masculino, geralmente caucasiano e com uma idade inferior a 30 anos (*e.g.,* Bachmann, 2008; Fox & Holt, 2021; HackerOne, 2020, 2021; Nodeland & Morris, 2020; Steinmetz, 2016; Taylor, 1999).

Quanto às habilitações literárias e ocupação profissional, a maioria dos *hackers* detém a conclusão dos estudos, especialmente graus de instrução de nível mais elevado (*e.g.,* licenciatura, mestrado e doutoramento) (Bachmann, 2010; HackerOne, 2020, 2021; Steinmetz,

2016; Woo, 2003). Apesar dos conhecimentos e capacidades na área da tecnologia e informática (Fox & Holt, 2021; Steinmetz, 2016), estes tendem a posicionar o *hacking* como um *part-time* ou um *hobbie*, sendo poucos os indivíduos que se encontram totalmente empregados neste meio (Bachmann, 2008; HackerOne, 2020, 2021; Steinmetz, 2016; Taylor, 1999). Contudo, grande parte dos sujeitos que participam em conferências sobre a temática do *hacking*, tendem a executar estes comportamentos profissionalmente, no âmbito de empregos na área da tecnologia (HackerOne, 2020, 2021; Steinmetz, 2016).

No que diz respeito à parte contextual e social, nas investigações científicas é possível constatar que estes indivíduos fazem parte de uma rede de pares, seja amizades *online* (*e.g.,* fóruns e grupos na *internet*) e/ou *offline (e.g.,* contexto escolar e conferências internacionais de *hacking,* como a *Defcon* e a *CCC*) (Fitch, 2004; Leukfeldt *et al.,* 2017; Skinner & Fream, 1997). Estas informações permitem quebrar com a ideia de introversão e isolamento anteriormente associadas ao *hacking*. Ademais, a faceta social dos *hackers* tem sido igualmente evidenciada na *"presença de laços maritais e familiares"* (Steinmetz, 2016, p. 45), no qual estes indivíduos se envolvem em relações amorosas (*e.g.*, namoro, casamento, divórcio), havendo diversos elementos nas amostras que constituem família (Steinmetz, 2016, Taylor, 1999). Ademais, estes indivíduos apresentam uma relação de proximidade com os seus pais, tendo uma perceção positiva e íntima da mesma (Ferreira & Guedes, 2021; Steinmetz, 2016).

Por fim, relativamente à ocupação dos tempos livres, a maioria dos participantes considerados *hackers* nas amostras desta linha de investigação apresentam uma maior utilização das tecnologias (*e.g.*, computador, *internet*, *sites online*), despendendo mais horas diárias a este tipo de lazer do que os indivíduos sem envolvimento nos comportamentos de *hacking* (Holt, 2007; Steinmetz, 2016). Um dado complementar, é que o primeiro contacto destes sujeitos com a tecnologia é precoce, situando-se no período da pré-adolescência. Isto é visto por diversos autores como um fator explicativo para o *hacking* juvenil (Holt *et al.*, 2020; Steinmetz, 2016; Taylor, 1999).

Estes dados fornecem informação sobre as caraterísticas e vida dos *hackers*, permitindo romper com o estereótipo advindo do senso comum e da opinião pública (Steinmetz, 2016).

2.4. Tipologias de *Hackers*

No âmbito da compreensão dos *hackers* e dos seus comportamentos, no final da década de 80 a comunidade científica iniciou a elaboração de tipologias ou classificações, trazendo um novo *insight* para a forma como se perspetivava estes indivíduos (Peacock, 2013; Seebruck,

2015). Em 1985, os autores Landreth e Rheingold publicam uma das primeiras classificações de *hackers*, tornando-se o ponto de partida para o desenvolvimento da investigação desta temática. Partindo da evidência empírica, estes estabelecem as seguintes categorias: 1) *Novice*; 2) *Student;* 3) *Tourist*; 4) *Crasher*; 5) *Thief*. Nestas descrevem as motivações e a forma como os indivíduos veem o *hacking*.

Os *Novices* caraterizam-se por serem *hackers* com idades inferiores a 14 anos que percecionam o *hacking* como algo divertido que permite pregar partidas. Estes, apesar de terem um gosto pelos computadores e pelas tecnologias, detêm pouca experiência nos mesmos, dado que somente os utilizam para arranjarem um entretenimento nos tempos livres. Os *Students* diferem em larga medida da categoria anterior, dado que a motivação base é a curiosidade e a aprendizagem. Os indivíduos que cabem nesta categoria apresentam uma necessidade de conhecer os computadores e os seus sistemas, dedicando diversas horas para alcançar este propósito. Para estes, o *hacking* é sinónimo de erudição, que embora acedam aos sistemas e contas de outrem, não segue uma intenção maliciosa.

O terceiro tipo é o *Tourist*, um indivíduo inofensivo movido pela *"aventura e o desafio de resolver um puzzle"* (Landreth & Rheingold, 1985, p. 64). Este estabelece certas tarefas no seu processo de descoberta, tendo de ser executadas num determinado tempo, alcançando, assim, a vitória. Por outro lado, o *Crasher* realiza condutas que apresentam pouca ou nenhuma lógica, apenas direcionadas para causar problemas e provocar os outros. A intenção é ganhar visibilidade junto dos seus pares e mesmo das suas vítimas, geralmente assinando o seu ataque com um *nickname*, demonstrando o orgulho sentido pelo seu ato. Por fim, o *Thief* é considerado o tipo mais raro dentro dos *hackers*, o qual pode ser visto, acima de tudo, como um verdadeiro criminoso. A sua motivação é o lucro e o benefício financeiro indireto, onde o indivíduo acede e recolhe ilicitamente a informação de um determinado sistema informático e vende esses dados a outros indivíduos ou empresas. De acordo com os autores este é o *hacker* mais perigoso, dado que não dá qualquer sinal que navega nos sistemas computacionais e causa danos irreparáveis (Landreth & Rheingold, 1985).

Neste seguimento, Rogers (2006) concebe um modelo circumplexo bidimensional que retrata dois aspetos centrais: as habilidades tecnológicas e as motivações base dos indivíduos. Quanto ao primeiro, os conhecimentos dos *hackers* podem oscilar numa escala gradual, detendo mais ou menos habilidades técnicas. Relativamente ao segundo, o autor estipula quatro motivações principais: a) *curiosidade*, caraterizada pelo desejo de conhecimento, pela procura de sensações e pelo ganho intelectual; b) *notoriedade*, dirigida à visibilidade por parte dos

media e à fama ou estatuto; c) *vingança*, podendo ser direcionada contra uma empresa/instituição, uma pessoa singular e/ou uma nação; d) *financeira*, essencialmente tendo em vista o benefício monetário e a ganância.

Partindo destes dois critérios, Rogers (2006) estabelece uma taxonomia (*i.e.*, criação ou definição de classes com identidades delineadas) com nove classificações, orientada para a criação de uma realidade que corresponda à diversidade de *hackers* existente. Primeiramente, o autor aborda as tipologias *Novice*, *Cyber-Punks* e *Petty Thieves*, apresentando uma caraterização idêntica às categorias *Novice*, *Crasher* e *Thief* de Landreth e Rheingold (1985), respetivamente. Clarificando, a primeira tipologia age pela curiosidade e possui habilidades de programação e computação reduzidas. A segunda detém a motivação da notoriedade, e contém capacidades técnicas medianas. Já a terceira tipologia é movida pelo aspeto financeiro, conseguindo dominar alguns aspetos dos sistemas computacionais (Rogers, 2006).

A adicionar a estas, Rogers (2006) introduz a categoria *Internals*, sendo sujeitos com elevadas capacidades técnicas que exercem ou exerciam funções profissionais numa empresa. Estes, motivados por vingança, agem contra a instituição, violando a confiança da mesma. Outra tipologia é a *Old Guard*, constituída por *hackers* de primeira geração, movidos pela curiosidade e interesse nas tecnologias. Estes agregam habilidades técnicas soberbas, utilizando-as de forma ética e sem intenções maliciosas. Contudo, na visão do autor, estes apresentam, igualmente, um *"alarmante desrespeito pela propriedade pessoal dos outros"* (p. 99), dado que realizam um acesso não autorizado.

Ademais, Rogers (2006) retrata os *Professional Criminals*, sendo um tipo impulsionado pelo ganho financeiro e pela continuidade das condutas criminais. Geralmente são pessoas com elevadas habilidades informáticas, recrutadas por organizações criminosas. A categoria *Virus Writers* é constituída por indivíduos habilidosos em termos tecnológicos, dedicados especialmente à criação de vírus informáticos e ao esboço os seus *scripts* e guiões (Gordon, 2000). Estes atuam em grupo, apresentando essencialmente uma motivação vingativa (Rogers, 2006). Além desta, os *Information Warriors* são sujeitos altamente treinados e inteligentes, agindo com base no patriotismo. Estes trabalham para uma determinada nação e realizam atos para proteger o próprio sistema e, paralelamente, destruir os sistemas de outros países. Por fim, o autor somente refere a categoria *Political Activists*, não a caraterizando detalhadamente. Sobre esta, pode afirmar que se move pela vontade de ser reconhecida, possuindo capacidades tecnológicas acima da média.

Em 2010, o autor compila os escritos mencionados em sete categorias, descartando a *Internals* e a *Old Guard*. Seguindo a ordem apresentada anteriormente, as restantes tipologias passam a ser intituladas da seguinte forma: *Script Kiddies*; *Cyber-Punks*; *Thieves*; *Professionals*; *Virus Writers*; *Cyberterrorists*; *Hacktivists*. Os trabalhos de Rogers (2006, 2010) influenciaram, em grande medida, as tipologias futuras, como a de Meyers e colaboradores (2009), a de Hald e Pedersen (2012) e a de Seebruck (2015) que seguiram a mesma linha de pensamento.

Seebruck (2015) trata a natureza multidisciplinar dos *hackers* de forma igualitária a Rogers (2006, 2010), com o *Weighted Arc Circumplex Model*, onde representa as motivações e as capacidades técnicas e informáticas. Assim, Seebruck (2015) elenca cinco motivações que possam estar na base dos comportamentos, sendo as mesmas quatro de Rogers (2006), adicionando somente a *ideologia* (*i.e.,* ação por posição política ou religiosa). Conjugando os dois aspetos, o autor estipula por ordem crescente os seguintes tipos de *hackers*: 1) *Novices* – indivíduos que recorrem a técnicas básicas e simples pré-existentes na *internet*, sendo movidos pela mera curiosidade; 2) *Crowdsources* – não detêm capacidades sofisticadas, apenas movem esforços coletivos para executarem vingança; 3) *Punks* – são motivados pela excitação do ato desviante e pela vingança, podendo ter habilidades baixas a elevadas; 4) *Hacktivists* – possuem capacidades tecnológicas intermédias e agem segundo a ideologia política; 5) *Insiders* – indivíduos que atuam por vingança e lucro, possuindo capacidades medianas; 6) *Criminals* – agem por lucro financeiro advindo do crime, auxiliados por habilidades médio-altas; 7) *Coders* – são *hackers* não maliciosos que procuram prestígio no seu ato, conseguindo alcançar isto pelas suas capacidades elevadas; 8) *Cyber Warriors* – realizam ataques sofisticados com base na ideologia e no lucro financeiro (Seebruck, 2015).

Embora estas classificações sejam elucidativas e complexas, a tipologia mais disseminada na comunidade científica é a de Moore (2015), que, além das ideias dos autores supracitados, aborda os contornos da legalidade e da ética no *hacking*. O autor refere as categorias *Script Kiddies*, *Hactivists* e *Cyberterrorists*, apresentando a mesma caraterização que Landreth e Rheingold (1985), Rogers (2006, 2010) e Seebruck (2015). Adicionalmente, o seu trabalho destaca-se pela conceção de outras três tipologias designadas por: *Black-hat hackers*; *White-hat hackers*; *Gray-hat hackers*; servindo de alicerce a outras investigações científicas.

Os *Black-hat hackers* são *"um resumo de tudo o que o público receia num ataque criminal a um computador"* (Moore, 2015, p. 24), apresentando-se como a imagem que a sociedade tem de um *hacker*, personificando o medo que a mesma sente (Jaquet-Chiffelle &

Loi, 2020). Estes indivíduos situam-se na ilegalidade da lei, que, agindo com intenções maliciosas, invadem os computadores, as redes de segurança e os sistemas informáticos. O único propósito é destruir e danificar os mesmos, tirando partido das suas vulnerabilidades para obter benefício financeiro junto das empresas afetadas. Para tal, detêm um conhecimento informático e tecnológico desenvolvido, dominando-o (Moore, 2015).

A classificação *White-hat hackers* tem sustento nos escritos de Barber (2001), sendo o oposto do tipo mencionado previamente. Embora agregue igualmente sujeitos com habilidades elevadas, estes contam com um leque de valores éticos, situando-se no perímetro lícito da lei. De um modo geral, apresentam-se como *hackers* profissionais empregados numa empresa de segurança informática, com a finalidade de detetar fragilidades nos seus sistemas, corrigir as mesmas, e impedir a invasão dos *hackers* maliciosos (Barber, 2001; Moore, 2015). Paralelamente, podem executar as mesmas tarefas isoladamente, sem qualquer benefício financeiro, apenas com o propósito de alertar as empresas e modificar as falhas dos seus sistemas (Moore, 2015).

Por fim, os *Gray-hat hackers* localizam-se na divisória entre o que é considerado legal e ilegal. Estes abrangem caraterísticas dos grupos descritos anteriormente, nomeadamente a correção das vulnerabilidades dos sistemas informáticos empresariais dos *White-hat hackers*, mas a execução deste ato é efetuada a troco de uma recompensa ou ganho financeiro, como os *Black-hat hackers*. Derivado desta chantagem, esta tipologia é conhecida como oportunista, que embora não tenha uma intenção nociva, dá um uso questionável às suas capacidades de programação e conhecimento informático (Moore, 2015).

As linhas de trabalho supramencionadas continuam presentes nas estipulações mais recentes de tipologias de *hackers* (*e.g.,* Moeckel, 2019). Embora a categorização dos *hackers* consiga clarificar e desconstruir as ações destes indivíduos, reforça-se que os seres humanos são complexos e não unidimensionais (Rogers, 2010). Logo, estes podem pertencer a mais do que uma tipologia, movidos por diversas intenções (Ferreira & Guedes, 2021; Moeckel, 2019).

CAPÍTULO III – FUNDAMENTOS TEÓRICOS E EMPÍRICOS

A análise dos pressupostos que decompõem o *hacking* efetuada no capítulo anterior permite concluir que este é um fenómeno criminal complexo, que origina múltiplas e díspares perspetivas na comunidade científica. Mediante este facto, os esforços têm convergido para a procura de fatores de risco que possam explicar a prática destes comportamentos (Fox & Holt, 2021). Assim, as investigações científicas têm apostado na testagem e aplicação de racionais

teóricos à explicação destes comportamentos (*e.g.,* Teoria da Escolha Racional de Clarke & Cornish, 1985), com o intuito de aprofundar os conhecimentos que se detém (Fox & Holt, 2021; Sharma, 2007; Stalans & Donner, 2018).

Como tal, o presente capítulo apresenta o segundo foco desta investigação – os aspetos constituintes da Teoria Geral do Crime de Gottfredson e Hirschi (1990) e da Teoria da Aprendizagem Social de Akers (1998). A escolha destas teorizações é concordante com o desenvolvimento dos trabalhos teóricos e empíricos em torno do *hacking*, dado que a aplicabilidade destas duas teorias é dos tópicos mais abordados na explicação destes comportamentos criminais (Back *et al.*, 2018). Posto isto, expõem-se as premissas centrais de cada teoria, complementadas com os resultados empíricos advindos da sua aplicação às condutas de *hacking* malicioso.

3.1. Teorias Criminológicas

3.1.1. Teoria Geral do Crime

Na década de 90 inicia-se um período de desenvolvimento teórico na Criminologia, caraterizando-se como um contexto promissor à emergência de novas correntes. É neste momento que Gottfredson e Hirschi (1990) avançam com a sua teoria, intitulada de Teoria Geral do Crime (TGC), incluída, ao nível criminológico, nas teorias do controlo e laços sociais (Akers, 2012; Britt & Rocque, 2016). Nisto, contrariamente aos racionais clássicos, os autores questionam 'porque é que as pessoas não cometem crimes?', propondo que a ofensa criminal irá ocorrer, a menos que seja prevenida por fortes controlos sociais e pessoais (Akers, 2012).

A TGC é apresentada como uma teoria universal capaz de descrever e explicar o comportamento criminal e o ato desviante segundo o mesmo conjunto de pressupostos. Os autores quebram com a tradição clássica e reformulam o olhar dado ao crime e à sua concetualização, redirecionando o enfoque existente – o fenómeno criminal – para o indivíduo e as suas caraterísticas (Burt, 2020). Neste sentido, Gottfredson e Hirschi (1990) definem o crime como *"ato de força ou fraude, praticado na procura do interesse individual"* (p. 15), que se relaciona intrinsecamente com um determinado momento espácio-temporal.

Para os autores, a ofensa criminal relaciona-se com o conceito de autocontrolo, apresentado como o núcleo da teoria – uma caraterística intrínseca e individual central no cometimento de crime. Gottfredson e Hirschi (1990) concetualizam o autocontrolo como o indicador da propensão dos indivíduos para o comportamento criminal, dado que é através deste que as pessoas conseguem impedir, inibir e controlar os seus impulsos. Numa primeira

aproximação ao conceito, o autocontrolo reside na capacidade individual de evitar punições e obter recompensas, no qual o sujeito adota certos comportamentos neste sentido. Logo, os autores explicam que indivíduos com baixo autocontrolo agem de acordo com os seus desejos, não perspetivando as consequências tardias dos mesmos.

Gottfredson e Hirschi (1990) caraterizam o autocontrolo através de elementos que se relacionam com o comportamento criminal, designadamente: 1) gratificação imediata; 2) tarefa de execução fácil; 3) atividades físicas; 4) propensão para o risco; 5) autocentração; 6) baixa tolerância à frustração. Estas dimensões permitem fazer a associação entre o baixo nível de autocontrolo e o cometimento de atos criminais, uma vez que os indivíduos ao possuírem, em maior nível, certas vulnerabilidades, encontram-se mais propensos a envolverem-se em atos ilícitos (Gottfredson & Hirschi, 1990).

Segundo os autores, as pessoas pretendem satisfazer os seus desejos, todavia a tomada de decisão varia consoante os níveis de autocontrolo. Explicam que pessoas com baixos níveis de autocontrolo caraterizam-se por *"responderem a um estímulo ambiental que fornece recompensas instantâneas"* (p. 89), independentemente das consequências que possam advir. Um desses estímulos é a criminalidade, sendo uma ação que oferece regalias imediatas. Tal não acontece com pessoas com altos níveis de autocontrolo. Ademais, indivíduos com baixos níveis de autocontrolo não são dotados de tenacidade ao longo da vida, resultando no pobre planeamento futuro e mínimas capacidades cognitivas. Assim, tendem a preferir atividades físicas em detrimento de circunstâncias que exijam raciocínio e pensamento. Estes fatores ampliam a probabilidade destes indivíduos se envolverem na criminalidade, dado que é considerada um caminho fácil, rápido e físico na obtenção de recompensas. Nestes sujeitos observa-se, igualmente, a seleção de situações relacionadas com o risco e o perigo, no qual apresentam uma propensão para o envolvimento em comportamentos que ofereçam excitação e emoção, tal como o crime e/ou comportamentos antissociais (*e.g.,* consumo de substâncias ilícitas). Com este tipo de ações os indivíduos obtêm a gratificação que pretendem, saciando um dos seus muitos desejos.

Em função desta última questão, Gottfredson e Hirschi (1990) descrevem os indivíduos com baixos níveis de autocontrolo como *"autocentrados, indiferentes ou insensíveis ao sofrimento e necessidades dos outros"* (p. 89). Este aspeto conecta com a dor e o desconforto da vítima advindo do evento criminal, daí estes indivíduos não terem dificuldade em envolver-se neste tipo de comportamentos. Neste seguimento, apresentam uma tolerância mínima à frustração e uma fraca capacidade de criação de resposta verbal e argumentativa, originando o

confronto físico e violento, ou seja, o crime. Este, além de dar o benefício abordado previamente, oferece um alívio à irritação momentânea que a pessoa sente.

Clarificando os elementos expostos, 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).

Ademais, salienta-se que além dos elementos, o conceito de autocontrolo pauta-se pela ideia de versatilidade e continuidade. Por versatilidade, os autores entendem que os ofensores não possuem uma inclinação para um crime específico (*e.g.,* roubo, violação sexual ou homicídio), mas antes o cometimento de uma multiplicidade de atos criminais e desviantes, dado que os indivíduos com baixo autocontrolo não possuem a capacidade de resistir às tentações do meio. Referente à noção de estabilidade, de acordo com a teoria, os níveis de autocontrolo estabelecem-se num período precoce da vida do indivíduo. Assim, as diferenças encontradas entre os indivíduos que apresentam níveis mais elevados de autocontrolo face aos níveis mais baixos estabelecem-se precocemente e persistem ao longo do tempo (Gottfredson & Hirschi, 1990).

Tendo em conta esta caraterização do conceito de autocontrolo, os autores esclarecem que o mesmo não deve ser entendido como uma componente que está ou não presente, mas antes algo que se expressa numa escala gradual, capaz de assumir múltiplas posições. Defendem que os indivíduos não estão determinados a delinquir somente por manifestarem um baixo nível de autocontrolo, uma vez que na visão dos autores o comportamento criminal resulta da fusão entre os baixos níveis de autocontrolo e as oportunidades existentes no meio social envolvente.

Nesta linha de pensamento, Gottfredson e Hirschi (1990) *"procuram as causas do autocontrolo (...) onde o sistema pode correr mal"* (p. 98), atribuindo especial relevo ao papel da família e da educação da criança, mais concretamente às fragilidades e falhas que a supervisão parental pode assumir. A supervisão parental é considerada adequada quando os educadores forem capazes de reconhecer comportamentos criminais e desviantes, para, consequentemente, prevenirem o envolvimento da criança em tais atos. Deste modo, a criança é efetivamente socializada quando está reunido o seguinte conjunto de condições: monitorização das condutas da criança, reconhecimento do comportamento desviante e punição do mesmo. Ao existirem estes aspetos, a criança dever-se-á capaz de adiar a gratificação, desenvolver empatia e sensibilidade aos interesses dos outros, resolver os seus conflitos por

argumentos verbais e recorrer menos à violência. Contudo, ocorrem falhas no processo de socialização, situadas no contexto familiar (Gottfredson & Hirschi, 1990).

Pelos pressupostos expostos pelos autores, o baixo autocontrolo tem um lugar estável e persistente na vida do indivíduo, sendo solidificado pelo papel desempenhado pelos educadores nos primeiros anos de vida de uma criança. De acordo com LeBlanc (2006), o conceito de autocontrolo de Gottfredson e Hirschi (1990) advém, essencialmente, de uma concetualização de índole comportamental, no qual os atos que indicam o nível de autocontrolo são os mesmo que o autocontrolo pretende explicar. Esta posição é vista pela comunidade científica como uma tautologia, uma vez que o baixo autocontrolo é usado como preditor do envolvimento no crime, e este preditor é, igualmente, usado como indicador de baixo autocontrolo (Arneklev *et al.,* 2006).

3.1.2. Teoria da Aprendizagem Social

A Teoria da Aprendizagem Social (TAS) é proposta por Akers (1998) como um racional teórico capaz de explicar o cometimento de comportamentos criminais e desviantes, à semelhança da teoria de Gottfredson e Hirschi (1990). Todavia, a abordagem deste autor é díspar comparativamente à proposição do papel do autocontrolo, uma vez que o objetivo principal passaria pela ligação entre os princípios gerais da psicologia comportamental com os nove elementos propostos por Sutherland (1947) na Teoria da Associação Diferencial (Akers & Jennings, 2016).

Neste contexto, Burgess e Akers (1966) focam-se, essencialmente, numa das premissas elencadas por Sutherland (1947), no qual o comportamento, seja normativo ou desviante, é aprendido num processo inerente a um contexto situacional, a interações e à estrutura social. Ademais, a propensão para o crime e o desvio, advinda do processo de aprendizagem social, apresenta variações ao nível inter-individual (*i.e.,* entre indivíduos) e intra-individual (*i.e.,* no mesmo indivíduo). Isto permite analisar o decurso da aprendizagem nas diferentes fases desenvolvimentais do sujeito, percebendo a influência das circunstâncias sociais na tendência para o envolvimento nestes comportamentos (Akers, 2010).

Proveniente das ideias de Sutherland (1947), os autores listam sete pressupostos caraterizadores do processo de aprendizagem. Contudo, estes foram recebidos com criticismo por parte da comunidade científica, originando uma modificação e refinamento teórico, no qual o esforço de Akers se distanciou destas listagens de princípios anteriormente criadas (Akers & Jennings, 2016). Posto isto, Akers (1998) propõe o núcleo do processo de aprendizagem social, sendo este constituído por quatro elementos teóricos: 1) associação diferencial; 2) reforço

diferencial; 3) imitação; 4) definições. O autor adianta que a probabilidade de o comportamento normativo ou desviante ocorrer, depende da forma como estas componentes agem e operam no processo de aprendizagem (Akers, 2010).

Relativamente ao conceito de *Associação Diferencial*, este corresponde à interação direta que o indivíduo tem com os seus grupos mais próximos ou íntimos, nomeadamente o grupo primário (*e.g.,* a família, o grupo de pares) e o grupo secundário (*e.g.,* as figuras da comunidade, os *media*). A consideração de proximidade e significância que o sujeito tem face a estas figuras varia consoante a sua fase desenvolvimental, na medida em que a família representa um papel de relevo na infância, porém, é substituída, gradualmente, pela escola e pelo grupo de pares no período da adolescência. Assim, é nesta associação com os outros, com os seus valores e atitudes, sejam normativos ou desviantes, que os indivíduos aprendem e retêm os padrões comportamentais expostos pelo grupo, acionando os mecanismos em que o processo de aprendizagem social opera (Akers, 2010; Akers & Jennings, 2016). Ademais, a associação diferencial varia consoante as seguintes modalidades: frequência (*i.e.,* quão frequente é a interação do sujeito com o grupo proximal); duração (*i.e.,* tempo despendido na interação); prioridade (*i.e.,* ocorrência da interação numa fase precoce da vida do sujeito); intensidade (*i.e.,* significância, saliência e importância que o sujeito atribui à interação). Akers (2010) explica este pressuposto, no qual *"as associações que ocorram cedo (prioridade), durem mais e ocupem mais tempo (duração), ocorram mais frequentemente (frequência) e envolvam outros com quem se tem relações mais importantes (intensidade), vão ter mais efeito no comportamento criminal ou na conformidade com a lei."* (p. 64).

O *Reforço Diferencial* relaciona-se com a perceção, experiência e antecipação de uma recompensa ou punição, que por sua vez acompanha determinado comportamento. Este elemento opera na presença de um estímulo, interno ou externo, desencadeando uma resposta automática por parte do indivíduo. Face a isto, o reforço pretende aumentar a realização de tal comportamento, sendo para isso utilizado o reforço positivo (*i.e.,* repetição do comportamento com o intuito de obter uma recompensa ou reação aprovativa) e/ou reforço negativo (*i.e.,* repetição do comportamento para evitar sensações ou eventos aversivos). À semelhança do elemento anterior, o reforço diferencial varia em termos de quantidade, frequência e probabilidade, sendo que quanto maior for a própria recompensa ao comportamento, a frequência da recompensa e a chance de o indivíduo ser recompensado, mais provável é a ocorrência do comportamento (Akers, 2010).

A componente *Imitação* é recuperada do conceito de reforço vicariante de Bandura (1979), no qual os indivíduos *"observam diretamente os comportamentos realizados pelos outros, incluindo as suas consequências"* (Akers & Jennings, 2016, p. 234). A observação das ações dos grupos íntimos, juntamente com a receção do reforço, leva o indivíduo a assimilar e a processar a sucessão entre comportamento e consequência. Neste seguimento, observar alguém próximo a cometer um crime ou ato desviante e ter uma consequência positiva, aumenta a probabilidade do indivíduo se envolver no mesmo comportamento, imitando-o. Salienta-se que Akers (2010) defende que a imitação, por si só, não tem um papel determinante, uma vez que se encontra sempre dependente dos outros mecanismos de aprendizagem.

Por último, as *Definições* são sustentadas teoricamente pelo trabalho de Sutherland (1947), elucidadas pelo autor como o conjunto de orientações, motivos, racionalizações e atitudes em torno da criminalidade ou normatividade, que as rotulam como certas ou erradas, desejáveis ou indesejáveis. Akers (2010) simplifica esta questão, traduzindo o conceito em significados relacionados com os comportamentos, podendo estes serem favoráveis ou desfavoráveis a essa ação ou situação. O autor explica que as definições se expressam de forma geral (*i.e.,* visão que abrange um conjunto de comportamentos) ou de forma específica (*i.e.,* visão orientada para atos concretos). Com especial relevo, aborda as definições favoráveis ao crime, podendo ser positivas – crenças que tornam o comportamento desejável – ou neutralizadoras – justificações para determinado comportamento – recuperando as ideias de Sykes & Matza (1957). A perceção que o sujeito tem de determinada conduta, seja criminal ou normativa, baseia-se na racionalização do próprio indivíduo e, igualmente, nas racionalizações a que este é expostos no processo de socialização (Akers, 2010).

Integrando os pressupostos abordados, pode afirmar-se que o comportamento é aprendido junto dos grupos íntimos, que permitem reforçar esse comportamento, bem como as próprias definições pertencentes ao indivíduo. Neste contexto, pela observação dos outros, o sujeito começa a imitar e a adotar comportamentos semelhantes (Akers, 2010; Akers & Jennings, 2016).

3.2. Evidência Empírica

A aplicabilidade da TGC e da TAS na explicação do *hacking* malicioso tem sido analisada em grande escala ao nível empírico, tendo sempre como suporte os alicerces teóricos expostos previamente (Holt *et al.*, 2012; Winfree Jr. & Abadinsky, 2017). Embora na Criminologia esta seja uma área subdesenvolvida quando comparada a outros tópicos de

análise, as investigações existentes fornecem resultados esclarecedores quanto aos preditores do *hacking* malicioso. De seguida apresentam-se os principais resultados empíricos relativos à relação existente entre os comportamentos maliciosos, o autocontrolo e os elementos da aprendizagem social.

3.2.1. Análise da Teoria Geral do Crime

Relativamente ao relevo prático dos pressupostos da TGC na explicação do *hacking* malicioso, este tem sido demonstrado em alguns estudos que pretendem perceber a relação entre o autocontrolo e diversos comportamentos cibercriminais. Frisa-se que o autocontrolo se apresenta como um dos correlatos mais influentes no crime tradicional (*e.g.,* Pratt & Cullen, 2000) e nas diferentes formas de cibercrime (*e.g.,* Donner *et al.*, 2014).

Ao nível internacional, Holt e Steinmetz (2021), com uma amostra de 48.825 alunos de diversos países, mediram as variáveis de autocontrolo e de *hacking* com o objetivo de testarem a aplicabilidade da teoria de Gottfredson e Hirschi (1990). Os autores mediram o *hacking* questionando sobre a sua perpretação nos últimos 12 meses[2], e o autocontrolo através de 12 dos 24 itens da Escala de Grasmick *et al*. (1993). Os resultados obtidos traduzem uma relação negativa e forte entre o autocontrolo e a prática de *hacking* malicioso. Mais concretamente, o baixo autocontrolo aparece como um preditor significativo na explicação desses comportamentos. Utilizando a mesma forma de operacionalização das variáveis, Back *et al.* (2018) recorreram aos participantes do *Second International Self-Report Delinquency Study*, no qual em 18.985 sujeitos, os que tinham baixos níveis de autocontrolo apresentavam 80% de probabilidade de se envolverem em atos de *hacking* malicioso. Este dado foi transversal aos diversos países presentes no estudo. Ainda à escala mundial, Udris (2016) corrobora os resultados dos estudos anteriores.

Adicionalmente, investigações com a mesma finalidade dispõem de resultados similares. Nos Estados Unidos, as investigações com estudantes universitários têm constatado que o baixo autocontrolo aparece como um preditor dos atos de acesso e de utilização não autorizada a computadores (Donner *et al.,* 2014), nomeadamente relacionado com a entrada não autorizada a contas *Facebook* de outrem e a um *website* (Marcum *et al.*, 2014). Na Coreia do Sul, Moon e colegas (2010) com um estudo longitudinal, encontraram que participantes que reportavam níveis mais baixos de autocontrolo tinham mais probabilidade de cometer *hacking* malicioso.

[2] Salienta-se que a questão destinada a medir o cometimento de *hacking* não continha nenhuma nota ou informação sobre uma definição do comportamento (Holt & Steinmetz, 2021).

Por sua vez, na Austrália destaca-se o estudo de Holt *et al.* (2021), que operacionaliza o *hacking* malicioso de forma mais complexa. Esta variável foi medida pelo posicionamento dos participantes numa escala de *Likert* de 1 (nunca) a 6 (várias vezes ao dia) relativamente ao envolvimento em certos atos maliciosos nos últimos 12 meses (*e.g.,* aceder ao dispositivo de outra pessoa sem a sua permissão para obter informações, fotos, vídeos ou outros ficheiros; adicionar, eliminar ou alterar informação ou ficheiros no dispositivo de outra pessoa sem o seu conhecimento). Embora os autores tenham subdividido o *hacking*, todas as formas se encontraram relacionadas com o baixo autocontrolo.

Posto isto, os dados obtidos pelas diversas investigações suportam a hipótese da teoria, no qual o baixo autocontrolo aparece como um preditor relevante para o cometimento de *hacking* malicioso. Analisando esta relação, pode-se concluir que estes indivíduos possuem uma menor resistência à tentação apresentada pelo ilícito criminal e acabam por aproveitar a oportunidade de obter recompensas imediatas (Bossler & Burruss, 2011). Ademais, tais como Gottfredson e Hirschi (1990) deduzem, o criminoso é alguém que procura a aventura e o risco, sendo refletido na vontade dos *hackers* em realizarem atos que forneçam estímulo e excitação, todavia, no contexto *online* (Taylor *et al.,* 2014).

Contudo, alguns estudos empíricos têm obtido resultados divergentes, onde a relação entre o autocontrolo e o *hacking* malicioso é positiva (*i.e.,* indivíduos com níveis mais elevados de autocontrolo apresentam mais probabilidade de cometer atos de *hacking* malicioso). A investigação de Holt e Kilger (2008) é um destes exemplos, que contando com a participação de 54 indivíduos licenciados e/ou mestres nas áreas de *software*, sistemas de informação e informática, obteve uma relação significativa entre os comportamentos de *hacking* malicioso e níveis de autocontrolo mais elevados. Pelas palavras dos autores, este resultado pode refletir *"os traços gerais necessários para se tornar um hacker qualificado, incluindo a capacidade de aprendizagem, de diligência e de ponderação"* (p. 76), ou seja, este tipo de amostra possui a cognição e a capacidade de planeamento – caraterísticas associadas aos elevados níveis de autocontrolo (Gottfredson & Hirschi, 1990). Resultados similares são encontrados por Bossler e Burruss (2011).

Embora os dados mencionados sejam inconsistentes com o perfil criminal traçado por Gottfredson e Hirschi (1990), estes fornecem *insights* importantes a ter em consideração na análise da relação entre as variáveis, no qual o tipo de amostra, a forma de *hacking* examinada e o seu nível de sofisticação informática pode ter influência nos níveis de autocontrolo obtidos nos estudos (Bossler & Burruss, 2011). Por exemplo, formas menos sofisticadas de *hacking*

(*e.g., download* de um vírus; tentar adivinhar uma *password*) fornecem uma gratificação fácil e imediata (Taylor *et al.,* 2014), sendo associadas a níveis mais baixos de autocontrolo e semelhante ao perfil criminoso apresentado por Gottfredson e Hirschi (1990).

Ademais, em alguns estudos o autocontrolo não aparece como uma variável explicativa consistente e significativa, especialmente quando é inserida uma terceira variável no modelo de análise (*e.g.,* Marcum *et al.,* 2014; Nodeland & Morris, 2020).

3.2.2. Análise da Teoria da Aprendizagem Social

A capacidade de explicação da TAS na cibercriminalidade tem sido um dos aspetos a avaliar por parte da comunidade científica. Unanimemente, as componentes da teoria são reconhecidas como preditores robustos de diversas formas de cibercrime, incluindo o *cyberbullying* (*e.g.,* Holt *et al.*, 2012; Shadmanfaat *et al.*, 2020), a pirataria digital (*e.g.,* Gunter, 2008; Higgins *et al.*, 2006) e o *hacking* (*e.g.,* Holt *et al.*, 2010; Miller & Morris, 2016).

No que concerne ao foco desta investigação, o estudo que deu impulso ao desenvolvimento empírico da temática do *hacking* malicioso foi o de Skinner e Fream, de 1997. Os autores recolheram dados de 581 alunos universitários com o intuito de testar os pressupostos da teoria nos seguintes comportamentos: 1) adivinhar ou tentar adivinhar *passwords* para aceder ao computador de outrem; 2) aceder ao computador de outra pessoa sem a sua autorização; 3) adicionar, eliminar, alterar ou imprimir informação de um computador sem autorização; 4) criar ou utilizar um *malware*. Esta variável foi medida numa escala de *Likert* de 5 itens relativamente ao envolvimento dos participantes nestes atos durante a vida e nos últimos 12 meses.

Quanto à variável independente, a aprendizagem social foi operacionalizada consoante as dimensões que decompõem o construto, designadamente, a associação diferencial, as definições, a imitação e o reforço diferencial. Para medir a associação diferencial, os autores questionaram os participantes sobre o envolvimento dos seus pares nos comportamentos de *hacking* malicioso, no qual tinham de se posicionar numa escala de *Likert* de 0 (‘nenhum amigo’) a 4 (‘todos os amigos’). Relativamente às definições foi pedido aos indivíduos para discordarem ou concordarem de um conjunto de preposições relativas à cibercriminalidade (*e.g.,* aspeto legal, acesso a informação e ficheiros, entrada ilegal em computadores). Quanto à imitação, esta foi medida pela aprendizagem de *hacking* com diversas fontes de conhecimento (*e.g.,* família, computador, livros), no qual foi apresentada uma escala de *Likert* de 1 (‘não aprendi nada’) a 5 (‘aprendi tudo’). Por fim, o reforço diferencial foi medido pela posição dos

indivíduos face à probabilidade de serem apanhados a aceder a um computador sem autorização, e por quão severa seria a punição caso fossem apanhados.

O principal achado desta investigação é o suporte moderado que as quatro dimensões da TAS concedem à explicação do cometimento de *hacking* malicioso, sendo proeminente o papel da associação diferencial e das definições favoráveis ao crime (Skinner & Fream, 1997). Como mencionado previamente, estes esforços serviram de base para os trabalhos que se seguiram, tanto para a estipulação dos objetivos do estudo, como para a própria metodologia e operacionalização das variáveis (Rogers, 2001).

Neste ponto destaca-se a investigação empírica de Bossler e Burruss (2011), na qual participaram 566 alunos universitários. Os autores concluíram que o processo de aprendizagem social relevou-se ser um forte preditor da prática de *hacking* malicioso. Explicam que para se cometer estes comportamentos *"a maioria dos indivíduos necessita de se associar com outros hackers, aprender os seus valores e ser reforçado socialmente neste domínio"* (Bossler & Burruss, 2011, p. 57).

Mediante estes resultados pode afirmar-se que durante as últimas duas décadas a comunidade científica tem agregado informação concordante relativamente aos efeitos das componentes da aprendizagem social. Semelhante ao que ocorre com o crime tradicional, o cometimento de *hacking* malicioso é impulsionado em grande medida pela presença e influência de pares desviantes, sejam estes *online* ou *offline* (Bossler & Burruss, 2011). Diversos estudos concluem que os indivíduos que detêm uma rede de amigos envolvida nesses comportamentos, ou noutros atos ciberdesviantes, apresentam mais probabilidade de praticar *hacking* (*e.g.,* Bossler & Burruss, 2011; Holt *et al.,* 2010; Morris & Blackburn, 2009; Rogers, 2001, Young & Zhang, 2005). Além destes dados, outra componente relevante é a existência de definições favoráveis ao crime. Estas são elencadas como um dos preditores significativos para a cibercriminalidade, dado que os valores, ideias e justificações dos indivíduos são concordantes com esse estilo de vida (Bossler & Burruss, 2011; Holt *et al.,* 2010; Morris & Blackburn, 2009; Rogers, 2001).

Pelos resultados advindos dos estudos empíricos compreende-se que estas duas componentes se destacam na explicação do *hacking* malicioso, e que, por outro lado, embora a imitação e o reforço diferencial apresentem uma relação positiva, esta carateriza-se por ser fraca e não significativa (Hollinger, 1992; Skinner & Fream, 1997; Morris & Blackburn, 2009).

3.2.3. Análise Conjunta da TGC e da TAS

O papel individual de cada racional teórico na explicação do *hacking* malicioso tem sido reconhecido e comprovado, embora na última década a comunidade científica tenha convergido para uma análise conjunta das variáveis mencionadas. O trabalho tem sido direcionado para uma integração teórica, de modo a produzir um entendimento mais completo e multifacetado (Bossler & Burruss, 2011; Maimon & Louderback, 2019; Stalans & Donner, 2018).

Holt e a sua equipa de investigadores (2012) conduziu um estudo (*n*= 435 alunos) com a finalidade de explorar a interação entre o autocontrolo, a associação a pares desviantes e as diversas formas de cibercrime, onde incluiu o *hacking*. A medição das variáveis em causa encontra similaridades com o estudo de Holt e Steinmetz (2021) e de Skinner e Fream (1997). À semelhança de estudos abordados previamente, os resultados obtidos confirmam o papel preditivo isolado do baixo autocontrolo e da associação a pares desviantes na elucidação da prática de *hacking* malicioso. Esta pesquisa aborda uma análise integrada das variáveis, agregadas num único modelo estatístico. Desta feita, concluem que embora o baixo autocontrolo possa ser considerado um preditor, esta relação alcança uma maior magnitude quando a associação a pares desviantes está presente. Ou seja, pela visão dos autores, esta última variável exacerba e medeia o efeito do baixo autocontrolo no *hacking* malicioso, uma vez que a probabilidade de explicação duplica quando se insere a componente da aprendizagem social. Assim, afirmam que a análise deste cibercrime deve ser feita pela utilização conjunta das variáveis (Holt *et al.,* 2012).

Os resultados referidos foram igualmente encontrados no estudo de Marcum e colegas (2014), no qual a relação entre o autocontrolo e o cometimento de *hacking* malicioso era significativa quando os indivíduos tinham como redes de pares, amigos que se envolviam nestes comportamentos. Neste seguimento, enfatiza-se o estudo de Bossler e Burruss (2011), no qual os autores concluíram que os indivíduos com baixo autocontrolo se associavam a outros *hackers* para aprenderem as técnicas e os valores necessários à prática de *hacking* malicioso. Todavia, quando controladas as componentes da aprendizagem social, *"os indivíduos que não se associavam a outros hackers (...) requeriam níveis elevados de autocontrolo para serem capazes de aprender por si próprios a cometer estas ofensas"* (Bossler & Burruss, 2011, p. 59).

Na mesma linha de investigação emergem resultados anuentes, contudo com uma nova interpretação da relação entre as variáveis. Nodeland e Morris (2020), contando com uma amostra de 428 universitários, verificaram que os dados não demonstram uma relação direta entre o autocontrolo e os atos de *hacking* malicioso, mas antes um papel moderador desta

variável independente. Para os autores, a relação entre as componentes do processo de aprendizagem e o *hacking* é moderada pelo autocontrolo, no qual explicam que um indivíduo com definições favoráveis ao crime, caso tenha níveis elevados de autocontrolo, a probabilidade de praticar *hacking* diminui. Algo idêntico acontece com a associação a pares desviantes, que apesar do indivíduo estar neste meio, caso tenha um grau mais elevado de autocontrolo, encontra-se menos propenso para se envolver neste cibercrime.

Posto isto, as investigações elencadas providenciam um *insight* fundamental para a análise da relação entre o autocontrolo, o *hacking* malicioso e a aprendizagem social. Compreende-se que têm sido obtidos resultados mistos e incertos, especialmente quando está presente o autocontrolo, dado que tanto *scores* mais baixos como elevados têm sido associados à explicação do *hacking* malicioso (Bossler & Burruss, 2011). Posto isto, conclui-se que é transversal a importância de realizar uma análise combinada e conjunta das teorias, dado que só assim se alcança uma imagem geral da explicação do fenómeno. Este pressuposto é evidenciado por Stalans e Donner (2018) no qual recomendam

> *"(...) a criação – e a testagem – integrada de teorias, com base nos conceitos teóricos que já foram identificados como preditores consistentes do cibercrime (e.g., aprendizagem social, baixo autocontrolo) (...) Só assim teremos uma compreensão mais completa do motivo pelo qual as pessoas se envolvem em comportamentos desviantes como o hacking (...)"* (p. 40).

CAPÍTULO IV – ESTUDO EMPÍRICO

4.1. Metodologia

O presente capítulo destina-se à apresentação do estudo empírico conduzido no âmbito da dissertação. Em concreto, serão elencados os objetivos gerais e específicos, bem como as hipóteses que orientaram a investigação. Adicionalmente, descrevem-se as caraterísticas do estudo, nomeadamente o seu *design*, a constituição amostral, a construção do instrumento de recolha de dados (questionário) e respetiva operacionalização das medidas. Por fim, apresentam-se os procedimentos de recolha de dados e os procedimentos analíticos executados.

4.1.1. Objetivos Gerais e Específicos

No seguimento da informação exposta nos capítulos anteriores, a presente investigação tem como *objetivo geral* analisar o papel da TGC e da TAS na explicação da prática de *hacking* malicioso. Como corolário deste, emergem os seguintes *objetivos específicos*:

a) Testar a aplicabilidade da TGC e da TAS na explicação da prática de *hacking* malicioso;

b) Explorar a relação entre o autocontrolo e a prática de *hacking* malicioso;

c) Explorar a relação entre as quatro componentes da aprendizagem social e a prática de *hacking* malicioso;

d) Analisar a relação indireta entre as variáveis – autocontrolo, associação diferencial e prática de *hacking* malicioso – recorrendo a modelos de mediação;

4.1.2. Hipóteses de Investigação

Com base nas teorias e investigação prévia abordadas no capítulo anterior, bem como nos objetivos formulados, delineia-se o seguinte conjunto de *hipóteses de investigação* a testar:

H1: Indivíduos com níveis mais baixos de autocontrolo são mais propensos a praticar *hacking* malicioso;

H2: Existe uma relação positiva entre a associação a pares desviantes e a prática de *hacking* malicioso;

H3: Não existe uma relação significativa entre o reforço diferencial e a prática de *hacking* malicioso;

H4: Indivíduos com mais definições favoráveis ao crime praticam mais comportamentos de *hacking* malicioso;

H5: A relação existente entre o autocontrolo e a prática de *hacking* malicioso é mediada pela associação a pares desviantes.

4.2. Desenho de Investigação

A presente investigação é de índole quantitativa, na medida em que se procedeu à utilização de um questionário para efetuar a recolha de dados com vista a atingir os objetivos delineados e a testar o conjunto de hipóteses de investigação (Creswell & Creswell, 2017; Munck & Verkuilen, 2005). O estudo detém um caráter correlacional e transversal, dado somente se observar e medir as variáveis, sem manipulação experimental, e a recolha de dados ser efetuada num único momento temporal. Ademais, pode afirmar-se que é uma investigação explicativa, sendo que procura elucidar, de forma parcial, a prática de *hacking* malicioso, examinando a sua potencial associação com o autocontrolo e com as componentes da aprendizagem social, contribuindo, assim, para o conhecimento científico do fenómeno (Marôco, 2010).

4.3. Constituição da Amostra

A amostra total deste estudo é composta por 680 indivíduos que responderam ao questionário aplicado *online*. Primeiramente, foi enviado por *e-mail* o pedido de colaboração no estudo para diversas entidades das áreas da engenharia da tecnologia, da informática e da programação (universidades, faculdades, institutos politécnicos, escolas profissionais e empresas). No seguimento, a amostra foi constituída em dois momentos principais. Num primeiro momento, pelos indivíduos pertencentes às instituições que responderam espontânea e positivamente ao pedido de colaboração no estudo. Num segundo momento, devido à ausência de resposta por parte da maioria das entidades com que se pretendia colaborar, realizou-se um *follow-up* dos pedidos enviados, de modo a obter algum tipo de resposta. Neste segundo contacto frisou-se que a disseminação do questionário poderia estender-se a alunos e docentes de outras áreas de conhecimento, dado que algumas faculdades colocaram entraves a uma recolha de dados cingida a indivíduos da área das TIC.

Relativamente ao método de constituição da amostra, este foi do tipo não probabilístico, dado que não se pode afirmar que cada elemento teve a mesma probabilidade de ser incluído na amostra, face à população geral. Para além disso, tratou-se de uma amostragem por conveniência, em virtude de se ter selecionado um conjunto de indivíduos pela sua maior acessibilidade e disponibilidade no momento da investigação (Marôco, 2010).

4.4. Operacionalização do Instrumento e das Medidas

Como mencionado previamente, optou-se pela elaboração de um questionário para se proceder à recolha de dados, sendo este construído na plataforma *LimeSurvey*. O instrumento utilizado é constituído por um conjunto de variáveis que permite materializar os objetivos de investigação e testar as hipóteses formuladas.

Antes da apresentação do instrumento, propriamente dito, importa referir que a primeira página do questionário se destinou à obtenção do consentimento informado dos indivíduos. Assim, antes de acederem ao questionário, os participantes foram informados dos objetivos do estudo, da forma como decorreria a sua participação e da voluntariedade da mesma, assim como do seu anonimato e da confidencialidade dos dados (Maxfield & Babbie, 2014). Apenas os indivíduos que consentiram a sua participação, de forma informada, tiveram acesso ao questionário.

Posto isto, seguidamente descrevem-se os diferentes grupos de variáveis incluídos no questionário e a forma como cada variável foi operacionalizada. Em concreto, o questionário

subdivide-se nos seguintes grupos: i) dados sociodemográficos; ii) comportamentos de *hacking* malicioso; iii) componentes da aprendizagem social; iv) autocontrolo; v) desejabilidade social (cf. Anexo I e II). A descrição da forma como cada variável foi operacionalizada estruturar-se-á por cada um destes grupos.

Grupo I – Aspetos Sociodemográficos

A primeira parte do questionário refere-se à recolha de dados pessoais, tendo como principal objetivo fornecer informação para descrever e caraterizar a amostra em estudo (Field, 2013; Pallant, 2016). Relativamente ao *género*, este foi medido enquanto variável nominal (0= feminino; 1=masculino; 2=outro), a *idade* foi mensurada em anos, sendo uma variável quantitativa, e o *estado civil* foi medido como variável nominal (1=solteiro/a; 2=união de facto; 3=casado/a; 4=ex-união de facto; 5=divorciado/a; 6=viúvo/a; 7=outro). Quanto às *habilitações literárias*, a questão foi subdivida em habilitações concluídas (1=4.º ano; 2=6.º ano; 3=9.º ano; 4=12.º ano; 5=curso profissional; 6=licenciatura; 7=pós-graduação; 8=mestrado; 9=doutoramento) e em habilitações a frequentar (mantiveram-se as opções das habilitações concluídas, adicionando somente a opção 'nenhuma').

Quanto à *situação profissional*, os participantes posicionaram-se nas seguintes opções: 1=desempregado/a; 2=empregado/a por conta própria; 3=empregado/a por conta de outrem; 4=estudante; 5=trabalhador-estudante; 6=reformado/a; 7=outro. Esta foi complementada com uma questão de filtro, referente a trabalhar ou estudar na área das *TIC*, sendo uma variável binária (0=não; 1=sim). Por fim, foi pedido aos respondentes para indicarem o seu nível de *conhecimento informático*, uma variável ordinal de 5 opções (1=baixo; 2=médio-baixo; 3=médio; 4=médio-alto; 5=alto).

Grupo II – Comportamentos de *Hacking Malicioso*

O segundo grupo é constituído por perguntas relacionadas com uma das variáveis centrais em estudo – o *hacking malicioso* – caraterizando-se por ser a variável dependente. Neste grupo foram colocadas questões relativas ao cometimento de comportamentos de *hacking* malicioso, incidindo em dois períodos temporais: durante a vida do indivíduo e nos últimos 12 meses. Ademais, foi apresentada uma questão referente à idade aproximada em que o participante se envolveu nos comportamentos mencionados e uma outra questão referente à imitação desses comportamentos. Seguidamente apresenta-se, de um modo mais detalhado, cada uma destas variáveis.

a) Prática dos comportamentos de *hacking malicioso*

É possível constatar diferentes formas de medição dos comportamentos de *hacking* malicioso entre a comunidade científica. Por um lado, existe um conjunto de estudos empíricos que trata a variável como dicotómica (*e.g.,* Back *et al.,* 2018; Fox & Holt, 2021; Holt & Steinmetz, 2021). Por outro lado, algumas investigações operacionalizam-na através de uma escala de *Likert* (*e.g.,* Donner *et al.,* 2014; Holt *et al.,* 2010; Marcum *et al.,* 2014). No presente estudo, optou-se por esta última forma de operacionalização, de modo a obter informação mais detalhada sobre a prática destes comportamentos e ter a possibilidade de tratar a variável de diferentes formas após a recolha dos dados.

Assim, com base em estudos científicos prévios (*e.g.,* Bossler & Burruss, 2011; Donner *et al.,* 2014; Holt *et al.,* 2010; Holt *et al.,* 2012; Holt *et al.,* 2021; Skinner & Fream, 1997), foi criada uma escala de comportamentos de *hacking* malicioso, agregando os seguintes atos: 1) adivinhei ou tentei adivinhar *passwords* para aceder a um computador ou conta *online* de outra pessoa sem autorização; 2) acedi a um computador ou conta *online* de outra pessoa sem autorização; 3) adicionei, eliminei, alterei ou imprimi informação de um computador ou conta *online* de outra pessoa sem autorização; 4) usei um *malware* para causar danos ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, *worms*); 5) criei um *malware* para causar danos ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, *worms*). Os comportamentos elencados variam, de um modo crescente, em dificuldade técnica, permitindo analisar a prática dos comportamentos pelo seu grau de dificuldade e sofisticação tecnológica.

Os participantes foram também questionados sobre quantas vezes se envolveram nestes comportamentos durante a sua vida e nos últimos 12 meses, com o intuito de perceber se estas práticas eram ou não recentes na vida do indivíduo. As respostas foram dadas numa escala de *Likert* de 0 a 4 pontos (0=nunca; 1=1 a 2 vezes; 2=3 a 5 vezes; 3=6 a 9 vezes; 4=10 ou mais vezes). Posteriormente, foi calculado um índice através da soma dos pontos de cada comportamento mencionado, podendo este variar de 0 a 20 pontos. Portanto, quanto maior for o *score*, maior é envolvimento do indivíduo no *hacking* malicioso (durante a vida e nos últimos 12 meses). Ademais, de modo a formar uma ideia geral da prática dos comportamentos, a variável foi também dicotomizada (0=nenhum comportamento praticado; 1=pelo menos um comportamento de *hacking* malicioso praticado) em ambos os períodos temporais.

b) Idade de início do envolvimento nos comportamentos de *hacking* malicioso

De seguida, caso o participante tivesse indicado a prática de pelo menos um comportamento, foi pedido que indicasse a *idade*, aproximada, em que cometeu pela primeira vez esse(s) comportamento(s). A finalidade desta questão é permitir a identificação de comportamentos antissociais e criminais precoces, e a caraterização de potenciais carreiras criminais. As respostas foram de índole quantitativa, em que os indivíduos indicaram a idade em anos.

c) Imitação dos comportamentos de *hacking* malicioso

A pergunta final deste grupo prende-se com uma das componentes do processo de aprendizagem social – a *imitação*. Esta foi colocada na sequência do envolvimento nos comportamentos de *hacking*, de modo que as perguntas seguissem uma ordem lógica e se evitassem repetições. Assim, durante a construção do questionário, entendeu-se que a sua integração funcionaria melhor no presente grupo do que no Grupo III, onde se encontram os outros elementos do processo de aprendizagem social. Como tal, foi requerido aos participantes que assinalassem a principal fonte com que aprenderam esse(s) comportamento(s). As opções de resposta variaram entre: 1=pais; 2=família; 3=professor/es; 4=amigos; 5=livros/revistas; 6=televisão/filmes; 7=*internet*/*sites online*; 8=outro. Estas fontes foram adaptadas dos trabalhos de Skinner e Fream (1997).

Grupo III – Elementos do Processo de Aprendizagem Social

As questões incluídas no terceiro grupo relacionam-se com a medição das componentes inerentes ao processo de aprendizagem social, designadamente, a associação diferencial, as definições e o reforço diferencial. De seguida, apresenta-se a forma como cada componente foi operacionalizada e as investigações que serviram de suporte a este processo.

a) Associação Diferencial

De modo a medir a *associação diferencial* de cada participante, e, assim, obter informação sobre comportamentos de *hacking* do grupo de pares e de pessoas próximas do indivíduo, foi colocada a seguinte questão: '*quantos amigos seus se envolvem ou envolveram nos seguintes comportamentos?'*. Foram apresentados os cinco comportamentos de *hacking* mencionados no Grupo II, no qual o participante se posicionou numa escala de *Likert* de 5 pontos (1=nenhum; 2=alguns; 3=metade; 4=mais de metade; 5=todos) para cada comportamento. Posteriormente, foi criada uma escala global, em que os valores situam-se num intervalo de 5 a 25 pontos. Quanto maior for o *score*, mais associações desviantes o respondente

possui. Esta medida foi adaptada das investigações empíricas de Bossler e Burruss (2011), Holt e colegas (2012) e Skinner e Fream (1997).

b) Definições

Relativamente à componente *definições*, foram elencadas 7 afirmações relativas ao uso de computadores, à navegação *online* na *internet* e aos aspetos legais e éticos destes últimos dois pontos. Estas foram adaptadas dos estudos de Holt e colegas (2010), Morris e Blackburn (2009) e de Skinner e Fream (1997), no qual foi questionado em que medida os participantes concordavam ou discordavam das frases expostas quando utilizam um computador ou a *internet* (*e.g.,* "se as pessoas não querem que eu tenha acesso ao seu computador ou conta *online*, deveriam usar sistemas de segurança melhores") (cf. Grupo III do Anexo I). Para cada afirmação, a resposta foi dada numa escala de *Likert* de 4 pontos (1=discordo fortemente; 2=discordo; 3=concordo; 4=concordo fortemente). Os valores dos itens foram somados para criar um índice geral, podendo o mesmo variar entre 6 e 24 pontos, em que valores mais elevados indicam uma maior concordância com definições pró-criminais.

c) Reforço Diferencial

No que concerne ao *reforço diferencial*, foram colocadas três questões relativas à frequência com que: 1) o indivíduo testemunhou um professor, chefe ou colega de trabalho a ter orgulho de praticar atividades ilegais e não éticas decorrentes do uso de um computador; 2) presenciou uma dessas figuras a incentivar este tipo de atividades; 3) foi alvo de um incentivo por parte dessas figuras para praticar este tipo de atividades. As respostas possíveis oscilaram numa escala de *Likert* de 5 pontos, de 1 (nunca) a 5 (10 ou mais vezes). Este tipo de questões tem sido útil para apurar em que medida os indivíduos são alvo de um reforço e imagem positiva quanto ao cometimento de certos atos ilegais. Assim, a medição desta variável foi adaptada dos seguintes estudos: Holt e colaboradores (2010); Morris e Blackburn (2009); Nodeland e Morris (2020); e Skinner e Fream (1997). À semelhança das componentes anteriores, criou-se um índice geral de reforço diferencial, podendo o mesmo oscilar entre 3 e 15 pontos. *Scores* superiores significam níveis de reforço mais elevados.

Grupo IV – Autocontrolo

Relativamente ao Grupo IV, este engloba uma medida de *autocontrol*o, outra das variáveis independentes em estudo. Para mensurar este conceito utilizou-se a Escala de Grasmick *et al.* (1993) devido às suas propriedades psicométricas e ao facto de ser uma escala amplamente usada pela comunidade científica, tanto internacional como portuguesa.

Quanto à sua composição, esta inclui 24 itens atitudinais agregados nas seguintes categorias: 1) impulsividade; 2) tarefas simples; 3) procura do risco; 4) atividades físicas; 5) autocentração; 6) temperamento (cf. Grupo IV Anexo I). Cada uma destas foi concebida pelos autores com o intuito de recolher informação sobre os aspetos que caraterizam o autocontrolo enquanto indicador de propensão criminal proposto por Gottfredson e Hirschi (1990). A operacionalização dos itens é concretizada numa escala de *Likert* de 1 (discordo fortemente) a 4 (concordo totalmente), no qual cada participante obtém um *score* quantitativo entre 24 e 96 pontos (Bossler & Burruss, 2011). Nesta escala os *scores* elevados remetem para níveis mais baixos de autocontrolo, recaindo numa interpretação reversa (Gibson & Wright, 2001).

Grupo V – Desejabilidade Social

Por fim, o Grupo V compreende a medição da *desejabilidade social*, no qual foi utilizado o instrumento EPQ-RS de Eysenck e Eysenck (1998), a forma revista e encurtada do *Eysenck Personality Questionnaire-Revised* (EPQ-R) dos mesmos autores. A versão original é constituída por 100 itens dicotómicos ('sim', 'não'), divididos por quatro dimensões: neuroticismo; extroversão; psicoticismo e; desejabilidade social. O EPQ-RS, por sua vez, é composto por 48 itens, no qual os autores selecionaram 12 itens de cada dimensão da versão original, de modo a criarem uma variante menos extensa (Aluja *et al.*, 2003).

No presente estudo recorreu-se somente à dimensão de desejabilidade social, de modo a integrar uma variável de controlo que permitisse aferir a honestidade das repostas. Ou seja, com esta variável é possível perceber a forma como os indivíduos respondem a afirmações relativas a comportamentos e atitudes socialmente indesejáveis, porém comuns (Ferrando & Anguiano-Carrasco, 2010) (*e.g.,* fazer batota no jogo; estragar ou perder algo de outra pessoa) (cf. Grupo V Anexo I). Caso os participantes respondam de forma socialmente desejável a estes pequenos aspetos, pode-se concluir que tiveram uma posição semelhante nas respostas anteriores.

4.5. Procedimentos de Recolha de Dados

Previamente à aplicação do questionário, procedeu-se à realização de um pré-teste *online*. O objetivo deste ensaio foi avaliar a formulação das perguntas, a composição geral do questionário e o tempo despendido para o preenchimento do mesmo (Hill & Hill, 1998a; Maxfield & Babbie, 2014). Para tal, foi selecionada uma pequena amostra de nove pessoas, composta por cinco participantes do sexo masculino, cinco pessoas com licenciatura concluída

e caraterizada por uma média de idades de 37 anos. O *feedback* de cada participante foi analisado, e, de modo geral, foram evidenciados os seguintes pontos: 1) introduzir uma pergunta referente às habilitações literárias a frequentar no Grupo I; 2) alterar a aparência de algumas das perguntas do Grupo I; 3) corrigir a pontuação de alguns itens do Grupo IV e do Grupo V. Relativamente ao tempo despendido para o preenchimento do questionário, os participantes demoraram entre 5 e 10 minutos, sendo o antecipado na sua construção.

Elaboradas as modificações no questionário, o pedido de colaboração no estudo foi enviado por *e-mail* para as reitorias de diversas universidades (*e.g.,* Porto, Coimbra, Lisboa) e para as faculdades, os institutos politécnicos e as escolas profissionais que agregam cursos de interesse (*e.g.,* engenharia informática, programação, tecnologias). O pedido foi igualmente enviado para empresas que operam na área das TIC. O objetivo foi a disseminação do questionário pelos estudantes e docentes das instituições, bem como funcionários das empresas, por todo o país e ilhas, de modo a se conseguir alcançar o máximo de participantes. Contudo, como somente algumas das entidades contactadas responderam ao pedido de colaboração, procedeu-se a um *follow-up*, informando-se as instituições de ensino que o questionário poderia ser disseminado por alunos e docentes de outras áreas, dada a dificuldade de divulgação circunscrita reportada por diversas instituições. Não obstante, os respondentes foram indagados sobre se eram ou não eram da área das TIC, como uma pergunta de filtro, tal como referido previamente.

Posto isto, o questionário foi disseminado e preenchido *online*, caraterizando-se por ser uma forma mais simples e célere de recolher dados (Maxfield & Babbie, 2014), bem como mais adequada para o objeto de estudo. A fase de recolha de dados teve a duração de 2 meses. Findo este período, procedeu-se à exportação dos dados para *softwares* e deu-se início à análise estatística.

4.6. Procedimentos Analíticos

Como referido anteriormente, os dados dos questionários foram exportados do *LimeSurvey* para bases de dados do *software IBM SPSS® 28* e do *software JASP*, procedendo-se à análise estatística dos dados a partir destes *softwares*. Os procedimentos estatísticos efetuados durante a análise de dados, podem ser divididos em três tipologias principais: a) análise preliminar dos dados; b) análise estatística descritiva e; 3) análise estatística inferencial. Frisa-se, que tendo por base o Teorema Limite Central, dado que a amostra é superior a 30 participantes, foram executados testes paramétricos (Marôco, 2010).

4.6.1. Análise Preliminar dos Dados

Numa primeira fase, realizou-se o procedimento de *screening*, com o principal objetivo de verificar a adequação dos dados às variáveis presentes no estudo. Pretendeu-se averiguar se existiam valores que poderiam não estar integrados no intervalo de valores possíveis para cada variável. Dado que a quantidade de dados introduzida no *software* é elevada, podem surgir erros, inviabilizando ou tornando imprecisos os resultados em fases de análise posteriores (Pallant, 2016).

4.6.2. Análise Estatística Descritiva

Nesta etapa, os procedimentos estatísticos têm a finalidade de descrever e caraterizar a amostra da investigação (Pallant, 2016), sendo utilizadas diversas técnicas consoante a natureza da variável em estudo (Marôco, 2010), como se descreve de seguida.

- *Teste de Fiabilidade*

Primeiramente, 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. Tal assumiu especial relevância para as escalas criadas com base em diferentes estudos empíricos (*e.g.,* escala dos comportamentos de *hacking* malicioso). 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, 1998b; Field, 2013).

- *Estatística Descritiva*

Numa segunda fase, realizaram-se os procedimentos de estatística univariada. Para a análise das variáveis quantitativas recorreu-se a medidas de tendência central e medidas de dispersão (Marôco, 2010). Assim, para este tipo de variáveis (*e.g.,* idade, escala de autocontrolo) utilizaram-se medidas como a média amostral ($\bar{x}$) e o desvio-padrão (S.D.), permitindo perceber a colocação dos valores de cada variável nos dados gerais e em que medida se desviam da média (Field, 2013; Marôco, 2010). Quanto às variáveis qualitativas (*e.g.,* género, fontes de imitação), recorreu-se a percentagens, sendo esta a melhor forma de descrever a informação das variáveis desta natureza (Field, 2013).

- *Testes Bivariados (Testes t* e *testes Qui-quadrado)*

Nesta etapa foram realizados testes estatísticos bivariados designadamente testes *t* para amostras independentes (para a comparação de médias) e testes Qui-quadrado (para a comparação de proporções). Por exemplo, foram conduzidos testes *t* para verificar se havia diferenças significativas nas médias de autocontrolo dos *hackers* maliciosos e dos *hackers* não maliciosos,

e testes Qui-quadrado para averiguar se havia diferenças significativas de proporções ao nível do género no cometimento, ou não, de comportamentos de *hacking* malicioso.

4.6.3. Análise Estatística Inferencial

De modo a atingir os objetivos gerais e específicos do estudo, em primeiro lugar, foram utilizados coeficientes de correlação de Pearson (*r*), de modo a analisar e quantificar a intensidade e a direção da associação entre variáveis. Em segundo lugar, foram realizadas análises de regressão logística. Primeiramente, para determinar os fatores explicativos para a prática de comportamentos de *hackin*g malicioso, construíram-se três modelos parcelares com as seguintes variáveis: 1) incluiu-se as variáveis sociodemográficas; 2) incluiu-se o autocontrolo; 3) incluiu-se as três componentes da aprendizagem social (associação diferencial, definições e reforço diferencial). Posteriormente, elaborou-se um modelo final com todas as variáveis anteriormente mencionadas. Portanto, o propósito da elaboração destes diferentes modelos foi, numa primeira fase, analisar os efeitos preditores dos diferentes conjuntos de variáveis independentes separadamente e, numa segunda fase, em interação. De seguida, para averiguar se a relação entre o autocontrolo e a prática de *hacking* malicioso era mediada pela associação diferencial, foi realizado um modelo de mediação utilizando a extensão *PROCESS* do *SPSS*. Os procedimentos mencionados foram realizados para o *hacking malicioso* durante a vida e nos últimos 12 meses.

CAPÍTULO V – ESTUDO EMPÍRICO (RESULTADOS)

5.1. Caraterização da amostra com base em Variáveis Sociodemográficas

A amostra do estudo é constituída por 680 indivíduos. No que respeita à variável *idade*, os inquiridos têm idades compreendidas entre os 18 e os 74 anos, com uma média de cerca de 28 anos (27.63) e um desvio padrão de 12.80. Na Tabela 1 apresentam-se as frequências das variáveis sociodemográficas de índole qualitativa.

Tabela 1: Características sociodemográficas da amostra total (N=680)

	Total	
Variáveis	n	%
Género		
Feminino	264	38.8
Masculino	415	61.1
Outro	1	0.1
Estado Civil		
Solteiro/a	525	77.2
União de Facto	34	5.0
Casado/a	104	15.3
Ex-União de Facto	3	0.4

Divorciado/a	11	1.6
Viúvo/a	3	0.4
Situação Profissional		
Desempregado/a	16	2.4
Empregado/a por Conta Própria	14	2.1
Empregado/a por Conta de Outrem	184	27.1
Estudante	369	54.3
Trabalhador-Estudante	85	12.5
Reformado/a	4	0.6
Outro	8	1.2
Habilitações Concluídas		
4.º ano	2	0.3
6.º ano	0	0.0
9.º ano	82	12.1
12.º ano	238	35.0
Curso Profissional	60	8.8
Licenciatura	138	20.3
Pós-Graduação	20	2.9
Mestrado	78	11.5
Doutoramento	62	9.1
Habilitações a Frequentar		
Nenhuma	166	24.4
4.º ano	0	0.0
6.º ano	0	0.0
9.º ano	5	0.7
12.º ano	10	1.5
Curso Profissional	130	19.1
Licenciatura	230	33.8
Pós-Graduação	5	0.7
Mestrado	95	14.0
Doutoramento	39	5.7
Pertencer à área das TIC		
Não	260	38.2
Sim	420	61.8
Conhecimento Informático		
Baixo	31	4.6
Médio-Baixo	78	11.5
Médio	215	31.6
Médio-Alto	236	34.7
Alto	120	17.6

Relativamente ao *género*, predomina o masculino face ao feminino (61.1% e 38.8%, respetivamente), e somente um participante se identificou com a opção 'outro'. Quanto ao *estado civil*, 77.2% dos indivíduos da amostra total são solteiros (*n*=525) e 15.3% são casados (*n*=104). Com percentagens mais baixas encontram-se os participantes em união de facto (n=34, 5%), divorciados (*n*=11, 1.6%), em ex-união de facto (*n*=3, 0.4%) e viúvos (*n*=3, 0.4%).

Referente à *situação profissional*, constata-se que mais de metade dos participantes se encontra a estudar (*n*=369, 54.3%), 27.1% encontra-se empregada por conta de outrem (*n*=184) e 12.5% encontra-se com estatuto de trabalhador-estudante (*n*=85). As situações profissionais com percentagens mais reduzidas são: estar desempregado/a (*n*=16, 2.4%); estar empregado/a

por conta própria (*n*=14, 2.1%); outra situação (*n*=8, 1.2%), sendo referido pelos participantes em questão que se encontravam com estatuto de bolseiro/a; e, estar reformado/a (*n*=4, 0.6%).

No que concerne às *habilitações académicas concluídas*, constata-se que os três graus concluídos mais predominantes são o 12.º ano (*n*=238, 35%), a licenciatura (*n*=138, 20.3%) e o 9.º ano (*n*=82, 12.1%). Porém, as percentagens de outras opções encontram-se próximas deste último valor, nomeadamente o mestrado (11.5%), o doutoramento (9.1%) e o curso profissional (8.8%). A pós-graduação, o 4.º ano e o 6.º ano são as habilitações com menor frequência (2.9%, 0.3% e 0%, respetivamente). Quanto às *habilitações a frequentar*, verifica-se que 33.8% da amostra se encontra a frequentar uma licenciatura (*n*=230), 19.1% um curso profissional (*n*=130) e 14.0% um mestrado (*n*=95). Com percentagens mais reduzidas encontram-se os participantes a frequentar um doutoramento (n=39, 5.7%), o 12.º ano (*n*=10, 1.5%), o 9.º ano (*n*=5, 0.7%) e uma pós-graduação (*n*=5, 0.7%). Contudo, 24.4% afirmou não estar a frequentar qualquer tipo de habilitação literária (*n*=166).

Relativamente aos indivíduos que estejam ou tenham estado empregados ou a estudar na área das *TIC*, predomina a resposta afirmativa (61.8%) face à resposta negativa (38.2%). Por fim, quanto ao *conhecimento informático*, 34.7% dos participantes estimaram o seu conhecimento como médio-alto e 31.6% como médio. As percentagens mais reduzidas pertencem ao conhecimento informático alto (17.6%), médio-baixo (11.5%) e baixo (4.6%).

5.2. Caraterização da amostra com base no *Hacking* Malicioso

Caraterizada a amostra face às caraterísticas sociodemográficas, de seguida carateriza-se segundo a variável dependente em estudo – o *hacking* malicioso – tanto durante a vida, como nos últimos 12 meses. Para tal, foram calculadas percentagens (Tabelas 2 e 3).

Tabela 2: Prevalência da prática de comportamentos de hacking malicioso durante a vida (N=680)

Variáveis	Total	
	n	%
Prática de *hacking* malicioso durante a vida		
Comportamento 1		
Nunca	307	45.1
1 a 2 vezes	146	21.5
3 a 5 vezes	115	16.9
6 a 9 vezes	34	5.0
10 ou mais vezes	78	11.5
Comportamento 2		
Nunca	405	59.6
1 a 2 vezes	171	25.1
3 a 5 vezes	66	9.7
6 a 9 vezes	13	1.9

10 ou mais vezes	25	3.7
Comportamento 3		
Nunca	575	84.6
1 a 2 vezes	76	11.2
3 a 5 vezes	12	1.8
6 a 9 vezes	3	0.4
10 ou mais vezes	14	2.1
Comportamento 4		
Nunca	606	89.1
1 a 2 vezes	49	7.2
3 a 5 vezes	15	2.2
6 a 9 vezes	3	0.4
10 ou mais vezes	7	1.0
Comportamento 5		
Nunca	644	94.7
1 a 2 vezes	23	3.4
3 a 5 vezes	6	0.9
6 a 9 vezes	2	0.3
10 ou mais vezes	5	0.7
Dicotomização da Prática de *hacking* malicioso durante a vida		
Não (0)	269	39.6%
Sim (1)	411	60.4%

Relativamente ao cometimento de *hacking malicioso durante a vida*, observa-se que 60.4% dos indivíduos reportaram ter cometido, pelo menos, um comportamento de *hacking* malicioso. Em concreto, para todos os comportamentos presentes na escala, prevalece o facto de os indivíduos reportarem nunca terem praticado tais comportamentos, sendo a opção 'nunca' a mais frequente.

Referente ao comportamento 1 – "*adivinhar ou tentar adivinhar passwords para aceder a um computador ou conta online de outra pessoa sem autorização"* – 21.5% reportou ter praticado entre 1 a 2 vezes, 16.9% entre 3 a 5 vezes, 11.5% ter praticado 10 ou mais vezes, e 5% entre 6 a 9 vezes. No comportamento 2 – "*aceder a um computador ou conta online de outra pessoa sem autorização"* – observa-se que 25.1% dos participantes afirmaram ter cometido este comportamento 1 a 2 vezes, 9.7% ter cometido 3 a 5 vezes, 3.7% ter cometido 10 ou mais vezes e apenas 1.9% ter cometido 6 a 9 vezes.

No que concerne ao comportamento 3 – "*adicionar eliminar, alterar ou imprimir informação de um computador ou conta online de outra pessoa sem autorização"* – 11.2% reportou ter praticado esse ato 1 a 2 vezes, 2.1% ter praticado 10 ou mais vezes, 1.8% 3 a 5 vezes, e 0.4% 6 ou mais vezes. Relativamente ao comportamento 4 – *"usar um malware para causar dano ou destruir dados num computador ou sistema de computadores (exemplo: vírus, worms)"* – constata-se que 7.2% afirmou ter cometido esse comportamento entre 1 a 2 vezes, 2.2% ter cometido entre 3 a 5 vezes, 1% ter cometido 10 ou mais vez e 0.4% entre 6 a 9 vezes.

Por fim, no comportamento 5 – *"criar um malware para causar dano ou destruir dados num computador ou sistema de computadores (exemplo: vírus, worms)"* – as percentagens foram diminutas. Apenas 3.4% dos participantes reportou ter praticado tal ato entre 1 a 2 vezes, 0.9% ter praticado entre 3 a 5 vezes, 0.7% ter praticado 10 ou mais vezes e 0.3% entre 6 a 9 vezes.

Relativamente à *idade de início* de envolvimento nos comportamentos, os dados obtidos são heterogéneos, oscilando entre o valor mínimo de 6 anos e o valor máximo de 40 anos. Denota-se que a média de idades se situa nos 15 anos (15.16), com um desvio padrão de 4.70.

Tabela 3:Prevalência da prática de comportamentos de hacking malicioso nos últimos 12 meses (N=680)

	Total	
Variáveis	n	%
Prática de *hacking* malicioso nos últimos 12 meses		
Comportamento 1		
Nunca	542	79.7
1 a 2 vezes	106	15.6
3 a 5 vezes	24	3.5
6 a 9 vezes	4	0.6
10 ou mais vezes	4	0.6
Comportamento 2		
Nunca	654	96.2
1 a 2 vezes	7	1.0
3 a 5 vezes	13	1.9
6 a 9 vezes	1	0.1
10 ou mais vezes	5	0.7
Comportamento 3		
Nunca	656	96.5
1 a 2 vezes	13	1.9
3 a 5 vezes	6	0.9
6 a 9 vezes	2	0.3
10 ou mais vezes	3	0.4
Comportamento 4		
Nunca	646	95.0
1 a 2 vezes	26	3.8
3 a 5 vezes	2	0.3
6 a 9 vezes	2	0.3
10 ou mais vezes	4	0.6
Comportamento 5		
Nunca	660	97.1
1 a 2 vezes	14	2.1
3 a 5 vezes	2	0.3
6 a 9 vezes	2	0.3
10 ou mais vezes	2	0.3
Dicotomização da Prática de *hacking* malicioso nos últimos 12 meses		
Não (0)	522	76.8%
Sim (1)	158	23.2%

Na Tabela 3 observa-se que 23.2.% dos indivíduos reportaram ter cometido, pelo menos, um comportamento de *hacking* malicioso, nos últimos 12 meses. À semelhança do que foi descrito relativamente aos comportamentos durante a vida, também a opção 'nunca' foi a mais identificada pelos participantes quanto ao cometimento de *hacking malicioso nos últimos 12 meses*. Todavia, os comportamentos mais praticados foram o comportamento 1 (*n*=138, 20.3%) e o comportamento 4 (*n*=34, 5%), embora a frequência seja substancialmente díspar entre os dois.

5.2.1 Índices dos Comportamentos de Hacking Malicioso

A Tabela 4 é relativa aos índices do envolvimento no *hacking* malicioso. Para o envolvimento durante a vida, foi obtida uma média de 2.31, com um desvio padrão de 3.13. Para o envolvimento nos últimos 12 meses, foram obtidos os seguintes valores: $\bar{x}$=.53±1.66.

Os comportamentos anteriormente elencados foram integrados numa escala de *Hacking* Malicioso durante a vida, tendo-se obtido um alfa de *Cronbach* de .76 para a mesma. Para o índice de *Hacking* Malicioso nos últimos 12 meses, obteve-se também um alfa aceitável (α =.80).

Tabela 4: Descrição da amostra com base nos índices de hacking malicioso

Variáveis	**Amostra total**				
	Min.-Máx.	*n*	$\bar{x}$	S.D.	α
***Hacking* Malicioso durante a vida**	0-20	680	2.31	3.13	.76
***Hacking* Malicioso nos últimos 12 meses**	0-20	680	.53	1.66	.80

5.3. Diferenças de médias entre *hackers* não-maliciosos e *hackers* maliciosos para Variáveis Sociodemográficas

No que se refere à idade, pela análise das Tabelas 5 e 6, os resultados dos testes *t* permitem concluir que existem diferenças significativas entre os grupos em análise, dado que os valores do *p-value* são inferiores a .05. Constata-se que os *hackers* maliciosos apresentam médias de idades inferiores aos *hackers* não-maliciosos, seja nos comportamentos praticados durante toda a vida ($\bar{x}$=23.92±8.43 vs. $\bar{x}$=33.30±15.81), como nos comportamentos praticados nos últimos 12 meses ($\bar{x}$=22.39±6.86 vs. $\bar{x}$=29.21±13.67).

Tabela 5: Descrição da amostra com base em diferenças de médias entre hackers não maliciosos vs. hackers maliciosos (durante a vida)

Variáveis	**Não-Maliciosos**			**Maliciosos**				
	n	$\bar{x}$	*S.D.*	*n*	$\bar{x}$	*S.D.*	*t*	*p*
Idade	269	33.30	15.81	411	23.92	8.43	8.925	< .001

Tabela 6: Descrição da amostra com base em diferenças de médias entre hackers não maliciosos vs. hackers maliciosos (nos últimos 12 meses)

Variáveis	Não-Maliciosos			Maliciosos				
	n	$\bar{x}$	*S.D.*	*n*	$\bar{x}$	*S.D.*	*t*	*p*
Idade	522	29.21	13.67	158	22.39	6.86	8.432	< .001

5.4. Testes Qui-Quadrado entre *hackers* não-maliciosos e *hackers* maliciosos para Variáveis Sociodemográficas

De modo a examinar as proporções das variáveis qualitativas consoante os grupos em análise (*hackers* maliciosos e não-maliciosos) foram realizados testes de Qui-quadrado (Tabelas 7 e 8).

Tabela 7: Testes Qui-Quadrado para variáveis sociodemográficas entre hackers não-maliciosos vs. hackers maliciosos (durante a vida)

Variáveis	Total		Não-Maliciosos		Maliciosos		X^2	*p*
Género	**n**	**%**	**n**	**%**	**n**	**%**		
Feminino (0)	264	38.9	143	53.4	121	29.4	39.051	<.001
Masculino (1)	415	61.1	125	46.6	290	70.6		
Estado Civil								
Não-Solteiro/a (0)	155	22.8	92	34.2	63	15.3	32.905	<.001
Solteiro/a (1)	525	77.2	177	65.8	348	84.7		
Situação Profissional								
Não-Empregado/a (0)	397	58.4	136	50.6	261	63.5	11.215	<.001
Empregado/a (1)	283	41.6	133	49.4	150	36.5		
Habilitações Concluídas								
Grau < Licenciatura (0)	382	56.2	117	43.5	265	64.5	29.076	<.001
Grau ≥ Licenciatura (1)	298	43.8	152	56.5	146	35.5		
Habilitações a Frequentar								
Não (0)	166	24.4	93	34.6	73	17.8	24.901	<.001
Sim (1)	514	75.6	176	65.4	338	82.2		
Pertencer à área das TIC								
Não (0)	260	38.2	146	54.3	114	27.7	48.485	<.001
Sim (1)	420	61.8	123	45.7	297	72.3		
Conhecimento Informático								
Baixo (0)	324	47.6	166	61.7	158	38.4	35.286	<.001
Alto (1)	356	52.4	103	38.3	253	61.6		

Tabela 8: Testes Qui-Quadrado para variáveis sociodemográficas entre hackers não-maliciosos vs. hackers maliciosos (nos últimos 12 meses)

Variáveis	Total		Não-Maliciosos		Maliciosos		X^2	*p*
Género	**n**	**%**	**n**	**%**	**n**	**%**		
Feminino (0)	264	38.9	226	43.4	38	24.1	19.057	<.001
Masculino (1)	415	61.1	295	56.6	120	75.9		
Estado Civil								
Não-Solteiro/a (0)	155	22.8	134	25.7	21	13.3	10.562	.001
Solteiro/a (1)	525	77.2	388	74.3	137	86.7		
Situação Profissional								
Não-Empregado/a (0)	397	58.4	285	54.6	112	70.9	13.244	<.001
Empregado/a (1)	283	41.6	237	45.4	46	29.1		
Habilitações Concluídas								
Grau < Licenciatura (0)	382	56.2	270	51.7	112	70.9	18.090	<.001
Grau ≥ Licenciatura (1)	298	43.8	252	48.3	46	29.1		
Habilitações a Frequentar								
Não (0)	166	24.4	146	28.0	20	12.7	15.409	<.001
Sim (1)	514	75.6	376	72.0	138	87.3		
Pertencer à área das TIC								
Não (0)	260	38.2	235	45.0	25	15.8	43.780	<.001
Sim (1)	420	61.8	287	55.0	133	84.2		
Conhecimento Informático								
Baixo (0)	324	47.6	286	54.8	38	24.1	45.942	<.001
Alto (1)	356	52.4	236	45.2	120	75.9		

Pela análise dos dados presentes nas Tabelas 7 e 8 é possível aferir que existem diferenças estatisticamente significativas em todas as variáveis sociodemográficas analisadas em função da variável dependente *hacking* malicioso (p<.05). Tal significa que, em ambos os períodos analisados (durante a vida e nos últimos 12 meses), existe uma dependência entre as variáveis. Assim, o *hacker* malicioso encontra-se associado: ao género masculino; a estar solteiro; a não estar empregado; a deter um grau inferior a uma licenciatura; a estar a frequentar algum tipo de habilitação literária; a pertencer à área das TIC; e a deter um conhecimento informático alto.

5.5. Caraterização da amostra com base nas Componentes da Teoria da Aprendizagem Social

De seguida apresenta-se a caraterização da amostra com base noutra das variáveis independentes – as *Componentes das Aprendizagem Social* (Tabelas 9, 10, 11 e 12).

Tabela 9: Componente Associação Diferencial (N=618)

	Total	
Variáveis	n	%
Amigos que praticam/praticaram *hacking* malicioso		
Comportamento 1		
Nenhum	256	41.4
Alguns	293	47.3
Metade	36	5.8
Mais de Metade	31	5.0
Todos	2	0.3
Comportamento 2		
Nenhum	307	49.7
Alguns	281	45.5
Metade	16	2.6
Mais de Metade	13	2.1
Todos	1	0.2
Comportamento 3		
Nenhum	427	69.1
Alguns	182	29.4
Metade	5	0.8
Mais de Metade	3	0.5
Todos	1	0.2
Comportamento 4		
Nenhum	488	79.0
Alguns	119	19.3
Metade	6	1.0
Mais de Metade	4	0.6
Todos	1	0.2
Comportamento 5		
Nenhum	546	88.3
Alguns	67	10.8
Metade	3	0.5
Mais de Metade	1	0.2
Todos	1	0.2

Referente à componente *Associação Diferencial* (Tabela 9), a opção 'nenhum' foi a mais usual nos comportamentos, exceto no comportamento 1, no qual predomina a opção 'alguns' (*n*=293, 47.3%). Pela análise ascendente das opções e dos comportamentos, constata-se que a prevalência dos participantes vai diminuindo, ou seja, a opção 'todos' é a que conta

com as menores frequências em todos os comportamentos (igual ou inferior a 0.3%), e o comportamento 5 é o que detém a percentagem mais reduzida de ter amigos envolvidos nos *hacking* malicioso (11.7%).

Tabela 10: Componente Imitação (N=372)

Variáveis	Total	
	n	%
Fontes de Imitação		
Pais	5	1.3
Família	5	1.3
Professor/es	13	3.5
Amigos	80	21.5
Livros/Revistas	2	0.5
Televisão/Filmes	27	7.3
Internet/Sites Online	225	60.5
Outro	15	4.0

No que concerne à fonte de *imitação* dos comportamentos de *hacking* malicioso (Tabela 10), destacam-se as opções '*internet*/*sites online'* (60.5%) e 'amigos' (21.5%). Com percentagens mais reduzidas encontram-se as fontes: 'televisão/filmes' (7.3%); 'outro' (4%); 'professor/es' (3.5%); 'pais' (1.3%); 'família' (1.3%); e 'livros/revistas' (0.5%).

Tabela 11: Componente Definições (N=618)

Variáveis	Total	
	n	%
Definições		
1- *"Como é contra a lei, eu nunca faria nada ilegal através de um computador"*		
Discordo Totalmente	106	17.2
Discordo	171	27.7
Concordo	186	30.1
Concordo Totalmente	155	25.1
2- *"É importante que as pessoas saibam o que podem ou não fazer com os recursos computacionais na escola e no local de trabalho"*		
Discordo Totalmente	9	1.5
Discordo	17	2.8
Concordo	233	37.7
Concordo Totalmente	359	58.1
3- *"Há regras claras do que é um comportamento online aceitável e ético"*		
Discordo Totalmente	97	15.7
Discordo	138	22.3
Concordo	215	34.8
Concordo Totalmente	168	27.2
4- *"Se as pessoas não querem que eu tenha acesso ao seu computador ou conta online, deveriam usar sistemas de segurança melhores"*		
Discordo Totalmente	134	21.7

Discordo	174	28.2
Concordo	202	32.7
Concordo Totalmente	108	17.5
5- *"Eu deveria ter acesso a qualquer tipo de informação que o governo, a escola, o emprego ou um indivíduo tem sobre mim, mesmo que eles não me deem acesso"*		
Discordo Totalmente	67	10.8
Discordo	133	21.5
Concordo	236	38.2
Concordo Totalmente	182	29.4
6- *"Nunca denunciaria um amigo meu por ter tido acesso não autorizado a um computador ou conta online de outra pessoa"*		
Discordo Totalmente	56	9.1
Discordo	205	33.2
Concordo	195	31.6
Concordo Totalmente	162	26.2
7- *"As pessoas que entram nos sistemas computacionais estão, na verdade, a ajudar a sociedade"*		
Discordo Totalmente	115	18.6
Discordo	316	51.1
Concordo	155	25.1
Concordo Totalmente	32	5.2

Relativamente às *definições* favoráveis ao crime (Tabela 11), foram analisados sete tipos de afirmações, sendo as opções das definições 1 e 3 recodificadas para a forma reversa. De um modo geral, a amostra posicionou-se de forma homogénea pelas opções dadas a cada tipo de definição, exceto na definição 2 e na definição 7, em que prevaleceu com uma percentagem superior a 50% a opção 'concordo totalmente' e a opção 'discordo', respetivamente.

Tabela 12: Componente Reforço Diferencial (N=618)

	Total	
Variáveis	n	%
Reforço		
1- "Quantas vezes testemunhou um professor, chefe ou colega de trabalho a ter orgulho por ter utilizado um computador de forma não ética ou ter praticado atividades ilegais?"		
Nunca	318	51.5
1 a 2 vezes	147	23.8
3 a 5 vezes	92	14.9
6 a 9 vezes	20	3.2
10 ou mais vezes	41	6.6
2- "Quantas vezes testemunhou um professor, chefe ou colega de trabalho a incentivar alguém para usar um computador de forma não ética ou para praticar atividades ilegais?"		
Nunca	378	61.2
1 a 2 vezes	123	19.9
3 a 5 vezes	72	11.7
6 a 9 vezes	12	1.9
10 ou mais vezes	33	5.3
3- "Quantas vezes um professor, chefe ou colega de trabalho o/a incentivou a usar um computador de forma não ética ou a praticar atividades ilegais?"		
Nunca	404	65.4

1 a 2 vezes	139	22.5
3 a 5 vezes	48	7.8
6 a 9 vezes	10	1.6
10 ou mais vezes	17	2.8

Referente à componente *Reforço Diferencial* (Tabela 12), analisou-se a frequência de participantes que foram alvo de um reforço, seja de forma indireta (reforço 1 e 2) ou de forma direta (reforço 3). Embora em todas as formas a maioria dos indivíduos tenha reportado nunca ter sido reforçado para o uso não ético ou prática de atividades ilegais (frequências superiores a 50% em cada reforço), constata-se que uma média de 22% dos participantes revela ter sido alvo de reforço entre '1 a 2 vezes'. Salienta-se que, embora com valores diminutos, a opção '10 ou mais vezes' ocupa a 3.º posição mais elevada das vezes que os indivíduos afirmam ter sido alvo de reforço, contando 6.6% para o reforço 1, 5.3% para o reforço 2, e 2.8% para o reforço 3.

5.5.1. Índices das Componentes de Aprendizagem Social

A Tabela 13 é relativa aos índices das componentes de aprendizagem social. No caso da associação diferencial, foi obtida uma média de 7.03 com um desvio padrão de 2.33. Para a escala das definições, obteve-se uma média de 14.87 com um desvio padrão de 3.78. Por fim, a média da escala de reforço diferencial foi de 5.14 com um desvio padrão de 3.00.

Relativamente à fiabilidade, na escala da Associação Diferencial foi obtido um alfa de .84 e na escala do Reforço Diferencial obteve-se um alfa de .93. No que concerne à escala de Definições, o alfa de *Cronbach* inicialmente obtido foi de .67. Contudo, caso a definição 2 fosse excluída da presente escala, o alfa aumentava para .73.

Tabela 13: Descrição da amostra com base nos índices das componentes de aprendizagem social

Variáveis	**Amostra total**				
	Min.-Máx.	*n*	$\bar{x}$	S.D.	α
Associação Diferencial	5-25	618	7.02	2.33	.84
Definições	6-24	618	14.87	3.78	.73
Reforço Diferencial	5-15	618	5.14	3.00	.93

5.6. Correlação entre componentes da Aprendizagem Social e *Hacking* Malicioso

Os resultados das correlações entre as componentes da aprendizagem social e o *hacking* malicioso demonstram-se significativos (p<.05) (cf. Anexo III). Para os comportamentos durante a vida encontrou-se uma relação positiva moderada (*i.e.,* .30 < r < .50) entre a associação diferencial (r=.50), as definições (r=.47) e o reforço diferencial (r=.50). Para os comportamentos nos últimos 12 meses, existe, igualmente, uma relação positiva entre a

associação diferencial (r=.32), as definições (r=.20) e o reforço diferencial (r=.29). Contudo, a intensidade da relação altera-se, dado que para as definições e para o reforço diferencial passa a ser considerada fraca (r< .30) (Cohen, 1988).

5.7. Diferenças de médias entre *hackers* não-maliciosos e *hackers* maliciosos para as componentes da Teoria da Aprendizagem Social

Expostos os resultados das componentes da TAS para a amostra geral, de seguida elencam-se os resultados relativos aos testes de diferenças de médias entre os grupos *hackers* não-maliciosos e *hackers* maliciosos (Tabelas 14 e 15).

Tabela 14: Descrição das componentes da TAS com base em diferenças de médias entre hackers não maliciosos vs. hackers maliciosos (durante a vida)

Variáveis	Não-Maliciosos			Maliciosos				
	n	$\bar{x}$	*S.D.*	*n*	$\bar{x}$	*S.D.*	*t*	*p*
Associação	240	5.71	1.786	378	7.86	2.256	-13.117	< .001
Definições	240	12.67	2.971	378	16.26	3.579	-13.511	< .001
Reforço	240	3.52	1.628	378	6.16	3.208	-13.465	< .001

Tabela 15: Descrição das componentes da TAS com base em diferenças de médias entre hackers não maliciosos vs. hackers maliciosos (nos últimos 12 meses)

Variáveis	Não-Maliciosos			Maliciosos				
	n	$\bar{x}$	*S.D.*	*n*	$\bar{x}$	*S.D.*	*t*	*p*
Associação	470	6.47	1.929	148	8.78	2.625	-9.884	< .001
Definições	470	14.15	3.475	148	17.16	3.822	-8.536	< .001
Reforço	470	4.42	2.404	148	7.398	3.529	-9.558	< .001

Observando as tabelas, conclui-se que as médias para as variáveis associação, definições e reforço são mais elevadas para os *hackers* maliciosos face aos *hackers* não maliciosos, tanto nos comportamentos durante a vida como nos últimos 12 meses. Tendo como referência o período durante da vida do indivíduo, encontra-se que os *hackers* maliciosos detêm mais amigos que se envolvem/envolveram nos comportamentos de *hacking* ($\bar{x}$=7.86±2.26 vs. $\bar{x}$==5.71±.1.79), são mais concordantes com definições favoráveis ao crime ($\bar{x}$=17.16±3.82 vs. $\bar{x}$=14.15±3.48) e são mais reforçados face a comportamentos ilegais e não éticos sobre o uso de computadores ($\bar{x}$=7.40±3.53 vs. $\bar{x}$=4.42±2.40). Com recurso ao valor do *teste t*, percebe-se que, de facto, existem diferenças estatisticamente significativas entre os grupos para as variáveis em análise, dado que os valores do *p-value* são inferiores a .05.

5.8. Caraterização da amostra com base no Autocontrolo

Atendendo à Tabela 16, para o índice de autocontrolo foi obtida uma média de 50.82 e um desvio padrão de 10.51. Nesta escala, o alfa de *Cronbach* revela uma boa fiabilidade (α =.90).

Tabela 16: Descrição da amostra com base no índice de autocontrolo

Variáveis	Amostra total				
	Min.-Máx.	*n*	$\bar{x}$	S.D.	α
Autocontrolo	24-96	618	50.82	10.51	.90

5.9. Correlação entre Autocontrolo e *Hacking* Malicioso

Relativamente às correlações entre o autocontrolo e o *hacking* malicioso, verifica-se uma relação positiva, fraca e significativa para os comportamentos durante a vida (*r*=.14). Embora positiva (*r*=.074), a relação encontrada para os atos cometidos nos últimos 12 meses não é significativa (cf. Anexo III). Salienta-se que *scores* mais elevados representam níveis mais baixos de autocontrolo, sendo necessária uma interpretação reversa.

5.10. Diferenças de médias entre *hackers* não-maliciosos e *hackers* maliciosos para o Autocontrolo

Atendendo aos resultados do testes *t* expostos nas Tabelas 17 e 18, conclui-se que existem diferenças significativas entre os *hackers* não-maliciosos e os *hackers* maliciosos para o autocontrolo, dado que os valores de *p-value* são inferiores a .05. Efetivamente, na prática de atos durante a vida, os *hackers* maliciosos apresentam médias mais elevadas, *i.e.,* níveis de autocontrolo mais baixos ($\bar{x}$=46.94±10.47), comparativamente aos *hackers* não-maliciosos ($\bar{x}$=53.21±9.88). Uma diferença semelhante é obtida na prática de comportamentos nos últimos 12 meses.

Tabela 17: Diferença de médias entre hackers não-maliciosos vs. hackers maliciosos (durante a vida) para o Autocontrolo (N=587)

Variáveis	Não-Maliciosos			Maliciosos				
	n	$\bar{x}$	*S.D.*	*n*	$\bar{x}$	*S.D.*	*t*	*p*
Autocontrolo	223	46.94	10.365	364	53.21	9.879	-7.235	< .001

Tabela 18: Diferença de médias entre hackers não-maliciosos vs. hackers maliciosos (nos últimos 12 meses) para o Autocontrolo (N=587)

Variáveis	Não-Maliciosos			Maliciosos				
	n	$\bar{x}$	*S.D.*	*n*	$\bar{x}$	*S.D.*	*t*	*p*
Autocontrolo	444	50.05	10.764	143	53.237	9.308	-3.421	< .001

5.11. Fatores Explicativos do *Hacking Malicioso* (durante a vida)

De modo a perceber que variáveis prediziam o *hacking* malicioso durante a vida, foram realizadas regressões logísticas, contando com três modelos parcelares (variáveis sociodemográficas; autocontrolo; componentes da aprendizagem social) e um modelo final (onde foram incluídas todas as variáveis dos modelos parcelares).

5.11.1. Modelos Parcelares

- *Variáveis Sociodemográficas*

O modelo preditivo do *hacking* malicioso com base nas variáveis sociodemográficas mostrou-se significativo (p<.001). Este modelo explica cerca de 27% da prática dos comportamentos (Nagelkerke R^2=.266) (cf. Anexo IV). Das variáveis incluídas, apresentam-se como significativas: o género; a idade; as habilitações a frequentar; e o conhecimento informático. Destaca-se o valor preditivo da idade, no qual ser mais jovem aumenta a probabilidade de cometer *hacking* malicioso (*OR*=.359; p<.001).

- *Autocontrolo*

Com base no autocontrolo, o modelo é significativo (p<.001), e por si só, consegue explicar cerca de 12% da variância na variável dependente (Nagelkerke R^2=.115) (cf. Anexo V). O autocontrolo mostrou-se preditor do *hacking* malicioso, em que os indivíduos com níveis mais baixos de autocontrolo apresentam uma chance quase 2 vezes maior (*OR*= 1.944; p<.001) de praticar *hacking* malicioso do que os indivíduos com níveis mais altos de autocontrolo.

- *Componentes Aprendizagem Social*

O modelo parcelar relativo às componentes da aprendizagem social é significativo (p<.001) e destaca-se por ser o que detém maior capacidade preditiva do *hacking* malicioso, explicando quase 47% destas práticas (Nagelkerke R^2=.468). A associação diferencial, as definições e o reforço diferencial mostraram-se preditores (p<.001). Salienta-se o poder preditivo da associação diferencial, no qual indivíduos que possuem *scores* mais elevados apresentam uma chance 2 vezes superior à dos indivíduos que detém *scores* mais baixos desta variável (*OR*=2.040; p<.001). Destaca-se, igualmente o papel do reforço diferencial (*OR*=2.044; p<.001) (cf. Anexo VI).

5.11.2. Modelo Final

As variáveis independentes anteriormente analisadas de forma isolada foram agregadas num modelo de regressão final, com o intuito de examinar a capacidade preditiva conjunta e se o papel de cada variável se mantém ou altera quando se inclui outras variáveis (Tabela 19). Pela observação da Tabela 19, verifica-se que o modelo é significativo (p<.001) e que 53.4% (Nagelkerke R^2=.534) da variância total do *hacking* malicioso é explicada pelas variáveis independentes presentes no modelo.

Tabela 19: Modelo Preditor Final dos Comportamentos de Hacking Malicioso (durante a vida)

Variáveis	**Modelo Final**			
	B	**SE**	**β**	**OR**
Idade	**-.066**	**.020**	**-.821**	**.439*** **
Género	.287	.255	.139	1.149
Estado Civil	.223	.197	.201	1.222
Habilitações Concluídas	-.031	.087	-.059	.942
Habilitações a Frequentar	-.016	.050	-.046	.955
Situação Profissional	.083	.165	.072	1.074
Pertencer à área das TIC	-.493	.284	-.236	0.789
Conhecimento Informático	**.333**	**.131**	**.343**	**1.409***
Autocontrolo	**.680**	**.299**	**.298**	**1.347***
Associação Diferencial	**2.001**	**.404**	**.944**	**2.570*** **
Definições	**1.024**	**.250**	**.640**	**1.896*** **
Reforço Diferencial	**.729**	**.223**	**.723**	**2.060** **
X^2 + p	*292.097 ; p<.001*			
-2. Log Likelihood	*479.223*			
Nagelkerke R^2	*.534*			

*B= coeficientes não estandardizados; SE= erro padrão; β= coeficientes estandardizados; OR= odds ratio *p<.05; **p<.01; ***p<.001*

Na explicação dos comportamentos de *hacking* malicioso durante a vida, a variável mais forte é a associação diferencial. Os indivíduos que possuem amigos que se envolvem em atos de *hacking* malicioso têm uma chance 2.5 vezes mais elevada de, igualmente, se envolverem nestes comportamentos, do que indivíduos que não detêm estas amizades (*OR*=2.570; p<.001). No mesmo sentido, ser reforçado a agir de forma ilegal aquando do uso de um computador (*OR*= 2.060; p=.001) e possuir definições favoráveis ao crime (*OR*=1.896; p<.001), aumenta as chances de praticar comportamentos de *hacking* malicioso. Outras variáveis significativas

presentes neste modelo que influenciam a perpetração destes comportamentos são: os baixos níveis de autocontrolo (*OR*=1.347; *p*=.023); o conhecimento informático elevado (*OR*=1.409; *p*=.011); e faixas etárias mais novas (*OR*=.439; *p*<.001).

5.12. Fatores Explicativos do *Hacking Malicioso* (nos últimos 12 meses)

O procedimento das regressões logísticas para os atos de *hacking* malicioso nos últimos 12 meses foi feito à semelhança do realizado para os comportamentos de *hacking* malicioso durante a vida.

5.12.1. Modelos Parcelares

- *Variáveis Sociodemográficas*

O modelo de regressão relativo às variáveis sociodemográficas é significativo (*p*<.001), e explica 23% (Nagelkerke R^2=.23) da variância da prática *hacking* malicioso dos últimos 12 meses (cf. Anexo VII). As variáveis significativas são: idade; estado civil; e conhecimento informático. Destaca-se que indivíduos que perspetivam o seu conhecimento informático como alto são mais propensos a reportar o cometimento de *hacking* malicioso (*OR*= 1.997; *p*<.001).

- *Autocontrolo*

Relativamente ao autocontrolo, o modelo parcial é significativo (*p*=.001), todavia, explica somente 2.5% (Nagelkerke R^2=.025) do cometimento dos comportamentos, verificando-se um decréscimo face ao modelo do autocontrolo durante a vida. Quanto ao poder preditivo da variável, mantém-se o resultado de que indivíduos com níveis mais baixos de autocontrolo apresentam uma maior probabilidade de se envolverem em atos maliciosos durante o último ano (*OR*=1.359; *p*=.002) (cf. Anexo VIII).

- *Componentes Aprendizagem Social*

Tal como para os atos durante a vida, também o modelo parcelar das componentes da aprendizagem social para os atos de *hacking* dos últimos 12 meses é significativo (*p*=.001), continuando a ser o conjunto de variáveis com maior poder preditivo isolado (Nagelkerke R^2=.315). Embora as três componentes sejam significativas e com valores de *Odds Ratio* semelhantes, tal como nos comportamentos de *hacking* durante a vida, destaca-se o papel da associação diferencial (*OR*=2.040; *p*<.001). Todavia, ser reforçado a agir de forma não ética ou ilegal quando se usa um computador ou se navega na *internet*, aumenta em 1.5 vezes mais a probabilidade de cometer este atos maliciosos, face a indivíduos que não são alvo de um reforço (*OR*=1.50; *p*<.001). Um similar valor preditivo é encontrado para indivíduos que possuem maior concordância com definições pró-criminais (*OR*=1.51; *p*<.05) (cf. Anexo IX).

5.12.2. Modelo Final

Pela observação da Tabela 20 conclui-se que o modelo final das variáveis independentes consegue explicar cerca de 38% (Nagelkerke R^2=.376) dos comportamentos de *hacking* malicioso praticados nos últimos 12 meses, sendo um modelo significativo (p<.001).

Tabela 20: Modelo Preditor Final dos Comportamentos de Hacking Malicioso (nos últimos 12 meses)

Variáveis	Modelo Final			
	B	**SE**	**β**	**OR**
Idade	**-.072**	**.026**	**-.900**	**.406***
Género	-.149	.274	-.072	.930
Estado Civil	.343	.219	.310	1.363
Habilitações Concluídas	-.096	.102	-.182	.8336
Habilitações a Frequentar	.001	.057	.003	1.003
Situação Profissional	.022	.188	.019	1.019
TIC	-.095	.342	-.045	.955
Conhecimento Informático	**.494**	**.160**	**.509**	**1.663****
Autocontrolo	.216	.300	.094	1.098
Associação Diferencial	**1.295**	**.280**	**.611**	**1.842*****
Definições	.437	.236	.273	1.313
Reforço Diferencial	**.395**	**.141**	**.392**	**1.479****
X^2 + p	*170.456 ; p<.001*			
-2. Log Likelihood	*477.837*			
Nagelkerke R^2	*.376*			

B= coeficientes não estandardizados; SE= erro padrão; β= coeficientes estandardizados; OR= odds ratio
**p<.05; **p<.01; ***p<.001*

Do modelo final em análise, tal como no modelo de *hacking* malicioso durante a vida, a associação diferencial é o preditor mais forte (*OR*=1.842; p<.001). Encontra-se, igualmente, que indivíduos que detêm níveis mais elevados de conhecimento informático (*OR*=1.663; p=.002), indivíduos mais jovens (*OR*=.406; p=.005) e indivíduos mais reforçados a agir ilegalmente quando usam um computador ou a *internet* (*OR*=1.479; p=.005) são mais propensos a cometer *hacking* malicioso. Salienta-se que neste modelo o autocontrolo e as definições deixam de ser variáveis significativas na explicação da variável dependente.

5.13. Modelo de Mediação entre Autocontrolo, Associação Diferencial e *Hacking* Malicioso

Pretendeu-se também compreender se existe um efeito indireto entre o autocontrolo e os comportamentos de *hacking* malicioso, pela via da associação diferencial. Ou seja, o propósito é testar se existe um efeito indireto da variável independente na variável dependente, através de uma variável mediadora (Hayes, 2018). Para tal, com recurso à extensão *PROCESS* do *SPSS*, realizou-se um modelo de mediação simples ou modelo 4 (Hayes, 2012, 2013), no qual a variável independente (*X*) é o autocontrolo, a variável dependente (*Y*) é o *hacking* malicioso e a variável mediadora (*M*) é a associação diferencial (cf. Anexo X).

5.13.1. Modelo de Mediação – Hacking Malicioso durante a vida

O modelo de mediação demonstra que não existe uma relação direta significativa entre o autocontrolo e os comportamentos de *hacking* malicioso durante a vida (*p*=.193). Embora não esteja presente esta relação, a associação diferencial enquanto variável mediadora produz um efeito indireto positivo e estatisticamente significativo, dado que o intervalo de confiança de 95% não inclui o valor 0 nos seus limites (.056 - .143). Este resultado é indicador de um modelo significativo (Hayes, 2012) (cf. Anexo XI).

5.13.2. Modelo de Mediação – Hacking Malicioso nos últimos 12 meses

À semelhança do modelo de mediação realizado anteriormente, não foi encontrada uma relação direta significativa entre o autocontrolo e o *hacking* malicioso cometido nos últimos 12 meses (*p*=.758). Contudo, o efeito indireto é positivo e estatisticamente significativo, sendo que o intervalo de confiança (95%) situa-se entre .031 e .102 (cf. Anexo XII).

DISCUSSÃO

A presente dissertação teve o propósito de analisar o cometimento de *hacking* malicioso reportado no contexto português, procurando testar a capacidade preditiva das componentes de duas teorias criminológicas (Teoria Geral do Crime de Gottfredson & Hirschi, 1990, e Teoria da Aprendizagem Social de Akers, 1998), percebendo se podem ser vistas como explicativas dos referidos comportamentos. Para tal, foi realizada uma investigação quantitativa, administrando um questionário *online* a uma amostra de 680 participantes.

Nos últimos anos, observa-se um elevado crescimento do uso diário dado às TIC, existindo uma relação de 'dependência' face a estas tecnologias. Isto, facilitou a emergência da cibercriminalidade, como é o caso dos comportamentos de *hacking*. Estes atos (*e.g.,* DDoS) fazem parte das principais formas de exploração de fragilidades informáticas e de violação de

dados (HackerOne, 2022; Hiscox, 2022), no qual os danos são sentidos não apenas em termos económicos, mas, também, ao nível do sentimento de insegurança (Chang & Whitehead, 2022). Embora seja um dos ilícitos mais imprevisíveis e danosos atualmente, o conhecimento que se possui acerca do *hacking* (legal, estatístico, teórico e/ou empírico) encontra-se subdesenvolvido (Chang & Whitehead, 2022), especialmente no contexto português, no qual, até à data e do nosso conhecimento, não existe nenhum estudo empírico que se foque inteiramente nos comportamentos de *hacking* malicioso, no seu ofensor e nos fatores explicativos.

Posto isto, considera-se pioneira esta investigação, dado que analisa um objeto de estudo pouco explorado, fornece resultados relevantes para a compreensão do fenómeno em Portugal, permite evoluir os conhecimentos criminológicos pela testagem de premissas teóricas e proporciona *insights* importantes para a área do cibercrime e da cibersegurança. De modo a facilitar a compreensão dos resultados apresentados previamente, o presente capítulo divide-se em: i) *hacking* malicioso e variáveis explicativas; ii) limitações e *guidelines* para investigações futuras; iii) implicações nas estratégias de atuação.

i) *Hacking* Malicioso e Variáveis Explicativas

No presente estudo, 60.4% dos participantes afirmou ter cometido, pelo menos, um comportamento de *hacking* malicioso durante a sua vida, e 23.2% durante os últimos 12 meses, sendo valores relativamente superiores aos que têm sido obtidos na comunidade científica (*e.g.,* 7.6% para o período da vida no estudo de Fox & Holt, 2021 e, 5.4% para o período dos últimos 12 meses no estudo de Holt *et al.,* 2020). Todavia, na análise individual dos comportamentos, os resultados são similares aos estudos de Holt e colaboradores (2012) e de Skinner e Fream (1997), destacando-se a tendência para a "tentativa ou adivinhar *passwords* para aceder a um computador ou conta *online* de outra pessoa sem a sua autorização", contando com mais de 50% da amostra a reportar esta prática, tal como encontrado no presente estudo (54.9%). A perpetuação dos comportamentos de *hacking* analisados foi reportada por indivíduos que partilham entre si certas caraterísticas sociodemográficas, possibilitando a construção de um perfil comum – indivíduos jovens, solteiros e empregados do sexo masculino. Ademais, relacionam-se com a área das TIC e identificam o seu conhecimento informático como elevado.

Estes dados encontram semelhanças com achados internacionais (*e.g.,* Bachmann, 2010; Fox & Holt, 2021; HackerOne, 2020), todavia, nos modelos de regressão, somente a idade e o conhecimento informático se apresentaram como significativos em ambos os períodos temporais analisados. De facto, os dados sobre a idade fornecem *insights* importantes, não só

sobre a prática atual de *hacking*, mas igualmente do momento da sua iniciação. Constatou-se que a idade média de início dos comportamentos foi de 15 anos – o pico da adolescência. Contudo, embora existam indivíduos que identifiquem a primeira prática em idades precoces (*e.g.,* 6 anos), assiste-se, igualmente, a participantes reportarem a faixa etária dos 40 anos como o período em que cometeram *hacking* pela primeira vez. Como tal, contrariamente a outros fenómenos criminais, na sua generalidade, o *hacking* malicioso não deverá ser visto como uma *"outra forma de crime ou delinquência juvenil"* (Bossler & Burruss, 2011, p. 59), dado que mesmo que se associe a indivíduos jovens, os comportamentos relacionam-se igualmente com o emprego, detenção de um conhecimento informático elevado (*e.g.,* Holt *et al.,* 2020; Steinmetz, 2016; Woo, 2003), caraterísticas que não são congruentes com a adolescência. Neste seguimento, torna-se crucial analisar, individualmente, amostras juvenis e amostras mais velhas, de modo a entender quais as suas diferenças e semelhanças (Bossler & Burruss, 2011).

De modo a incidir nos principais objetivos do estudo, e assim contribuir com dados empíricos para os conhecimentos que a comunidade científica possui sobre o *hacking* malicioso, a presente investigação procurou perceber qual a capacidade explicativa do autocontrolo e das componentes da aprendizagem social (associação diferencial, definições e reforço diferencial) nos comportamentos.

No que concerne ao autocontrolo, testou-se a hipótese de que (1) *indivíduos com níveis mais baixos de autocontrolo encontram-se mais propensos a praticar hacking malicioso.* No presente estudo, o autocontrolo apresenta-se como uma das variáveis principais nos modelos finais, porém, destaca-se nos modelos isolados, dado que indivíduos que possuem níveis baixos de autocontrolo apresentam quase 2 vezes mais probabilidade de cometer *hacking,* comparativamente a indivíduos com níveis mais elevados *(OR*= 1.944; p<.001) tal como encontrado no estudo de Holt e colegas (2021) (*OR*=2.263; p<.001). Como tal, os dados obtidos direcionam-se na confirmação desta hipótese, indo ao encontro do que tem sido concluído nos estudos internacionais (*e.g.,* Holt & Steinmetz, 2021; Kim *et al.,* 2022). Estes resultados podem ser explicados retomando as ideias de Gottfredson e Hirschi (1990), no qual o cometimento do crime se relaciona com os baixos níveis de autocontrolo, por intermédio dos aspetos que caraterizam este conceito (*e.g.,* gratificação imediata, tarefas fáceis, propensão para o risco).

Especificamente no caso do *hacking* malicioso, derivada da motivação que se tem para o cometer, o objetivo pode ser cumprido de uma forma imediata (*e.g., script kiddies* podem satisfazer os seus 'desejos' simplesmente por fazerem o *download* de um vírus para o computador de alguém, dado que não lhes interessa a sofisticação e tipo de tecnologia envolvida

no ataque). Ademais, algumas formas de *hacking* podem ser relativamente simples e fáceis de executar, como *shoulder-surfing* (*i.e.,* olhar para o telemóvel ou computador de alguém para ver a *password*) ou mesmo tentar adivinhar a *password* pelo método de tentativa e erro (Taylor *et al.,* 2014). A prática de *hacking* malicioso pode encontrar relação com a propensão para o risco, já que, anteriores investigações (*e.g.,* Taylor *et al.,* 2014) verificaram que os *hackers* procuram a excitação e adrenalina na realização do comportamento, e quando o ato não consegue fornecer estes estímulos, os indivíduos param de os praticar, sentindo-se aborrecidos (Gordon, 1994). Outro aspeto que é demonstrado por alguns estudos (*e.g.,* Rogers, 2001; Chua & Holt, 2016) é o facto dos *hackers* maliciosos não se importarem com os efeitos negativos que os seus comportamentos acarretam, nos quais muitas vezes recorrem a técnicas de neutralização para afastar a sua responsabilidade pelo ato (*e.g.,* negação do dano) (Turgeman-Goldschimdt, 2005). Por exemplo, Jordan e Taylor (1998) constataram que os *hackers* tendiam a culpar a vítima por esta não conseguir evitar o ataque e não possuir as capacidades tecnológicas necessárias para se defender. Estes dados conseguem demonstrar a autocentração abordada por Gottfredson e Hirschi (1990) na sua teoria, na medida em que o criminoso se mostra insensível e indiferente aos outros, especialmente no que concerne ao seu sofrimento.

Embora a relação apareça bem estabelecida, algumas inconsistências têm sido encontradas, nomeadamente a existência de uma relação entre níveis mais elevados de autocontrolo e a prática de *hacking* malicioso, contrariando o pressuposto central da TGC. A este nível, estudos empíricos que recorrem a participantes com mais conhecimentos tecnológicos e analisam comportamentos de *hacking* mais sofisticados (*e.g.,* Bossler & Burruss, 2011; Holt & Kilger, 2008), de facto encontram este tipo de relação, não sendo congruente com o perfil criminal estabelecido por Gottfredson e Hirschi (1990). Tal resultado pode ser explicado à luz do tipo de comportamentos operacionalizados (*e.g.,* criação de um *malware*) necessitarem de habilidades técnicas, preparação e foco na recompensa futura, dado que não são atos fáceis de executar. Logo, torna-se crucial analisar isoladamente os comportamentos de *hacking* malicioso, onde, pelas ideias abordadas acima, se pode concluir que afeta os resultados obtidos ao nível do autocontrolo.

Um dos enfoques da literatura científica é a testagem e análise das componentes da aprendizagem social no *hacking* malicioso, tendo sido encontrados resultados relevantes em torno da associação diferencial, das definições e do reforço diferencial (*e.g.,* Morris & Blackburn, 2009; Skinner & Fream, 1997). Posto isto, primeiramente, procurou testar-se se (2) *existe uma relação positiva entre a associação a pares desviantes e a prática de hacking*

malicioso. Múltiplos estudos (*e.g.,* Nodeland & Morris, 2020; Skinner & Fream, 1997) têm demonstrado o papel relevante da associação a pares desviante nestas práticas nocivas, destacando-se de entre as outras componentes da aprendizagem social. A título de exemplo, Marcum e colegas (2014) encontraram que a associação aumentou em 7% a probabilidade de aceder à conta *facebook* de alguém e, em 10% de aceder a um *website* de forma não autorizada. Neste prisma, a presente investigação encontrou valores robustos e significativos, tornando possível confirmar a hipótese proposta. Como tal, obteve-se que a associação a outros *hackers* influencia o envolvimento nestes comportamentos, uma vez que a associação a pares desviantes, seja *online* ou *offline*, aumenta a probabilidade de praticar atos de *hacking* malicioso (Skinner & Fream, 1997). Todavia, de que modo ocorre esta relação?

Considerando os pressupostos da TAS, os *hackers* adquirem as capacidades e os conhecimentos tecnológicos através do contacto com os *hackers* mais experientes, que por sua vez os 'treinam' e lhes transmitem a informação necessária para realizar comportamentos de *hacking* (Bossler & Burruss, 2011). Embora estas relações não possuam, maioritariamente, a proximidade física entres os indivíduos (Jordan & Taylor, 1998), esta nem sempre parece ser necessária, dado que mesmo que as relações proximais ocorram em fóruns *online*, estas são vistas pelos jovens *hackers* como essenciais para a aprendizagem das técnicas de ação, para o estabelecimento de laços e para o aprofundamento do sentimento de pertença à 'subcultura' (Skinner & Fream, 1997).

Seguidamente, testou-se (3*) se não existe uma relação significativa entre o reforço diferencial e a prática de hacking malicioso*. Os resultados obtidos não permitem comprovar esta hipótese, no qual se obteve uma relação positiva e significativa entre os níveis de reforço e a prática de *hacking* em diversos testes estatísticos. Ao nível da evidência empírica, os resultados têm sido mistos, já que embora seja perspetivada como uma variável de relevo na explicação do *hacking* malicioso (*e.g.,* Bossler & Burruss, 2011; Holt *et al.,* 2010), os resultados obtidos nem sempre são significativos (*e.g.,* Nodeland & Morris, 2020; Skinner e Fream, 1997). Não obstante existirem inconsistências na comunidade científica, o presente estudo aproxima-se do que é elencado por Akers (1998, 2010) na sua teoria, uma vez que a existência de reforço aumenta a prática dos comportamentos analisados. Tal dado pode ser explanado à luz da *Hacking Culture*, no qual os seus membros encorajam e reforçam positivamente os *hackers* bem-sucedidos, prometendo mais estatuto e reconhecimento por parte da subcultura (Holt, 2009; Jordan & Taylor, 1998). Assim, e à semelhança do que estipula o autor, os *hackers* que

são elogiados e recompensados pelos seus atos, irão sentir maior pertença à comunidade e continuarão a realizar tais comportamentos (Akers, 2010; Bossler & Burrus, 2011).

Ainda relacionado com as componentes da TAS, propôs-se a hipótese de que (4) *indivíduos com mais definições favoráveis ao crime tendem a praticar mais comportamentos de hacking malicioso*. Esta é uma das componentes do processo de aprendizagem social que tem ganho destaque nas investigações desta área, sendo vista como um preditor de relevo no cibercrime e, em concreto no *hacking* (*e.g.,* Bossler & Burruss, 2011; Holt *et al.,* 2010). No presente estudo é possível confirmar esta premissa, dado que se encontrou nos *hackers* maliciosos uma maior concordância com definições pró-criminais, ao contrário dos *hackers* não maliciosos. Contudo questiona-se: porque é que são os *hackers* maliciosos que apresentam esta maior concordância? Retomando a ideia de associação a outros *hackers*, é nestas relações que são transmitidas não só as formas de agir, mas igualmente as formas de pensar, moldando o raciocínio dos indivíduos. Isto significa que o *hacker,* ao estar envolvido na subcultura, será exposto aos pensamentos, valores e afirmações concordantes com um estilo de vida desviante, que por si só se afastam das normas sociais e legais (Taylor *et al.,* 2014). Ademais, e como abordado no autocontrolo, os indivíduos podem já possuir técnicas de neutralização, que agem como mecanismos de defesa e, acabam por se solidificar na relação com os outros (Turgeman-Goldschimdt, 2005).

Por fim, como forma de seguir a análise integrada que tem sido efetuada por parte da comunidade científica entre as diferentes variáveis em estudo, procurou analisar-se se a (5) *relação existente entre o autocontrolo e prática de hacking malicioso é mediada pela associação a pares desviantes.* Com os resultados advindos do modelo de mediação, é possível confirmar a hipótese, tendo-se verificado que o efeito direito entre o autocontrolo no *hacking* malicioso não é significativo, mas quando se analisa o efeito indireto por intermédio da associação diferencial, a relação torna-se significativa. Assim, conclui-se que a relação existente entre o baixo autocontrolo e o envolvimento no *hacking* malicioso se modifica quando se insere a associação diferencial no modelo de análise. Como apresentado previamente, a evidência empírica tem demonstrado o baixo autocontrolo como um preditor robusto do *hacking*, todavia, este papel altera-se quando se adiciona a associação diferencial à equação (*e.g.,* Marcum *et al.,* 2014). O estudo de Bossler e Burruss (2011) elucida esta questão, no qual *"o baixo autocontrolo teve no hacking uma maior influência indireta, através do processo de aprendizagem social, do que um efeito direto isolado"* (p. 55). Todavia, tem de se procurar a

razão pelo qual o papel do baixo autocontrolo se altera quando é controlada ou adicionada a associação diferencial.

Considerando os indivíduos com baixos níveis de autocontrolo, segundo Gottfredson e Hirschi (1990) pode-se postular que estes se encontram mais propensos para auto selecionar relações com pares semelhantes a si, no qual esta associação pode, eventualmente, desencadear o cometimento de atos desviantes e criminais em grupo. Relacionando esta premissa com o *hacking* malicioso, pode-se concluir que sujeitos com níveis mais baixos de autocontrolo, ao se envolverem com indivíduos que praticam *hacking*, iniciam uma imersão no processo de aprendizagem, no qual aprendem as definições pró-criminais e o *modus operandi* com os outros *hackers*, sendo constantemente reforçados socialmente a agir de forma criminal (Bossler & Holt, 2010). Contudo, se o processo de aprendizagem social for controlado, especialmente retirando a componente da associação diferencial, reflete-se que os indivíduos não têm forma de aprender as técnicas e o conjunto de valores que regem os *hackers* maliciosos, logo, será necessário que estes indivíduos tenham níveis mais elevados de autocontrolo, de modo a conseguirem aprender por si próprios e, assim, cometer estes comportamentos (Bossler & Burruss, 2011).

Porém, este argumento acaba por contradizer algumas premissas de Gottfredson e Hirschi (1990), designadamente: a) indivíduos com níveis mais elevados de autocontrolo não cometem crime; b) no crime não há nada que requeira a transmissão de habilidades ou conhecimentos por parte de outras pessoas. Nisto, embora sejam firmes nestas ideias, Gottfredson e Hirschi (1987) fornecem um argumento que pode ser adaptado à relação de mediação, afirmando que *"as pessoas adquirem a propensão para a delinquência, encontram amigos delinquentes e depois cometem atos delinquentes, incluindo atos criminais graves"* (p. 597), sendo algo encontrado no presente estudo e noutros internacionais (*e.g.,* Bossler & Burrus, 2011). Posto isto, a relação entre as três variáveis não se encontra sedimentada, existindo abertura para dúvidas e incongruências, o que sugere que o *hacking* é um fenómeno complexo e único, que necessita da redefinição e adaptação de alguns argumentos dos racionais teóricos analisados.

Concluindo, pelos resultados apresentados e a posição de concordância ou discordância em relação às premissas teóricas e aos resultados de investigações internacionais, compreende-se que das variáveis independentes analisadas, as que apresentam mais relevo são as inerentes ao processo de aprendizagem social – associação diferencial, definições e reforço diferencial. Estas componentes, além de serem as variáveis mais correlacionadas com os comportamentos

de *hacking* malicioso em ambos os períodos temporais analisados, são igualmente as que apresentam uma maior capacidade preditiva, dado que os seus modelos parcelares conseguiram explicar entre 31% e 47% da prática de atos maliciosos. Assim, é possível afirmar que no presente estudo empírico, à semelhança dos resultados obtidos por outras investigações, os elementos da teoria de Akers (1998), enquanto fatores sociais e externos aos indivíduos, conseguem explicar e prever este tipo de cibercrime, de forma mais relevante e precisa, do que caraterísticas intrínsecas dos indivíduos, como é o caso do autocontrolo proposto por Gottfredson e Hirschi (1990).

ii) Limitações e *Guidelides* para Investigações Futuras

Embora a investigação proporcione resultados relevantes e significativos sobre os fatores explicativos do *hacking* malicioso, a mesma não está isenta de algumas limitações. Primeiramente, tanto a operacionalização e medição do *hacking,* como das componentes da aprendizagem social, foi executada a partir da conceção de escalas, e não a utilização de outras já existentes e validadas, como sucedeu no caso do autocontrolo. Ou seja, partindo dos estudos empíricos e *guidelines* internacionais, foram adaptados itens e formas de medir as variáveis em causa, resultando na criação da Escala de *Hacking* Malicioso (durante a vida e nos últimos 12 meses) e das Escalas de Associação Diferencial, de Definições e de Reforço Diferencial. Posto isto, apesar de atribuir um caráter inovador ao estudo, podendo essas escalas serem úteis em futuras investigações, é necessário ter cautela no momento de interpretação dos resultados, dado que nenhuma outra investigação mediu de forma igualitária as variáveis. Não obstante, na sua validação para o contexto português, os resultados de fiabilidade foram satisfatórios, no qual contou com alfas entre .70 e .80 (*hacking* malicioso e definições), entre .80 e .90 (associação diferencial) e superiores a .90 (reforço diferencial), sendo valores mais elevados que os encontrados noutras investigações empíricas (*e.g.,* Holt *et al.,* 2010; Skinner & Fream, 1997). Contudo, será crucial proceder a uma replicação do estudo.

Outra limitação prende-se com a amostra em causa. O objetivo era que se cumprisse o requisito dos participantes pertencerem ou terem pertencido à área das TIC, sendo o tipo de indivíduos que os estudos empíricos têm inquirido (*e.g.,* Skinner & Fream, 1997). Todavia, como algumas universidades e escolas profissionais colocaram entraves à disseminação do questionário pelos cursos específicos subjacentes a esta área, o mesmo acabou por ser respondido por pessoas sem relação às TIC (38.2% da amostra). Ademais, a não obtenção de aval positivo por parte da maioria das empresas com a qual se tentou estabelecer contacto,

contribuiu para a dificuldade sentida em fazer chegar o questionário à amostra pretendida. Contudo, como o inquérito tinha uma pergunta de 'filtro' (ser ou não da área das TIC), foi possível dividir a amostra e perceber a relação desta área com o *hacking* malicioso.

Por fim, como a variável dependente remete para comportamentos criminais auto-reportados, salienta-se que há sempre o risco de as questões terem sido respondidas de forma desejável ou inibida, mesmo controlando esta variável. Além disto, obteve-se respostas com informação não válida, que acabaram por ser excluídas durante o processo de *screening* estatístico.

Elencadas as limitações, seguem-se as *guidelines* para a investigação futura. Em primeiro lugar, salienta-se a necessidade de conhecer melhor o contexto de atuação dos *hackers* maliciosos, de modo a facilitar o encontro destes indivíduos e a sua participação nos estudos empíricos. Ademais, as variáveis em estudo conseguem explicar, no seu conjunto, cerca de 53% dos comportamentos de *hacking* malicioso, logo falta perceber que outros aspetos podem estar na base desta explicação, tais como a personalidade ou outros fatores de índole mais contextual. Referente aos objetivos que guiam o estudo, como a presente investigação analisou o *hacking* malicioso, um dos próximos passos a seguir é a análise do *hacking* ético (Holt, 2020), nomeadamente tentar estabelecer: i) a prevalência destes comportamentos na sociedade portuguesa; ii) um perfil dos *hackers* éticos, contrastando com os resultados obtidos quanto aos *hackers* maliciosos; iii) se as premissas da TGC e da TAS detêm capacidade preditiva nos comportamentos éticos. Relacionado com estes aspetos, seria crucial realizar uma abordagem mais proximal com os participantes (tanto maliciosos como éticos), por exemplo, pelo uso de entrevistas, dado que permitem obter um tipo de informação mais detalhada, do que a obtida por questionários (Maxfield & Babbie, 2014).

iii) Implicações nas Estratégias de Atuação

Por fim, nesta discussão abordam-se quais as estratégias a adotar, na prática, para lidar com os comportamentos de *hacking* malicioso. Com o enraizamento das tecnologias digitais na vida diárias dos cidadãos, os ciberataques são dirigidos tanto a organizações, como a indivíduos singulares, ocorrendo consequências nefastas ao nível dos dados e infraestruturas informáticas. Posto isto, a contínua realização de estudos empíricos sobre o *hacking* é imprescindível para aumentar o conhecimento que se detém sobre o fenómeno e, melhorar e atualizar as formas de agir contra estes ataques, seja de índole preventiva ou reativa.

Relativamente às empresas, estas têm de adaptar as suas estratégias de defesa informática aos novos contornos que estes ataques possuem. Para tal, a cibersegurança tem de estar no centro dos objetivos da empresa, seja em termos de alcance e sofisticação dos dispositivos informáticos, seja em termos de recursos humanos. Este último ponto deve ser o foco das organizações, incluindo postos de trabalho para *hackers* éticos (*white-hat hackers*), de modo a protegerem os sistemas informáticos de potenciais ataques e contra-atacar os mesmos (Nicholson, 2019). A ação destes indivíduos encontra-se regulamentada pela empresa e assenta num contrato ou acordo entre o *hacker* e a organização. Nisto, as principais funções devem focar-se na segurança da informação (*e.g.,* proteger de acesso não autorizado), na aplicação da segurança (*e.g.,* uso de *softwares*), na segurança operacional (*e.g.,* procedimentos de acesso a determinada informação), na segurança da *cloud (e.g*., proteger a *cloud* de ataques) e ajudar os colegas de trabalho a detetarem violações de dados (*e.g.,* ensinar a remover um ficheiro suspeito) (Li & Liu, 2021).

No caso dos indivíduos singulares, grande parte dos cidadãos não possui conhecimentos necessários para realizar uma proteção eficaz ao nível informático. Aqui a aposta será em medidas preventivas[3], nomeadamente: i) informar as pessoas sobre o *hacking* malicioso, os tipos de comportamentos e as formas como estes ataques podem ser realizados; ii) informar como agir preventivamente, nomeadamente ao nível da proteção do computador (*e.g.,* instalação e atualização de antivírus) e da proteção de contas *online* (*e.g.,* criação de *passwords* fortes e armazenamento das mesmas). Esta atuação preventiva torna-se crucial no dia a dia das pessoas, dado que é improvável que alguém suspeite de um ataque, e somente tenha conhecimento do mesmo quando ocorrem consequências notáveis (*e.g.,* levantamento de dinheiro da conta bancária, furto ou eliminação de ficheiros que se tinha num computador). A partilha de informação referida pode ser feita através de palestras, *workshops* e cursos, nomeadamente dirigidos a escolas, universidade e empresas, de modo a transmitir ideias sobre a navegação segura na *internet*, formas de proteger a informação e identidade digital, e ressalvar que os comportamentos de *hacking* malicioso são um crime. Isto deve acontecer especialmente junto dos jovens, dado que o início do envolvimento no *hacking* malicioso se associa ao período da adolescência.

Ademais, relacionada com esta última premissa, uma vez que a presente investigação elencou o papel de relevo da associação a pares desviantes e a presença de definições pró-

[3] Em Portugal ressalva-se que estas práticas têm sido realizadas por algumas entidades, como o Centro Nacional de Cibersegurança, onde o site contém elementos de sensibilização (*site:* https://www.cncs.gov.pt/).

criminais na prática de *hacking* malicioso, será importante apostar em formas de identificar estes grupos de indivíduos, por exemplo, em meio escolar, e procurar alterar as crenças 'desviantes' existentes através de programas de intervenção.

Por fim, dada a carência de conhecimento sobre o *hacking* (malicioso e ético), emerge a necessidade de interligar os saberes teóricos e empíricos da Criminologia com os saberes práticos da área das TIC (*e.g.,* programação, informática), dado que o conhecimento e atuação eficaz neste fenómeno requer uma abordagem multidisciplinar.

REFERÊNCIAS BIBLIOGRÁFICAS

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston: Northeastern University Press.

Akers, R. L. (2010). *Social learning and social structure: A general theory of crime and deviance*. Transaction Publishers.

Akers, R. L. (2012). Social Bonding and Control Theories. In *Criminological Theories: Introduction and Evolution* (5th ed., pp. 79-97). Routledge.

Akers, R. L., & Jennings, W. G. (2016). Social Learning Theory. In A. R. Piquero (Ed.), *The handbook of criminological theory*, (pp. 230-240). John Wiley & Sons.

Aluja, A., García, Ó., & García, L. F. (2003). A psychometric analysis of the revised Eysenck Personality Questionnaire short scale. *Personality and individual differences*, 35(2), 449-460.

Amador, N. J. R. (2012). *Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro* (Doctoral Thesis in Instituto Superior de Ciências Policiais e Segurança Interna). http://hdl.handle.net/10400.26/17168.

Arneklev, B. J., Elis, L., & Medlicott, S. (2006). Testing the General Theory of Crime: Comparing the Effects of "Imprudent Behavior" and an Attitudinal Indicator of "Low Self-Control". *Western Criminology Review*, *7*(3), 41-55.

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 and rationality of computer hackers. *International Journal of Cyber Criminology*, *4*(1), 643-656.

Back, S., Soor, S., & LaPrade, J. (2018). Juvenile hackers: An empirical test of self-control theory and social bonding theory. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1*(1), 40-55.

Bandura, A. (1979). *Social Learning Theory.* Englewood Cliffs, NJ: Prentice Hall.

Barber, R. (2001). Hackers profiled: Who are they and what are their motivations? *Computer Fraud & Security, 2001*(2), 14–17.

Becker, H. (1963). *Outsiders: Studies in the Sociology of Deviance*. New York: Free Press.

Bossler, A. M., & Burruss, G. W. (2011). The general theory of crime and computer hacking: low self-control hackers?. In T. J. Holt & B. H. Schell (Eds.) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 38-67). 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.

Britt, C. L., & Rocque, M. (2016). Control as an Explanation of Crime and Delinquency. In A. R. Piquero (Ed.) *The Handbook of Criminological Theory* (pp. 182-208). John Wiley & Sons.

Britz, M. T. (2013). Introduction and overview of computer forensics and cybercrime. In *Computer Forensics and Cyber Crime: An Introduction* (Vol.3, pp. 1-20), South Carolina, Pearson.

Burgess, R. L., & Akers, R. L. (1966). A differential association-reinforcement theory of criminal behavior. *Social Problems, 14,* 128–147.

Burt, C. H. (2020). Self-control and crime: Beyond Gottfredson and Hirschi's theory. *Annual Review of Criminology*, *3*(1), 43-73.

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.

Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. In T. J. Holt & A. M. Bossler (Eds.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 27-43). Palgrave Macmillan, Cham.

Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims & Offenders*, *11*(4), 534-555.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offender's decisions: A framework for research and policy. *Crime and Justice*, *6*, 147-185.

CNCS (2022). *Relatório Cibersegurança em Portugal: Riscos e Conflitos* (Nº3). Observatório de Cibersegurança. Available at: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Lawrence Erlbaum Associates, Publishers.

Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3), 255-277.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.

Dias, V. M. (2012). A Problemática da Investigação do Cibercrime. *Revista Jurídica Digital, 1*, 63-88.

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior, 34*, 165–172.

Ferreira, J., & Guedes, I. S. (2021). Hacking: Evolução, Perfis e Explicações Criminológicas. In I. S., Guedes & M. I. M., Gomes (Eds.), *Cibercriminalidade: Novos Desafios, Ofensas e Soluções* (pp. 181-201). Pactor.

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. *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.

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

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud & Security*, *2015*(10), 5-12.

Gibson, C., & Wright, J. (2001). Low self-control and coworker delinquency: A research note. *Journal of criminal justice*, *29*(6), 483-492.

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

Gordon, S. (2000). Virus Writers: The end of the Innocence?. *IBM*, 1-20.

Gottfredson, M., & Hirschi, T. (1987). The methodological adequacy of longitudinal research on crime. *Criminology*, *25*(3), 581-614.

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

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.

Gunter, W. D. (2008). Piracy on the high speeds: A test of social learning theory on digital piracy among college students. *International Journal of Criminal Justice Sciences, 3*(1), 54-68.

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.

HackerOne (2022). *The 2022 Hacker Report.* Available at: https://www.hackerone.com/resources/reporting/the-2022-hacker-report.

Hald, S. L., & Pedersen, J. M. (2012). An Updated Taxonomy for Characterizing Hackers according to their Threat Properties. Proceedings of the *IEEE: 14th International Conference on Advanced Communication Technology,* 81-86. https://ieeexplore.ieee.org/document/6174615.

Hayes, A. F. (2012). PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling. *Guildfor Press*, 1-39.

Hayes, A. F. (2013). *Model templates for PROCESS for SPSS and SAS: a Regression Based Approach*. Guilford Press.

Hayes, A. F. (2018). Partial, conditional, and moderated moderated mediation: Quantification, inference, and interpretation. *Communication Monographs*, *85*(1), 4-40.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. *Criminal Justice Studies*, *19*(1), 3-22.

Hill, M. M., & Hill, A. (1998a). *A construção de um questionário*. Lisboa: Dinâmica.

Hill, M. M., & Hill, A. (1998b). *Investigação empírica em ciências sociais: Um guia introdutório.* Lisboa: Dinâmica.

Hiscox (2022). *Cyber Readiness Report 2022*. Available at: https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054%20-%20Hiscox%20Cyber%20Readiness%20Report%202022-EN_0.pdf.

Hollinger, R. C. (1991). Hackers: Computer Heroes or Electronic Highwaymen?. *Computers and Society*, *21*(1), 6-17.

Hollinger, R. C. (1992). Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access. *Security Journal*, *4*(1), 2-12.

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.

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. (2009). Lone hacks or group cracks: Examining the social organization of computer hackers. In F. J. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 336-355). Prentice Hall Press.

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, Cham.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice*, *37*(3), 378-395.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and digital forensics: An introduction*. Routledge.

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), 31-61.

Holt, T. J., Cale, J., Brewer, R., & Goldsmith, A. (2021). Assessing the Role of Opportunity and Low Self-Control in Juvenile Hacking. *Crime & Delinquency*, *67*(5), 662-688.

Holt, T. J., & Kilger, M. (2008). Techcrafters and makecrafters: A comparison of two populations of hackers. *Proceedings of the IEEE: WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, 67-78. https://ieeexplore.ieee.org/xpl/conhome/4627300/proceeding.

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.

IBM Security and Ponemon Institute (2022). *Cost of a Data Breach Report 2022*. Available at: https://www.ibm.com/downloads/cas/3R8N1DZJ.

Internet Telecommunication Union (2022). *Individuals using the Internet (% of population)*. Available at: https://data.worldbank.org/indicator/IT.NET.USER.ZS.

Internet World Stats (2022). *World internet usage and population statistics.* Available at: https://www.internetworldstats.com/stats.htm#links.

Jaquet-Chiffelle, D. O., & Loi, M. (2020). Ethical and unethical hacking. In M. Christen, B. Gordjin, & M. Loi (Eds.) *The Ethics of Cybersecurity* (pp. 179-204). Springer Nature.

Jordan, T. (2017). A genealogy of hacking. *Convergence*, *23*(5), 528-544.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780.

Kim, J., Leban, L., & Lee, Y. (2022). Theoretical Explanations of the Development of Youth Hacking. *Crime & Delinquency*, 1-22.

Landreth, B., & Rheingold, H. (1985). *Out of the inner circle: a hacker's guide to computer security*. Bellevue, Washington: Microsoft Press.

LeBlanc, M. (2006). Self-control and social control of deviant behavior in context: development and interactions along the life course. In P. H. Wikström & R. J. Sampson (Eds.). *The explanation of Crime* (pp. 124-151). Cambridge University Press.

Lei do Cibercrime (LC) - Lei no 109/2009 de 15 de setembro. Diário da República no 179/2009, Série I de 2009- 09-15.

Leukfeldt, R., Kleemans, E. R., & Stol, W. (2017). Origin, growth, and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime Law and Social Change*, *67*, 39-53.

Levy, S. (1984). *Hackers: Heroes of the computer revolution* (Vol. 14). Garden City, NY: Anchor Press/Doubleday.

Levy, S. (2001). *Hackers: Heroes of the computer revolution*. New York: Penguin.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

MacFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday*, *8*(9), 1-10.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, *2*(1), 191-216.

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. (2010). *Análise Estatística com utilização do SPSS*. Lisboa: Edições Silabo.

Maxfield, M. G., & Babbie, E. R. (2014). *Research methods for criminal justice and criminology*. Cengage Learning.

Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering*, *17*(3), 17-24.

McLeod, K. (2014). *Pranksters*. New York University Press.

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.

Miller, B., & Morris, R. G. (2016). Virtual peer effects in social learning theory. *Crime & Delinquency*, *62*(12), 1543-1569.

Moeckel, C. (2019). Examining and constructing attacker categorisations: an experimental typology for digital banking. *Proceedings of the ARES'19: 14th International Conference on Availability, Reliability and Security*, 1-6. https://dl.acm.org/doi/10.1145/3339252.3340341.

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.

Morris, R. G., & Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice*, *32*(1), 1-34.

Munck, G. L., & Verkuilen, J. (2005). Research designs. *Encyclopedia of social measurement*, *3*, 385-395.

Nasution, M. D. T. P., Rossanty, Y., Siahaan, A. P. U., & Aryza, S. (2018). The Phenomenon of Cyber-crime and Fraud Victimization in Online Shop. *International Journal of Civil Engineering and Technology*, *9*(6), 1583-1592.

Nicholson, S. (2019). How ethical hacking can protect organisations from a greater threat. *Computer Fraud & Security*, *2019*(5), 15-19.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New media & society*, *6*(2), 195-217.

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

Pallant, J. (2016). *A Step by Step Guide to Data Analysis using IBM SPSS* (6th ed.) McG-raw-Hill Education.

Payne, B. K. (2020). Defining Cybercrime. In T. J. Holt & A. M. Bossler (Eds.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1-25). Palgrave Macmillan, Cham.

Peacock, D. (2013). *From underground hacking to ethical hacking* (Doctoral Thesis in University of Northumbria). http://nrl.northumbria.ac.uk/id/eprint/32285.

Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology*, *38*(3), 931-964.

RASI (2022). *Relatório de Segurança Interna – Ano 2022*. Available at: https://www.portugal.gov.pt/pt/gc23/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2022-.

Resolução da Assembleia da República n.º 88/2009 de 15 de setembro. Diário da República n.º 70/2009, Série I de 2009-04-09.

Richet, J. L. (2013). From Young *Hacker*s to Crackers. *International Journal of Technology and Human Interaction*, *9*(3), 53-62.

Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study* (Doctoral Thesis in University of Manitoba). http://hdl.handle.net/1993/19563.

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

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.

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

Shadmanfaat, S. M., Howell, C. J., Muniz, C. N., Cochran, J. K., Kabiri, S., & Fontaine, E. M. (2020). Cyberbullying perpetration: An empirical test of social learning theory in Iran. *Deviant Behavior*, *41*(3), 278-293.

Sharma, R. (2007). Peeping into a Hacker's Mind: Can Criminological Theories Explain Hacking?. *SSRN,* 1-20.

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.

Snyder, F. (2001). Sites of criminality and sites of governance. *Social & Legal Studies*, *10*(2), 251-256.

Stalans, L. J., & Donner, C. M. (2018). Explaining Why Cybercrime Occurs: Criminological and Psychological Theories. In H. Jahankhani (Ed.) *Cyber Criminology* (pp. 25-45), Springer.

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime* (Vol. 2). NYU Press.

Sutherland, E. H. (1947). *Principles of Criminology.* (4th ed.). Philadelphia: J. B. Lippincott.

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

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.

Turgeman-Goldschmidt, O. (2005). Hacker's accounts: Hacking as a social entertainment. *Social Science Computer Review*, *23*(1), 8-23.

Turkle, S. (1984). *The Second Self: Computers and the Human Spirit.* Granada.

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.

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

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), 183-205.

Wall, D. S., & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology & Criminal Justice*, *7*(4), 391-415.

Wark, M. (2004). *A Hacker Manifesto*. Harvard University Press.

Wark, M. (2006). Hackers. *Theory, Culture & Society*, *23*(2-3), 320-322.

Winfree Jr, L. T., & Abadinsky, H. (2017). An Introduction to Criminological Theory. In *Essentials of criminological theory* (pp. 2-18). Waveland Press.

Woo, H. J. (2003). *The hacker mentality: Exploring the relationship between psychological variables and hacking activities* (Doctoral Thesis in University of Georgia) https://getd.libs.uga.edu/pdfs/woo_hyung-jin_200305_phd.pdf.

World Economic Forum (2023). *Global Cybersecurity Outlook 2023 – INSIGHT REPORT JANUARY 2023.* Available at: https://www.weforum.org/reports/global-cybersecurity-outlook-2023/?DAG=3&gclid=EAIaIQobChMImYuRlIu5_gIV1-TVCh3OrwPeEAAYASAAEgJwO_D_BwE.

Yar, M. (2006). *Cybercrime and society*. Sage Publications.

Yar, M. (2016). Online crime. In *Oxford Research Encyclopedia of Criminology and Criminal Justice* (pp. 1-27). Criminology and Criminal Justice.

Young, R., & Zhang, L. (2005). Factors affecting illegal hacking behavior. *AMCIS*, 3258-3264.

ANEXOS

Anexo I – Questionário

GRUPO I

1. **Género:**

☐ Feminino

☐ Masculino

☐ Outro: _____

2. **Idade (em anos): _____**

3. **Estado Civil:**

☐ Solteiro/a

☐ União de Facto

☐ Casada/a

☐ Ex-União de Facto

☐ Divorciado/a

☐ Viúvo/a

☐ Outro: _____

4. **Habilitações Literárias Concluídas:**

☐ 4.º ano

☐ 6.º ano

☐ 9.º ano

☐ 12.º ano

☐ Curso Profissional

☐ Licenciatura

☐ Pós-Graduação

☐ Mestrado

☐ Doutoramento

5. Habilitações Literárias a Frequentar:

- ☐ Nenhuma
- ☐ 4.º ano
- ☐ 6.º ano
- ☐ 9.º ano
- ☐ 12.º ano
- ☐ Curso Profissional
- ☐ Licenciatura
- ☐ Pós-Graduação
- ☐ Mestrado
- ☐ Doutoramento

6. Situação Profissional:

- ☐ Desempregado/a
- ☐ Empregado/a por conta
- ☐ Empregado/a por conta de outrem
- ☐ Estudante
- ☐ Trabalhador-Estudante
- ☐ Reformado/a
- ☐ Outro:_____

7. Trabalha ou estuda na área das Tecnologias de Informação e Comunicação (TIC)?

- ☐ Não
- ☐ Sim

8. Por favor, indique o seu nível de conhecimento informático:

- ☐ Baixo
- ☐ Médio-Baixo
- ☐ Médio

☐ Médio-Alto

☐ Alto

GRUPO II

9. Durante a sua *vida*, quantas vezes praticou os seguintes comportamentos?

	Nunca	1 a 2 vezes	3 a 5 vezes	6 a 9 vezes	10 ou mais vezes
Adivinhei ou tentei adivinhar passwords para aceder a um computador ou conta online de outra pessoa sem autorização					
Acedi a um computador ou conta online de outra pessoa sem autorização					
Adicionei, eliminei, alterei ou imprimi informação de um computador ou conta online de outra pessoa sem autorização					
Usei um *malware* para causar danos ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, *worms*)					

Criei um *malware* para causar danos ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, *worms*)					

10. Durante os *últimos 12 meses*, quantas vezes praticou os seguintes comportamentos?

	Nunca	**1 a 2 vezes**	**3 a 5 vezes**	**6 a 9 vezes**	**10 ou mais vezes**
Adivinhei ou tentei adivinhar passwords para aceder a um computador ou conta online de outra pessoa sem autorização					
Acedi a um computador ou conta online de outra pessoa sem autorização					
Adicionei, eliminei, alterei ou imprimi informação de um computador ou conta online de outra pessoa sem autorização					
Usei um *malware* para causar danos ou destruir dados num computador ou sistema de					

computadores (ex: vírus, *worms*)					
Criei um *malware* para causar danos ou destruir dados num computador ou sistema de computadores (ex: vírus, *worms*)					

11. Caso tenha selecionado a prática de algum dos comportamentos nas perguntas 10 e/ou 11, por favor, indique a idade aproximada em que o(s) praticou pela primeira vez: _____

12. Caso tenha selecionado a prática de algum dos comportamentos nas perguntas 10 e/ou 11, por favor, indique a principal fonte com que aprendeu esse(s) comportamento(s):

- ☐ Pais
- ☐ Família
- ☐ Professor/es
- ☐ Amigos
- ☐ Livros/Revistas
- ☐ Internet/*Sites* Online
- ☐ Outro: _____

GRUPO III

13. Quantos amigos seus se envolvem ou envolveram nos seguintes comportamentos?

	Nenhum	**Alguns**	**Metade**	**Mais de Metade**	**Todos**
Adivinhar ou tentar adivinhar passwords para aceder a um computador ou conta online de outra					

pessoa sem autorização					
Aceder a um computador ou conta online de outra pessoa sem autorização					
Adicionar, eliminar, alterar ou imprimir informação de um computador ou conta online de outra pessoa sem autorização					
Usar um *malware* para causar danos ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, *worms*)					
Criar um *malware* para causar danos ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, *worms*)					

14. Em que medida concorda ou discorda das seguintes afirmações quando utiliza um computador ou a internet?

	Discordo Totalmente	Discordo	Concordo	Concordo Totalmente
Como é contra a lei, eu nunca faria nada ilegal através de um computador				
É importante que as pessoas saibam o que podem ou não fazer com os recursos computacionais na escola e no local de trabalho				
Há regras claras do que é um comportamento online aceitável e ético				
Se as pessoas não querem que eu tenha acesso ao seu computador ou conta online, deveriam usar sistemas de segurança melhores				
Eu deveria ter acesso a qualquer tipo de informação que o governo, a escola, o emprego ou um indivíduo tem sobre mim, mesmo que eles não me deem acesso				
Nunca denunciaria um amigo meu por ter tido acesso não autorizado a um computador ou conta online de outra pessoa				

As pessoas que entram nos sistemas computacionais estão, na verdade, a ajudar a sociedade				

15. Relativamente às seguintes questões, por favor, selecione a opção com que mais se identifica:

	Nunca	**1 a 2 vezes**	**3 a 5 vezes**	**6 a 9 vezes**	**10 ou mais vezes**
Quantas vezes testemunhou um professor, chefe ou colega de trabalho a ter orgulho por ter utilizado um computador de forma não ética ou ter praticado atividades ilegais?					
Quantas vezes testemunhou um professor, chefe ou colega de trabalho a incentivar alguém para usar um computador de forma não ética ou para praticar atividades ilegais?					
Quantas vezes um professor, chefe ou colega de trabalho o/a incentivou a usar um computador de forma não ética ou a praticar atividades ilegais?					

GRUPO IV

16. Para as seguintes afirmações, por favor, selecione a opção com a qual mais se identifica:

	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 me 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 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 me 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				
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 e a pensar				
Gosto mais de sair e de fazer coisas do que ler e pensar				
Eu sinto que tenho mais energia e mais necessidade de atividade 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 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 zangado 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 V

17. Para cada pergunta, por favor, selecione a opção com a qual mais se identifica:

	Não	**Sim**
Se afirma que fará determinada coisa, mantém a promessa, mesmo que isso venha a ser inconveniente?		
Já alguma vez atribuiu as culpas a alguém, mesmo sabendo que a culpa era sua?		
Todos os seus hábitos são bons ou desejáveis?		
As boas maneiras e a limpeza são importantes para si?		
Já alguma vez ficou com alguma coisa (mesmo que insignificante) que pertencia a outra pessoa?		

Já alguma vez estragou ou perdeu algo que pertencia a outra pessoa?		
Já alguma vez falou mal, ou de forma maldosa, de alguém?		
Quando era criança alguma vez foi atrevido/a ou descarado/a para os seus pais?		
Já alguma vez fez batota ao jogo?		
Já alguma vez se aproveitou de alguém?		
Costuma fazer sempre aquilo que diz?		
Algumas vezes deixa para amanhã o que deveria fazer hoje?		

Anexo II – Codificação das Variáveis

VARIÁVEIS

Variáveis Sociodemográficas	Codificação
Género	
	Feminino (0)
	Masculino (1)
	Outro (2) – inclui: não binário;
Idade	
	Medida aberta
Estado Civil	
	Solteiro/a (1)
	União de Facto (2)
	Casado/a (3)
	Ex-União de Facto (4)
	Divorciado/a (5)
	Viúvo/a (6)
	Outro (7)
Habilitações Literárias Concluídas	
	4.º ano (1) a doutoramento (9)
Habilitações Literárias a Frequentar	
	Nenhuma (0) a doutoramento (9)
Situação Profissional	
	Desempregado/a (1)

	Empregado/a por conta própria (2) Empregado/a por conta de outrem (3) Estudante (4) Trabalhador-Estudante (5) Reformado/a (6) Outro (7) – inclui: investigador/a; estagiário/a; bolseiro/a;
TIC	
	Não (0) Sim (1)
Conhecimento Informático	
	Baixo (1) Médio-Baixo (2) Médio (3) Médio-Alto (4) Alto (5)
Comportamentos *Hacking* Malicioso	**Codificação**
***Hacking* durante a Vida**	
Adivinhei ou tentei adivinhar passwords para aceder a um computador ou conta online de outra pessoa sem autorização; *Acedi a um computador ou conta online de outra pessoa sem autorização;* *Adicionei, eliminei, alterei ou imprimi informação de um computador ou conta online de outra pessoa sem autorização;* *Usei um malware para causar dano ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, worms);* *Criei um malware para causar dano ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, worms);*	Nunca (0) 1 a 2 vezes (1) 3 a 5 vezes (2) 6 a 9 vezes (3) 10 ou mais vezes (4)
***Hacking* nos últimos 12 meses**	

Adivinhei ou tentei adivinhar passwords para aceder a um computador ou conta online de outra pessoa sem autorização; *Acedi a um computador ou conta online de outra pessoa sem autorização;* *Adicionei, eliminei, alterei ou imprimi informação de um computador ou conta online de outra pessoa sem autorização;* *Usei um malware para causar dano ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, worms);* *Criei um malware para causar dano ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, worms);*	Nunca (0) 1 a 2 vezes (1) 3 a 5 vezes (2) 6 a 9 vezes (3) 10 ou mais vezes (4)
Idade de Início de *Hacking*	
	Medida aberta
Componentes Aprendizagem Social	**Codificação**
Imitação	
	Pais (1) Família (2) Professor/es (3) Amigos (4) Livros/Revistas (5) Televisão/Filmes (6) Internet/*Sites* Online (7) Outro (8) – inclui: não sabe; autodidata;
Associação Diferencial	
Adivinhar ou tentar adivinhar passwords para aceder a um computador ou conta online de outra pessoa sem autorização; *Aceder a um computador ou conta online de outra pessoa sem autorização;* *Adicionar, eliminar, alterar ou imprimir informação de um computador ou conta online de outra pessoa sem autorização;*	Nenhum (1) Alguns (2) Metade (3) Mais de Metade (4) Todos (5)

Usar um malware para causar dano ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, worms);	
Criar um malware para causar dano ou destruir dados num computador ou sistema de computadores (por exemplo: vírus, worms);	
Definições	
Como é contra a lei, eu nunca faria nada ilegal através de um computador;	Discordo Totalmente (1) Discordo (2) Concordo (3) Concordo Totalmente (4)
É importante que as pessoas saibam o que podem ou não fazer com os recursos computacionais na escola e no local de trabalho;	
Há regras claras do que é um comportamento online aceitável e ético;	
Se as pessoas não querem que eu tenha acesso ao seu computador ou conta online, deveriam usar sistemas de segurança melhores;	
Eu deveria ter acesso a qualquer tipo de informação que o governo, a escola, o emprego ou um indivíduo tem sobre mim, mesmo que eles não me deem acesso;	
Nunca denunciaria um amigo meu por ter tido acesso não autorizado a um computador ou conta online de outra pessoa;	
As pessoas que entram nos sistemas computacionais estão, na verdade, a ajudar a sociedade;	
Reforço Diferencial	
Quantas vezes testemunhou um professor, chefe ou colega de trabalho a ter orgulho por ter utilizado um computador de forma não ética ou ter praticado atividades ilegais?	Nunca (1) 1 a 2 vezes (2) 3 a 5 vezes (3) 6 a 9 vezes (4) 10 ou mais vezes (5)
Quantas vezes testemunhou um professor, chefe ou colega de trabalho a incentivar	

alguém para usar um computador de forma não ética ou para praticar atividades ilegais? *Quantas vezes um professor, chefe ou colega de trabalho o/a incentivou a usar um computador de forma não ética ou a praticar atividades ilegais?*	
Autocontrolo	**Codificação**
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 me 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 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 me 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;*	Discordo Totalmente (1) Discordo (2) Concordo (3) Concordo Totalmente (4)

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 e a pensar;

Gosto mais de sair e de fazer coisas do que ler e pensar;

Eu sinto que tenho mais energia e mais necessidade de atividade 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 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 zangado 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;

Desejabilidade Social	**Codificação**
Se afirma que fará determinada coisa, mantém a promessa, mesmo que isso venha a ser inconveniente?	Não (0) Sim (1)
Já alguma vez atribuiu as culpas a alguém, mesmo sabendo que a culpa era sua?	

Todos os seus hábitos são bons ou desejáveis?

As boas maneiras e a limpeza são importantes para si?

Já alguma vez ficou com alguma coisa (mesmo que insignificante) que pertencia a outra pessoa?

Já alguma vez estragou ou perdeu algo que pertencia a outra pessoa?

Já alguma vez falou mal, ou de forma maldosa, de alguém?

Quando era criança alguma vez foi atrevido/a ou descarado/a para os seus pais?

Já alguma vez fez batota ao jogo?

Já alguma vez se aproveitou de alguém?

Costuma fazer sempre aquilo que diz?

Algumas vezes deixa para amanhã o que deveria fazer hoje?

Anexo III – Relações de Correlação (*pearson's r*) entre *Hacking* Malicioso, Autocontrolo e Componentes da Aprendizagem Social

Variáveis	*Hacking* durante a vida	*Hacking* nos últimos 12meses	Auto controlo	Associação Diferencial	Definições	Reforço Diferencial
***Hacking* durante a vida**	- -					
***Hacking* nos últimos 12meses**	0.639 <.001	- -				
Auto Controlo	0.147 <.001	0.074 0.073	- -			
Associação Diferencial	0.500 <.001	0.321 <.001	0.188 <.001	- -		
Definições	0.478 <.001	0.206 <.001	0.197 <.001	0.388 <.001	- -	
Reforço Diferencial	0.503 <.001	0.296 <.001	0.150 <.001	0.567 <.001	0.555 <.001	- -

Anexo IV – Modelo Parcelar 1 de *Hacking* Malicioso (durante a vida) – predição do *hacking* malicioso com base nas variáveis sociodemográficas

Variáveis	Modelo Parcelar 1			
	B	**SE**	**β**	**OR**
Idade	-.080	.014	-1.022	.359***
Género	.566	.194	.276	1.317**
Estado Civil	.180	.147	.167	1.181
Habilitações Concluídas	.014	.065	.026	1.026
Habilitações a Frequentar	-.084	.038	-.247	0.781*
Situação Profissional	.219	.193	.193	1.212
TIC	.264	.128	.128	1.136
Conhecimento Informático	.377	.116	.397	1.487***
$X^2 + p$	*148.678 ; p<.001*			
-2. Log Likelihood	*746.681*			
Nagelkerke R^2	*.266*			

B= coeficientes não estandardizados; SE= erro padrão; β= coeficientes estandardizados; OR= odds ratio
**p<.05; **p<.01; ***p<.001*

Anexo V – Modelo Parcelar 2 de *Hacking* Malicioso (durante a vida) – predição do *hacking* malicioso com base no autocontrolo

Variáveis	Modelo Parcelar 2			
	B	**SE**	**β**	**OR**
Autocontrolo	1.518	.227	.665	1.944***
$X^2 + p$	*51.689 ; p<.001*			
-2. Log Likelihood	*726.401*			
Nagelkerke R^2	*.115*			

B= coeficientes não estandardizados; SE= erro padrão; β= coeficientes estandardizados; OR= odds ratio
**p<.05; **p<.01; ***p<.001*

Anexo VI – Modelo Parcelar 3 de *Hacking* Malicioso (durante a vida) – predição do *hacking* malicioso com base nas componentes da aprendizagem social

Variáveis	Modelo Parcelar 3			
	B	**SE**	**β**	**OR**
Associação Diferencial	2.470	.379	1.152	3.164***
Definições	1.278	.218	.806	2.238***
Reforço Diferencial	.716	.209	.715	2.044***

$X^2 + p$	*261.402 ; p<.001*
-2. Log Likelihood	*564.251*
Nagelkerke R^2	*.468*

*B= coeficientes não estandardizados; SE= erro padrão; β= coeficientes estandardizados; OR= odds ratio *p<.05; **p<.01; ***p<.001*

Anexo VII – Modelo Parcelar 1 de *Hacking* Malicioso (nos últimos 12 meses) – predição do *hacking* malicioso com base nas variáveis sociodemográficas

Variáveis	Modelo Parcelar 1			
	B	**SE**	**β**	**OR**
Idade	-.093	.022	-1.197	.302***
Género	.178	.236	.087	1.090
Estado Civil	.404	.197	.375	1.454*
Habilitações Concluídas	-.026	.083	-.049	.952
Habilitações a Frequentar	-.056	.049	-.166	.847
Situação Profissional	.159	.150	.141	1.151
TIC	.501	.279	.244	1.276
Conhecimento Informático	.657	.133	.692	1.997***
$X^2 + p$	*112.269 ; p<.001*			
-2. Log Likelihood	*623.075*			
Nagelkerke R^2	*.230*			

*B= coeficientes não estandardizados; SE= erro padrão; β= coeficientes estandardizados; OR= odds ratio *p<.05; **p<.01; ***p<.001*

Anexo VIII – Modelo Parcelar 2 de *Hacking* Malicioso (últimos 12 meses) – predição do *hacking* malicioso com base no autocontrolo

Variáveis	Modelo Parcelar 2			
	B	**SE**	**β**	**OR**
Autocontrolo	.702	.223	.307	1.359**
$X^2 + p$	*10.084 ; p=.001*			
-2. Log Likelihood	*641.303*			
Nagelkerke R^2	*.025*			

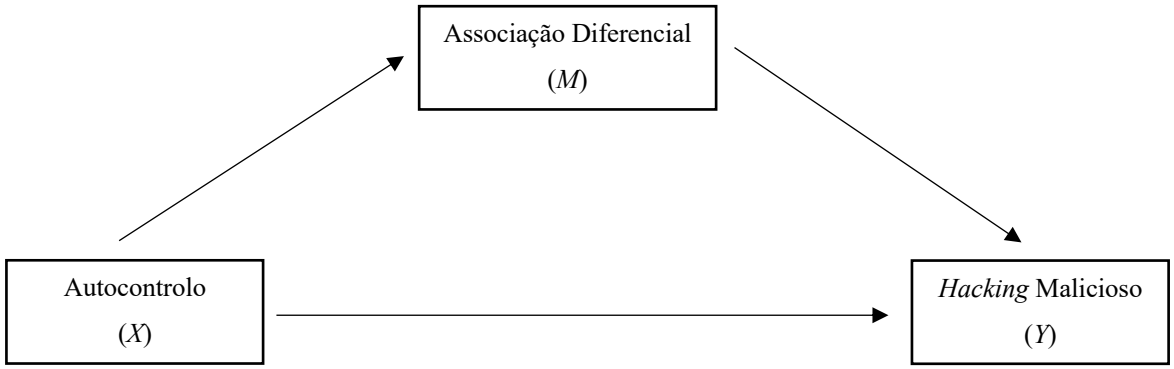
*B= coeficientes não estandardizados; SE= erro padrão; β= coeficientes estandardizados; OR= odds ratio *p<.05; **p<.01; ***p<.001*

Anexo IX – Modelo Parcelar 3 de *Hacking* Malicioso (últimos 12 meses) – predição do *hacking* malicioso com base nas componentes da aprendizagem social

Variáveis	Modelo Parcelar 3			
	B	**SE**	**β**	**OR**
Associação Diferencial	1.527	.284	.713	2.04***
Definições	.659	.215	.416	1.51**
Reforço Diferencial	.407	.127	.406	1.50**
$X^2 + p$	*145.962 ; p<.001*			
-2. Log Likelihood	*534.434*			
Nagelkerke R^2	*.315*			

*B= coeficientes não estandardizados; SE= erro padrão; β= coeficientes estandardizados; OR= odds ratio *p<.05; **p<.01; ***p<.001*

Anexo X – Representação gráfica do Modelo de Mediação



Anexo XI – Modelo de Mediação entre Autocontrolo, Associação Diferencial e *Hacking* Malicioso (durante a vida)

	Efeito	**SE**	***t***	***p***
Efeito direto de X em Y	0.325	0.250	1.300	0.193
	Efeito	**SE**	**IC 95%**	
Efeito indireto de X em Y	0.675	0.157	0.393 – 1.010	
Efeito indireto de X em Y estandardizado	0.096	0.022	0.056 – 0.143	

SE= erro padrão; IC= intervalo de confiança

Anexo XII – Modelo de Mediação entre Autocontrolo, Associação Diferencial e *Hacking* Malicioso (nos últimos 12 meses)

	Efeito	**SE**	***t***	***p***
Efeito direto de X em Y	0.042	0.137	0.307	0.758
	Efeito	**SE**	**IC 95%**	
Efeito indireto de X em Y	0.216	0.065	0.106 – 0.362	
Efeito indireto de X em Y estandardizado	0.062	0.017	0.031 – 0.102	

SE= erro padrão; IC= intervalo de confiança