MESTRADO INTEGRADO
PSICOLOGIADO COMPORTAMENTO DESVIANTE E DA JUSTIÇA

# Cibercrime: Um estudo exploratório da população universitária da Universidade do Porto

Ana Filipa Bettencourt Costa

**M**

**2020**

**Universidade do Porto**

**Faculdade de Psicologia e de Ciências da Educação**

# CIBERCRIME: UM ESTUDO EXPLORATÓRIO DA POPULAÇÃO UNIVERSITÁRIA DO PORTO

**Ana Filipa Bettencourt Costa**

Outubro, 2020

Dissertação apresentada no Mestrado Integrado de Psicologia, Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto, orientada pelo Professor Doutor ***Jorge Negreiros*** (FPCEUP).

## AVISOS LEGAIS

O conteúdo desta dissertação reflete as perspetivas, o trabalho e as interpretações do autor no momento da sua entrega. Esta dissertação pode conter incorreções, tanto conceptuais como metodológicas, que podem ter sido identificadas em momento posterior ao da sua entrega. Por conseguinte, qualquer utilização dos seus conteúdos deve ser exercida com cautela.

Ao entregar esta dissertação, o autor declara que a mesma é resultante do seu próprio trabalho, contém contributos originais e são reconhecidas todas as fontes utilizadas, encontrando-se tais fontes devidamente citadas no corpo do texto e identificadas na secção de referências. O autor declara, ainda, que não divulga na presente dissertação quaisquer conteúdos cuja reprodução esteja vedada por direitos de autor ou de propriedade industrial.

**Agradecimentos**

A conclusão de um ciclo não é fácil, e este encerra com a dissertação da minha tese de mestrado. Entrei em 2014 para esta casa e são demasiadas as pessoas a quem agradecer, mas vou tentar dar o meu melhor.

Quero agradecer ao professor Jorge Negreiros por me ter orientado na realização deste projeto.

À minha família, sem a qual a entrada nem tinha sido possível, quanto mais a conclusão.

Ao laranja e a todas as pessoas que lá conheci, que me fizeram sentir que pertencia a algo. A todos os momentos inesperados que passei e às lágrimas de alegria que derramei. Sei que vos levo a todos no coração.

À Tuna, que foi igualmente importante na descoberta de quem sou hoje.

Às grandes amizades que fiz, É-ssi, Drekah, Liv, Leo, Kafa, Diva, Alpha e tantas mais.

A ti Dilma, pelo teu amor e carinho desde o primeiro dia. És e sempre serás a minha alma gémea.

Aos meus padrinhos e madrinhas que são mais que as mães, e às minhas irmãs. Vocês sabem o quanto vos valorizo.

Às minhas crias, que só servem para dar dores de cabeça, mas de quem gosto tanto. A ti, cabrita montesa, que mais que uma afilhada, és uma amiga.

À minha terapeuta e psiquiatra. Obrigada por me terem ajudado nesta luta comigo própria.

E a todos os que fizeram de mim quem sou hoje e que me ajudaram neste percurso.

## Resumo

Os jovens estudantes universitários são um dos grupos que mais acompanha o desenvolvimento das novas tecnologias de informação e comunicação (TIC). Com a expansão destas tecnologias e da *internet*, o crime encontra novas formas de atuar, e esta população pode estar em maior risco de ser vitimada. O uso da *internet* e das redes sociais traz benefícios e conforto, mas o seu uso constante e pouco seguro gera consequências difíceis de corrigir e reverter. O cibercrime é um fenómeno que preocupa cada vez mais as autoridades nacionais e os magistrados, no entanto as investigações existentes ainda são insuficientes para prevenir e combater de modo eficaz este crime. Desta forma, o principal objetivo deste estudo é traçar o perfil das vítimas mais frequentes, numa amostra de estudantes, observar a frequência do cibercrime, e averiguar a influência que a consciência deste fenómeno, juntamente com a adoção de medidas de segurança e privacidade, possui na diminuição de uma experiência de vitimação. Esta investigação contou com a participação de 144 estudantes de várias faculdades da Universidade do Porto, com idades compreendidas entre os 18 e 27 anos ($M$ = 21.34, $DP$ = 1.80). Deste total, foi estabelecida uma subamostra de 43 estudantes que foram vítimas de cibercrime. Os nossos resultados demonstraram que as vítimas mais comuns eram do sexo feminino, de cursos socio humanísticos, e do 4º, 5º e 6º ano de faculdade. Estas também viviam sem a família, utilizavam muitas redes sociais, para comunicação e entretenimento, e possuíam pouca literacia digital. Em relação à consciência do cibercrime, e a adoção de medidas de segurança e de privacidade nas redes sociais, estes parecem estar relacionados com a diminuição da experiência de vitimação, mas apenas para alguns cibercrimes. Os crimes mais frequentes na nossa amostra, foram o assédio nas redes sociais, acesso ilegítimo às redes sociais, *phishing* e *cyberstalking*.



**Palavras-chave:** Cibercrime, Redes Sociais, Vitimação, Estudantes Universitários.

## Abstract

University students are one of the groups that most closely accompanies the development of information technologies. With the expansion of these technologies and of the internet, crime finds new ways to act, and this population may be at greater risk of being victimized. The use of the internet and social networks brings comfort, but its constant and unsafe use brings consequences that are difficult to correct and to reverse. Cybercrime is a phenomenon that worries national authorities and magistrates, however, the existing investigations are still insufficient to effectively prevent and combat this crime. The main objective of this study is to outline the profile of the most frequent victims, in a sample of university students, observe the frequency of cybercrime, and ascertain the influence of the awareness of this phenomenon, together with the adoption of security and privacy measures, in reducing a victimization experience. This investigation has a sample of 144 students from various colleges at the University of Porto, aged between 18 and 27 years old ($M$ = 21.34, $SD$ = 1.80). Of this total, a subsample of 43 students who were victims of cybercrime was established. Our results showed that the most common victims were female, from socio-humanistic courses, and from the 4th, 5th and 6th year of college. They also lived without their family, used many social networks, for communication and entertainment, and had a reduced digital literacy. In relation to cybercrime awareness, and the adoption of security and privacy measures on social networks, these seem to be related to the decrease in the victimization experience, but only for some cybercrimes. The most frequent crimes in our sample were harassment on social networks, illegitimate access to social networks, phishing and cyberstalking.



**Keywords:** Cybercrime, Social Networks, Victimization, University Students.

## Résumé

Les étudiants universitaires sont l'un des groupes qui accompagne le plus le développement des nouvelles technologies de l'information et de la communication. Avec l'expansion de ces technologies et d'*Internet*, le crime trouve de nouvelles façons d'agir, et cette population peut être plus à risque d'être victimisée. L'utilisation d'*Internet* et des réseaux sociaux apporte des avantages et du confort, mais leur utilisation constante et dangereuse a des conséquences difficiles à corriger et à inverser. La cybercriminalité est un phénomène qui inquiète les autorités nationales et les magistrats, pourtant les enquêtes existantes sont encore insuffisantes pour prévenir et combattre efficacement ce crime. Ainsi, l'objectif principal de cette étude est de dresser le profil des les plus frequentes victimes, dans un échantillon d'étudiants, observer la fréquence de la cybercriminalité, et déterminer l'influence que la conscience de ce phénomène, ainsi que l'adoption de mesures de confidentialité et sécurité, a réduit l'expérience de victimisation. Cette enquête a utilisé un échantillon de 144 étudiants, des différents collèges de l'Université de Porto, de 18 à 27 ans ($M$ = 21,34, $ET$ = 1,80). Sur ce total, un sous-échantillon de 43 étudiants victimes de cybercriminalité a été constitué. Nos résultats ont montré que les plus frequentes victimes étaient des femmes, de cours socio-humanistes, et la 4e, 5e et 6e année scolaire. Ils ne vivaient pas avec leur famille, ils utilisaient beaucoup de réseaux sociaux, pour communiquer et se divertir, et avait peu de connaissances informatiques. En ce qui concerne la sensibilisation à la cybercriminalité et l'adoption de mesures de sécurité et de confidentialité sur les réseaux sociaux, ceux-ci sont liés à la diminution de l'expérience de victimisation, mais seulement pour certains cybercrimes. Les délits les plus fréquents de notre échantillon étaient le harcèlement sur les réseaux sociaux, l'accès illégitime aux réseaux sociaux, le *phishing* et le cyberharcèlement.



**Mots-clés:** cybercriminalité, réseaux sociaux, victimisation, étudiants universitaires.

## Índice



## Lista de Anexos

# 1. GLOSSÁRIO

**Ciberespaço:** termo introduzido por William Gibson no seu romance "Neuromancer", de 1984, para representar o espaço virtual que conecta todos os computadores e seus usuários numa rede mundial;

***Cyberbullying:*** manifestação das práticas de *bullying* através da *internet*;

***Cyberstalking:*** comportamentos constantes de perseguição e ameaça realizados através da *internet*;

***Doxing:*** prática que envolve pesquisar e transmitir dados privados de um indivíduo ou instituição;

***Internet:*** rede que conecta todos os computadores do globo, permitindo a troca de informação entre eles;

***Pharming:*** crime que consiste em instalar um vírus no computador de um usuário, para o desviar para páginas falsas, e roubar informações pessoais e financeiras;

***Phishing:*** crime que consiste em enviar mensagens eletrónicas que contêm ligações para páginas de *internet* falsas, semelhantes a outras existentes, em que o objetivo é recolher informações referentes a contas bancárias e cartões;

***Sextortion:*** quando se ameaça revelar informações da vida privada ou confidenciais, caso não forneçam imagens de caracter sexual, favores sexuais ou dinheiro.

# 2. INTRODUÇÃO

## 2.1. Influência das TIC na sociedade

A evolução do Homem está intrinsecamente ligada ao progresso tecnológico (Ferreira & Monteiro, 2009), pois é através da tecnologia que o ser humano modifica o mundo em seu redor (Alves, 2009), permitindo a sua sobrevivência e constante adaptação. Ao longo da história é possível identificar várias fases da comunicação e as tecnologias utilizadas: a primeira assenta na tradição oral, dependente de lembranças e memórias auditivas; a segunda, na comunicação escrita e a invenção da imprensa tornou possível aos leitores um acesso mais fácil ao conhecimento; e a terceira, a era eletrónica e digital possibilitou um armazenamento e disseminação do conhecimento em massa (Lima, Pinto & Laia, 2002).

O século XXI significou a passagem de uma sociedade industrial, para uma informacional, em que o espaço físico cedeu o lugar ao ciberespaço e todos os seus sistemas de informação (Saldanha, Brum & Mello, 2016). As TIC têm um papel de destaque na nossa sociedade, sendo responsáveis por padrões de comportamento, lazer, trabalho e consumo, sistema de educação e mercado de trabalho, afetando também a própria estrutura social e conceção do conhecimento (Lima et al., 2002).

O desenvolvimento desta rede de infraestruturas comunicacionais foi fundamental para o processo de globalização (Campos & Canavezes, 2007). As inovações tecnológicas conectaram os indivíduos e instituições de todo o mundo, facilitando também a circulação de bens, serviços e pessoas (Campos & Canavezes, 2007). As TIC desempenham um papel tão relevante nas sociedades atuais que as redes locais e regionais de bens e serviços estão integradas numa rede global de dependências mútuas, com outros grupos financeiros multinacionais, através de tratados comerciais, políticos e diplomáticos (Alves, 2009). As tecnologias digitais permitem então a integração e aproximação das empresas, pela interligação de tarefas e pessoas e pelos esforços coletivos que desenvolvem (Lima et al., 2002). A própria Comissão Europeia (2020), admite que assegurar a *internet* e os sistemas de informação é essencial para manter a economia europeia a funcionar e prosperar.

Esta conetividade constante afeta o conceito de trabalho e vida pessoal do trabalhador (Lima et al., 2002). Atualmente, o bom profissional é visto como flexível e capaz de

acompanhar as mudanças tecnológicas, o que leva ao seu esgotamento, pois a sua capacidade de mudar a nível psíquico, cognitivo e físico não acompanha a velocidade com que as TIC se alteram (Lima et al., 2002).

Como referido anteriormente, as TIC levam a mudanças cognitivas, afetando o nosso pensamento e estilo de vida, sociais e também políticas (Alves, 2009), provocando uma metamorfose no próprio conceito de cidadania (Saldanha, et al., 2016). Para Alves (2009), quanto mais um individuo se informa, mais responsável é a nível social e político, a um nível local e global. Através das TIC, os cidadãos empoderam-se com a obtenção de informação, relevante para a tomada de decisões, e pressionam os governos com as suas causas reivindicativas (Giaretta & Di Giulio, 2018). A informação é um bem desejado (Alves, 2009), e sendo as TIC o seu principal meio de difusão, quanto mais um individuo as dominar, mais este pode exercer um papel ativo e responsável na sua sociedade. Por sua vez, quem não se adapta à tecnologia, corre o risco de ser excluído das relações interpessoais e de trabalho (Lima et al., 2002).

A fim de usufruir de todas as vantagens que o acesso às TIC proporciona, é necessário investimento financeiro e humano, o que leva a que os países com maior capital e poder de investimento ditem as suas regras de construção, utilização e acesso (Lima et al., 2002). Isto acarreta consequências técnicas, económicas, sociais e políticas nos países menos favorecidos, tornando-se apenas em consumidores passivos da informação disponibilizada (Lima et al., 2002). Se por um lado, a utilização das TIC diminui as diferenças sociais, com a criação de um espaço aberto de participação (Alves, 2009), a desigualdade no acesso à *internet* pode levar ao enfraquecimento da democracia, criando um fosso ainda maior entre ricos e pobres (Saldanha et al., 2016). Na atual sociedade da informação, dominar as tecnologias digitais e utilizá-las adequadamente atribui vantagens apenas a determinados grupos (Saldanha et al., 2016). E mesmo quando a sua utilização é possível, nem toda a informação se encontra disponível, assistindo-se a uma censura intelectual por parte de organismos privados (Lima et al., 2002).

É devido a esta dependência da informação nas sociedades modernas, que é necessário combater a infoexclusão (Ferreira & Monteiro, 2009), pois o acesso às possibilidades trazidas pelas TIC está longe de ser equitativo e igualitário (Giaretta & Di Giulio, 2018). A globalização é um processo a que apenas associamos vantagens, trazendo a melhoria das condições de vida de toda a população mundial, mas na prática é um processo de exclusão para os que não conseguem aceder à *internet* (Lima et al., 2002).

A universalização do acesso às TIC constitui uma condição para a liberdade humana na rede (Saldanha et al., 2016). Todos os dias, uma imensidão de pessoas utiliza a *internet* para comercializar, gerir negócios, comunicar através das redes sociais, ler revistas e jornais, e muitas mais atividades, surgindo a questão sobre se uma pessoa é realmente livre, mesmo que não utilize estes recursos por opção (Saldanha et al., 2016). É um dever de todos adotar uma postura critica sobre a realidade, a fim de construir uma sociedade da informação mais democrática (Lima et al., 2002).

De acordo com Ferreira e Monteiro (2009), são os jovens quem mais procuram as TIC. Crianças e adolescentes sentem-se mais à vontade com estas tecnologias, pois cresceram com elas, ao contrário dos pais, que não acompanham tão bem os filhos (Ferreira & Monteiro, 2009). O computador possui então um significado diferente para cada faixa etária: para uma criança possuí valor lúdico; na adolescência é um meio para escapar à realidade e constitui uma forma de identificação; para um adulto é visto como um instrumento de trabalho (Alves, 2009).

Nos adolescentes é visível uma verdadeira cultura do computador, sendo este um mediador para a construção de uma identidade *online* e para as interações sociais (Alves, 2009). A comunicação deixou de ser física, para passar a ser tecnológica (Alves, 2009), servindo-se das redes sociais, sem a total perceção dos seus perigos e vulnerabilidades (Ferreira & Monteiro, 2009). Com a crescente utilização destas aplicações, não são apenas as celebridades que captam audiências, mas pessoas comuns também. Ao partilhar uma fotografia na *internet* produzimos conteúdo para uma plateia *online*, o que remete para a ideia, referida por Alves (2009), de *persona*, ou seja, a personalidade que construímos *online*. O excesso de tempo livre combinado com as novas tecnologias, criam esta *persona*, onde o utilizador passa de consumidor a criador (Oliveria, 2017). O sujeito está agora ligado ao mundo virtual como produtor, consumidor e plateia, emissor e recetor (Alves, 2009).

### 2.1.1. Estatísticas de utilização em Portugal

Todas as TIC possuem mais ou menos riscos, uns confirmados e os outros apenas suposições (Ferreira & Monteiro, 2009). Tendo isto em conta, é relevante estudar as estatísticas portuguesas e averiguar a percentagem da população que consome estas tecnologias, e que por isso pode estar mais exposta.

É possível obter estes dados através do Inquérito à Utilização de Tecnologias de Informação e da Comunicação pelas Famílias (IUTICF), realizado anualmente pelo Instituto Nacional de Estatística (INE). O inquérito de 2019 contou com a participação de 6624

agregados domésticos, com pelo menos um individuo entre os 16 e 74 anos de idade. Os valores referidos dizem respeito a 3 meses ou 12 meses anteriores à realização da entrevista.

Do total da população inquirida, 76.2% relatou ter utilizado a *internet* nos 12 meses anteriores à entrevista. No entanto existe uma diminuição acentuada em relação à idade, a partir da faixa dos 55 anos ou mais (INE, 2019). Entre os 16 e os 44 anos o acesso à *internet* atinge percentagens superiores a 90%, sendo o valor mais elevado para o grupo etário dos 16 e 24 anos (99.5%) (INE, 2019). Em relação ao sexo, o acesso à *internet* apresenta valores muito semelhantes, sendo que os homens registam uma utilização de 77.5% e as mulheres 75.0% (INE, 2019).

Através do IUTICF podemos observar que a população estudante e os indivíduos que completaram o ensino superior são os que mais utilizam a *internet* (99.6% e 98.7% respetivamente), seguida pela que completou o ensino secundário (96.9%) e pela que está empregada (88.1%), (INE, 2019).

O consumo da *internet* móvel continua a aumentar, verificando-se que 84.1% dos entrevistados utilizaram-na fora de casa e do trabalho, através de dispositivos móveis, sendo o mais comum o telemóvel ou *smartphone* (82.5%), seguido pelo computador portátil (45.1%), (INE, 2019).

Em relação ao porquê de utilizarem a *internet*, 85.8% dos participantes admitiu trocar mensagens instantâneas, 84.4% para receber e enviar e-mails e 80.2% para participar em redes sociais, tudo num período de 3 meses anteriores à entrevista (INE, 2019). Tal como a utilização das redes sociais, o comércio eletrónico está a aumentar, sendo que os estudantes registam uma percentagem de utilização de 62.3% (INE, 2019).

### 2.2. Redes sociais virtuais

O conceito de rede social surgiu muito antes de todas as inovações tecnológicas das quais usufruímos nos nossos dias, sendo necessário distinguir este do termo rede social virtual. Uma rede social é descrita como uma estrutura composta por vários indivíduos e organizações, que estão ligados por relações e compartilham valores e objetivos em comum (Sousa & Cardoso, 2011). Uma rede social virtual partilha semelhanças com o conceito anterior, exceto que as relações estabelecidas entre os atores são virtuais, ou seja, as redes e

as conexões são criadas por sistemas computacionais (Mira & Bodoni, 2011). Destas interações realizadas por mediação digital, que são também de natureza social e cognitiva, nasce uma narrativa coletiva de experiências e conhecimento, partilhada pelos membros da comunidade (Miranda et al., 2011).

Os *sites* de relacionamentos, ou redes sociais virtuais são o resultado da necessidade de encontrar novos processos que facilitem o trabalho, produção, compras e relacionamentos (Santos & Santos, 2014). Com a expansão das TIC nos anos 90, novos tipos de relações sociais surgiram, interferindo nas estruturas políticas e económicas das sociedades do mundo (Angelo, 2016), que se perpetuam ao redor de redes sociais (Souza & Cardoso, 2011). Estas permitiram o aparecimento de novos sistemas de ação, nos campos da participação cívica, troca de informações e opiniões, encontros, partilha de fotografias, dicas, namoro e propostas de emprego (Santos & Santos, 2014), representando possibilidades a nível pessoal, profissional e educacional (Miranda et al., 2011).

As TIC são então recursos computacionais e técnicos que gerem o uso da informação, sendo as redes sociais virtuais uma massa dinâmica, fluida, constante e moderadamente organizada, que tem nas suas interações um padrão matematicamente avaliável (Mira & Bodoni, 2011). Para além de serem um instrumento de alcance global, capaz de influenciar a sociedade, a cultura, economia e educação (Angelo, 2016), as redes sociais virtuais são um ambiente criado para satisfazer as necessidades de interação dos indivíduos (Meşe & Aydin, 2019). As aplicações de trocas de mensagens instantâneas são um espaço fácil e acessível para interagir, e por isso potenciadoras do aprofundamento de laços sociais (Miranda et al., 2011). De acordo com Silva, Costa e Oliveira (2019), as redes sociais virtuais são sistemas criados para aumentar as relações humanas, que se aperfeiçoam por forma a permitir que os utilizadores se expressam cada vez melhor, e sendo por isso um espaço de socialização. A flexibilidade para reconfigurar e adaptar o seu sentido e objetivos, no seu processo de desenvolvimento é então uma característica marcante destas tecnologias digitais, juntamente com o seu modelo organizacional não hierárquico, não centralizado e horizontal, com interações e experiências sociais colaborativas e fluidas, num universo digital (Miranda et al., 2011).

A facilidade com que podem ser utilizadas, mesmo com pouco conhecimento computacional, levou à sua explosão na nossa sociedade (Mira & Bodoni, 2011), tornando-se num meio de comunicação indispensável no nosso quotidiano (Silva et al., 2019). E com a expansão da tecnologia móvel, aceder à *internet* em qualquer lugar e hora é cada vez mais

fácil, desempenhando um papel vital para a expansão das redes sociais virtuais (Saha & Guha, 2019), e para a flexibilização do espaço e tempo (Vermelho et al., 2014).

Para além de permitir o acesso a um banco de conhecimento global e informação atualizada (Saha & Guha, 2019), as redes sociais virtuais são uma plataforma em que os utilizadores expõem a sua vida privada, expressam sentimentos, ideias, opiniões, imagens e vídeos, sem qualquer limite de palavras, ou restrição física (Silva et al., 2019). Através disto, o cidadão pode ver e ainda ser visto, pode acolher e ser acolhido, e atuar no mundo, mesmo que à margem das instituições formais (Angelo, 2016).

As redes socais virtuais oferecem-nos liberdade e alcance, e possuem um enorme poder de mobilização, influência, interação e pertença (Angelo, 2016), pois no universo e na economia da informação, todos os indivíduos são livres e capazes de observar, responder, questionar e debater (Vermelho et al., 2014). Mas mesmo com a suas vantagens, estas podem afetar a vida dos utilizadores, dependendo do seu uso (Meşe & Aydin, 2019). Qualquer ferramenta apresenta aspetos positivos e negativos, cabendo aos consumidores adotar uma opinião crítica sobre a sua utilização (Angelo, 2016). Um exemplo disso, é a globalização do conhecimento, facilitado pela velocidade da partilha de informação, que leva ao desenvolvimento do potencial criativo dos consumidores (Mira & Bodoni, 2019). O conhecimento na *internet* e nestas redes é facilmente consultado, mas não sabemos se é confiável ou científico, podendo ser apenas o reflexo de opiniões pessoais sem fundamento teórico (Angelo, 2016). O conhecimento na rede passa a ser uma representação coletiva, flexível e complexa, dependente dos membros do grupo, cada um com uma presença social e cognitiva, num processo dinâmico de participação e envolvimento (Miranda et al., 2011).

As TIC não são uma mera ferramenta de comunicação e aprendizagem, são uma combinação entre o desejo das empresas, em colocar os seus produtos no mercado, e o desejo dos indivíduos de se relacionarem através destes (Santos & Santos, 2014). É possível identificar as redes sociais digitais mais utilizadas, mas proceder à sua caracterização é uma tarefa desafiante, pois possuem várias potencialidades e objetivos, juntamente com um público muito diversificado em relação aos seus interesses (Miranda et al., 2011). O *Instagram*, por exemplo, uma aplicação de publicação e partilha de fotografias e vídeo, requisita o preenchimento de um formulário de preferências, mais tarde utilizado pelos grupos económicos para publicitar os seus produtos, e aumentar o seu capital económico (Santos & Santos, 2014).

As novas mudanças tecnológicas implicam uma alteração na forma como compreendemos os processos de interação social, e como construímos o conhecimento,

sendo necessária uma nova visão sobre a interação dos grupos e do como os consumidores se organizam na rede (Miranda et al., 2011). As TIC e as redes sociais digitais estão cada vez mais presentes na nossa rotina, e é inegável a sua utilidade na forma como comunicamos, relacionamos e aprendemos (Santos & Santos, 2014). No entanto, estas tecnologias podem trazer consequências danosas às nossas comunidades, pois os propósitos que servem podem nem sempre ser positivos para o cidadão (Angelo, 2016). A simples presença das TIC não é suficiente, pois é necessário que os sujeitos as saibam utilizar corretamente nas suas relações interpessoais na produção de informação e construção de conhecimento e no seu processo de aprendizagem (Santos & Santos, 2014).

### 2.3. Estudantes universitários

Os estudantes do ensino superior são indivíduos que, embora não sejam adolescentes, não são adultos em todas as suas capacidades, podendo este período desenvolvimental estender-se entre os 18 e 24 anos de idade (Nogueira, 2017). Os estudantes universitários são um grupo vulnerável, cujos valores, crenças e atitudes, ensinados pela família, são colocados em causa, traduzindo-se a entrada no ensino superior como uma nova realidade cognitiva e emocional (Brito, Gordia & Quadros, 2016). O contexto académico, um ambiente físico, mas principalmente relacional, reflete uma nova dinâmica e cultura para o estudante, repleta de pressões e desafios a nível do estabelecimento de relações, integração, pressão parental e académica e questões financeiras (Nogueira, 2017).

Neste período de mudança, as redes como o *Facebook*, *Messenger* e *WhatsApp* oferecem uma forma de entretenimento e comunicação para os estudantes universitários (Saha & Guha, 2019), assumindo por isso um papel de elevada importância no seu quotidiano (Meşe & Aydin, 2019). Através destas, podem ser livres e publicar na rede o que lhes apetecer, fazer novos amigos e comentar as suas publicações, criando uma verdadeira comunidade virtual (Saha & Guha, 2019).

As redes sociais virtuais surgem de interações orientadas pela partilha e formação de grupos de interesse, existindo na sua base um sentido de construção coletiva, devido à sua flexibilidade e complexidade dos sistemas de informação, aprendizagem e conhecimento (Miranda et al., 2011). Nas redes sociais virtuais, os estudantes criam uma rede de contactos e de partilha de informação, ao redor de um perfil, que alargam à medida das suas necessidades comunicacionais e de desenvolvimento social (Miranda et al., 2011).

Através dos seus telemóveis, podem publicar as suas fotografias *online*, ver e comentar as dos colegas e ainda verificar o seu perfil, existindo até aplicações para servir esse fim, como o *Facebook* e o *Twitter* que dispõe de aplicações móveis e de fácil acesso (Saha & Guha, 2019). Os jovens estudantes universitários também utilizam as redes sociais virtuais como uma fonte de entretenimento, contactos profissionais, consultar informação, jogar e disponibilizar conteúdo (Miranda et al., 2011).

O mundo digital melhorou graças à criação das redes sociais virtuais, pois possibilitam a partilha de ideias, estados e materiais áudio visuais entre os jovens, influenciando até uma mudança de rotinas e comportamentos (Saha & Guha, 2019). Com estas interações sociais, expressão de opiniões e partilha de informação entre usuários, os jovens constroem a sua identidade e desenvolvem a sua autoimagem, que se traduz na criação de uma página pessoal e de entretenimento (Angelo, 2016). Para Silva et al., (2019), a identidade modifica-se de acordo com o convívio no meio social, e são as redes sociais virtuais que mostram o que é ou não agradável na nossa sociedade.

### 2.3.1. Perigos e impactos negativos de utilização

O uso intensivo da *internet* e a disseminação das TIC, levou ao aumento do número de redes socais virtuais, onde todos desejam usufruir da sua velocidade e alcance no espaço geográfico (Angelo, 2016). A *internet* deixou de ser um mero instrumento de pesquisa, para desempenhar um papel fundamental na vida social dos estudantes, tornando-se num espaço em que estes se relevam e passam a ser vistos, mesmo que os detalhes da sua vida íntima passem a ser do conhecimento de estranhos (Dias & Teixeira, 2008). Por este e por muitos outros motivos, as redes sociais virtuais provocam um impacto negativo nos estudantes universitários, afetando as suas vidas pessoais e sociais (Saha & Guha, 2019), e os seus ambientes educacionais, diminuindo assim o seu sucesso académico (Meşe & Aydin, 2019).

O estudo realizado por Saha e Guha (2019), em duas universidades de Bangladesh (N= 502), registou que 21.2% dos estudantes admitiram ter os estudos em atraso, devido às redes sociais virtuais, e 30.38% consideravam-nas um desperdício de tempo, pois ao invés de estudar, verificavam constantemente as suas mensagens. Continuando a analisar os resultados desta investigação, 48.5% verificavam constantemente as suas redes sociais virtuais, 9.8% relataram que o telemóvel interrompia as suas conversas e refeições, e 25.90% afirmaram ter problemas de visão (Saha & Guha, 2019).

Outra investigação levada a cabo por Miranda et al., (2011), com estudantes do ensino superior (N= 363), relevou que 11% possuíam opiniões negativas sobre as redes

sociais virtuais, como tempo perdido e o vício. Oliveira (2017), refere que em muitos casos, o uso da *internet* se transforma numa verdadeira compulsão e dependência.

O ambiente gerado pelas redes sociais virtuais, por ser instável e pouco seguro, pode levar ao colapso de relações, experiências de assédio, roubo de identidade e acesso ilegítimo aos perfis digitais (Nakala e Diunugala, 2020). Com a expansão dos aparelhos tecnológicos pessoais, o cibercrime aumenta (Nodeland & Morris, 2020), e por serem dos maiores consumidores, os jovens estudantes são potenciais vítimas. O estudo de Nakala e Dianugala (2020), com estudantes universitários, registou o *cyberstalking*, fraude, *doxing*, *hacking* e criação de contas falsas como os crimes mais reportados por esta população.

## 2.4. Cibercrime

O século XXI trouxe o progresso da tecnologia da informação e o aumento do acesso à *internet* (*Nakala* & Diunugala, 2020). Esta evolução foi, no entanto, responsável por abrir vias ao florescimento do cibercrime (Abdulai, 2020; Nzeakor, Nwokeoma & Ezeh, 2020), e o aparecimento dos novos aparelhos digitais permitiu a evolução de crimes de tipologia tradicional, agora em maior quantidade e mais velozes (Schreuders et al., 2020).

De acordo com a Associação de Apoio à Vítima (APAV), o cibercrime é um conjunto de crimes praticados com recurso a um computador ou internet (APAV, 2015), possuindo características únicas como a ambiguidade, rapidez, anonimato e ausência de limites geográficos (Nzeakor et al., 2020). Não existe no entanto uma definição clara ou um consenso geral sobre o que é um cibercrime, tendo em conta que crimes que recorrem vagamente a tecnologias e aparelhos digitais são colocados nesta categoria (França & Quevedo, 2020). É ainda inexistente uma teoria geral, capaz de explicar este fenómeno, existindo várias teorias que se enquadram em cada uma das suas manifestações (Payne & Hadzhidimova, 2020).

O cibercrime está em constante mudança e evolução (Nodeland & Morris, 2020), devido aos avanços tecnológicos que o tornam dinâmico e alteram a sua aparência (Abdulai, 2020). Os meios pelos quais atuam são diversificados, multiplicando-se e alterando-se por forma a despistar a atenção dos utilizadores e das autoridades (APAV, 2015). Por consequência é um conceito interdisciplinar, que liga várias áreas como a engenharia e

ciência computacional, tecnologia informática, criminologia, justiça, e psicologia, e que acarreta preocupações e problemas tenológicos, criminais, sociais e para os negócios (Payne & Hadzhidimova, 2020).

Esta tipologia de crime pode ser praticada por organizações criminosas e a título individual, com o objetivo de obter lucros ou vantagens (APAV, 2015). A imagem do *hacker* especialista em computadores é na verdade um mito, pois os seus perpetradores podem possuir poucos ou elevados conhecimentos informáticos e rendimentos, ser de qualquer estrato social e possuir muita ou pouca formação (APAV, 2015). As suas características pessoais também variam (APAV, 2015), mesmo assim, no caso da pirataria informática, muitos apresentam um baixo nível de autocontrolo, característica que partilham com indivíduos que praticam crimes tradicionais (Nodeland & Morris, 2020). De acordo com a APAV (2015), o perpetrador pode ser um conhecido, amigo, familiar e colega de trabalho, ou um completo desconhecido, em que a vítima é escolhida de forma aleatória, e o seu objetivo é obter lucros e benefícios. No segundo cenário, a sua identificação é muito difícil, pois muitas vezes utiliza a própria identidade da vítima (APAV, 2015). No caso em que o agressor é próximo da vítima, a sua motivação é difamar ou prejudicar, através da criação de perfis falsos nas redes socais ou acesso ilegítimo aos verdadeiros (APAV, 2015).

Qualquer pessoa com acesso à *internet* corre o risco de ser uma potencial vítima, sendo então importante tomar precauções para evitar prejuízos emocionais, financeiros e físicos (Nzeakor et al., 2020). Verifica-se, no entanto, que as vítimas estão mal-informadas e pouco protegidas, devido às escassas medidas de combate, e pelos efeitos deste crime serem subestimados (APAV, 2015). Os ofensores são capazes de atuar em qualquer lugar do mundo e passar despercebidos (Payne & Hadzhidimova, 2020), sendo o anonimato e a capacidade de se esconder *online* um fator que torna os agressores mais predispostos a ofender na *internet*, do que cara a cara (Conradie et al., 2020). Isto leva a que muitas vezes os indivíduos não percebam de imediato que foram vitimados (Abdulai, 2020; Nzeakor et al., 2020). O perfil das vítimas varia de acordo com o tipo de cibercrime. Mesmo assim, os fatores mais decisivos para a escolha da vítima são a estabilidade financeira e a facilidade com que o agressor consegue aceder aos dados que necessita para cometer o crime (APAV, 2015).

Por todo o mundo, a literatura coloca em claro os elevados desafios que são necessários ultrapassar, a fim de lidar com este crime e as suas ambiguidades, como a criação de infraestruturas próprias, treino e certificação dos profissionais, sensibilização junto da população e criação de legislação eficaz (Schreuders et al., 2020). A cibercriminalidade tem

captado a atenção dos governos, organizações de segurança, e dos académicos, por forma a serem desenvolvidas intervenções eficazes (Abdulai, 2020). Apesar disso, o seu carácter internacional impõe obstáculos legais, ao reforço das autoridades, preocupações jurídicas e problemas metodológicos, à sua intervenção e estudo (Payne & Hadzhidimova, 2020). As diferenças legislativas e preocupações de segurança entre cada país, relativas ao cibercrime, também dificultam o seu combate e prevenção (Schreuders et al., 2020).

### 2.4.1. Impacto negativo na vítima e sociedade

O impacto do cibercrime na nossa sociedade é gigantesco, e o número de vítimas aumenta cada vez mais (Nzeakor et al., 2020). Devido aos elevados mecanismos que pode adotar, e às variadas vítimas que pode escolher, o cibercrime não acarreta apenas consequências negativas para pessoas particulares, mas também para empresas e estados.

De acordo com a APAV (2015), o impacto do furto de identidade nos indivíduos, vertente mais comum do cibercrime, pode ser financeiro, legal, emocional, psicológico e prático. Ao roubar os dados pessoais da vítima e a sua identidade, através de um vírus e esquemas de *phishing*, o agressor pode ganhar acesso às suas contas bancárias e perfis de compras (Abdulai, 2020). Os valores monetários perdidos podem ser diretos, derivados da própria burla, ou indiretos, relativos aos processos judiciais e chamadas telefónicas que a vítima tem de efetuar para resolver as consequências resultantes do roubo da sua identidade (APAV, 2015). A vítima muitas vezes não sabe que foi alvo de um cibercrime (Abdulai, 2020; Nzeakor et al., 2020), o que a nível legal pode implicar que seja constituída arguida de um crime que não cometeu e que desconhece por completo (APAV, 2015).

As consequências emocionais e psicológicas variam de indivíduo para indivíduo, e de acordo com o tipo de crime, manifestando-se um espectro de sintomas como medo, desilusão, impotência, desamparo, ansiedade, raiva e desconfiança prolongada (APAV, 2015). Em casos de assédio *online* é comum a vítima sentir relutância em reportar o crime, e ainda culpa por ser sensível ao tema (Conradie et al., 2020). Em relação à partilha não autorizada de imagens íntimas, é frequente a vítima não denunciar o crime, pois sente-se culpada por ter sido a própria a fornecer o material ao agressor (França & Quevedo, 2020). Em alguns casos o ofensor é um conhecido, outro motivo pelo qual a vítima não realiza a denuncia (APAV, 2015). Para piorar a situação, as vítimas de cibercrime sentem que o seu caso não é tratado com seriedade, devido aos efeitos deste crime serem ainda subvalorizados (APAV, 2015). Para finalizar, as consequências práticas do cibercrime referem-se ao tempo perdido pela vítima, a tentar solucionar a situação (APAV, 2015).

O medo do cibercrime afeta também os governos e comunidade de negócios, sendo esta obrigada a gastar quantias consideráveis para garantir uma maior segurança contra os crimes *online* (Abdulai, 2020). Os sistemas de informação são agora indispensáveis para gerir as operações dos governos e negócios, mas as suas constantes mudanças geram dificuldades em gerir e proteger os seus dados (Lee, 2020). A cibercriminalidade é responsável por perdas monetárias de bancos, companhias de seguros e fornecedoras de bens e serviços, o que acaba por se refletir nos custos que o consumidor deve suportar para usufruir destes (APAV, 2015). Garantir a segurança da informação é uma tarefa desafiante para as empresas (Lee, 2015), e quando estas vêm os seus computadores violados e as informações dos clientes expostas, a sua credibilidade é abalada (APAV, 2015).

## 2.5. Legislação portuguesa

A Lei nº 109/2009 de 15 de Setembro, também conhecida como Lei do Cibercrime, veio a substituir a antiga Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de Agosto). Esta é responsável por ditar as disposições penais e processuais, cooperação internacional e ainda a recolha e armazenamento das provas eletrónicas (art.1, Lei do Cibercrime, 2009). Como referido anteriormente, a cibercriminalidade é um fenómeno que abrange um variado número de crimes, sendo a Lei do Cibercrime responsável por criminalizar estas condutas. Assim, podemos contar com seis disposições penais:

1. Falsidade informática: interferir no tratamento de dados informáticos e produção de dados e documentos falsos, para finalidades jurídicas enganosas e para serem utilizados como se fossem verdadeiros (art.3, Lei do Cibercrime, 2009);
2. Dano relativo a programas ou outros dados informáticos: apagar, alterar ou destruir programas ou dados informáticos, sem autorização do proprietário ou permissão legal, para dificultar a utilização de programas ou dados (art.4, Lei do Cibercrime, 2009);
3. Sabotagem informática: danificar ou perturbar gravemente um sistema informático, sem a autorização do proprietário ou permissão legal, sob qualquer forma de interferência (art.5, Lei do Cibercrime, 2009);
4. Acesso ilegítimo: aceder a um sistema informático, sem permissão legal ou autorização do proprietário (art.6, Lei do Cibercrime, 2009);

5. Interceção ilegítima: intercetar dados informáticos, sem autorização do proprietário ou permissão legal (art.7, Lei do Cibercrime, 2009);
6. Reprodução ilegítima de programa protegido: reprodução e divulgação, sem permissão legal, de um programa protegido por lei (art.8, Lei do Cibercrime, 2009).

No Código Penal, também estão previstas outras condutas, que apesar de não estarem enumeradas na Lei do Cibercrime, também constituem uma prática criminal deste fenómeno. Podemos então definir mais cinco disposições legais:

a) Devassa da vida privada: intercetar, gravar, registar ou divulgar comunicações telefónicas e mensagens de correio eletrónico, sem permissão do proprietário, para devassar a sua vida privada, familiar e sexual. Também inclui a fotografia ou filmagem da vida privada da vida, observar e escutar e divulgar factos íntimos (art.192, Decreto-lei nº48/95);
b) Devassa por meio de informática: criar, manter ou utilizar ficheiros com dados que identifiquem a origem étnica da vítima, e que refiram as suas convicções políticas, filosóficas e religiosas (art.193, Decreto-lei nº48/95);
c) Violação de correspondência ou de telecomunicações: abrir uma encomenda, carta ou outro documento escrito, tomar conhecimento ou divulgar o seu conteúdo, sem a permissão do proprietário (art.194, Decreto-lei nº48/95);
d) Gravação de fotografias ilícitas: fotografar e filmar a pessoa, e gravar palavras proferidas por esta, que não devem ser dirigidas ao público, mesmo que a vítima tenha participado de forma legitima na produção destes materiais (art.199, Decreto-lei nº48/95);
e) Burla informática e nas comunicações: intervir, interferir ou utilizar de forma incorreta o tratamento de dados, sem a devida autorização, por forma a obter lucros (art.221, Decreto-lei nº48/95).

Embora não esteja especificamente previsto no Código Penal, a APAV (2015), identifica o furto de identidade como o fenómeno mais comum do cibercrime, abrangendo este a obtenção de dados, posse ou transferência e utilização de dados ou segredos da vítima, sem a sua permissão e para finalidades criminosas. Desde que estas informações sejam obtidas ou transferidas e utilizados para praticar crimes através da *internet*, passam a pertencer a esta categoria (APAV, 2015).

## 2.6. Estatísticas nacionais

De acordo com o Relatório da Atividade de 2013, do Gabinete Cibercrime (Gabinete Cibercrime, 2013), não existem estatísticas englobantes sobre a cibercriminalidade no nosso país, sendo necessário contactar os magistrados para obter uma compreensão aprofundada das suas tendências. Devido a falhas de interpretação na Lei do Cibercrime (Lei nº 109/2009, de 15 de setembro), alguns crimes acabam por ser enquadrados noutras categorias. Um exemplo disso é o caso da criação de perfis falsos nas redes sociais, com o objetivo de difamar ou relatar factos privados da vida de uma pessoa, que acabam enquadrados em crimes de injúria/difamação, devassa da vida privada, ou ainda divulgação de fotografias (Gabinete Cibercrime, 2013).

Através das estatísticas mais recentes da APAV, podemos verificar que no ano de 2019 foram registados 84 casos de cibercrime, 699 de pornografia infantil, e 37 casos de violação de correspondência e telecomunicações (APAV, 2019). O crime de criação de perfis falsos surge como difamação/injúria, com 315 registos, e devassa da vida privada/gravações e fotografias ilícitas, com 113 casos (APAV, 2019).

A Linha Internet Segura da APAV presta apoio a vítimas de cibercrime, e funciona também como uma plataforma de denuncia (APAV, 2019). Entre Janeiro e Dezembro de 2019, no total de 701 denuncias, 679 foram relativas a pornografia infantil. Na vertente de apoio e aconselhamento à vítima, no total de 102 atendimentos, os crimes com valores mais elevados foram os de burla (20 casos), roubo de identidade (12 casos), *phishing* (9 casos), *sextortion* e devassa da vida privada (8 casos cada) e acesso ilegítimo e difamação/injúrias (7 casos cada) (APAV, 2019).

Os valores mais recentes que a APAV possui sobre o *cyberstalking* e *cyberbullying* são apenas de 2013. O Barómetro APAV, acerca das perceções da população sobre *stalking*, *cyberstalking*, *bullying* e *cyberbullying* contou com 1014 entrevistas pessoais e diretas, numa população entre os 15 e 64 anos (Barómetro APAV INTERCAMPUS, 2013). Através deste, podemos observar que os comportamentos mais comuns no *cyberstalking* são os comentários indesejados nas redes sociais e a publicação de falsos testemunhos/acusações em redes socias; e que no *cyberbullying* são a injúria e importunação (Barómetro APAV INTERCAMPUS, 2013).

## 2.7. Fatores de risco

A *internet* é extremamente apelativa, pois devido a uma falta de controlo centralizado, é possível dizer e escrever o que nos apetecer, mas isso também nos pode colocar em contacto com conteúdos ofensivos e abusivos (Caetano, Miranda & Soromenho, 2010). De acordo com a Teoria da Sociedade do Risco, de Ulrick Beck, é possível definir o risco como um estado entre a segurança e a destruição, que afeta o nosso pensamento e determina a nossa ação (Mendes, 2015). Assim, as sociedades preocupam-se com o seu debate, prevenção e gestão (Mendes, 2015).

Um pouco por todo o mundo, a cibercriminalidade é um fenómeno que capta cada vez mais a atenção dos académicos (Nakala & Diunugala, 2020), sendo que a compreensão da sua natureza pode levar a sua prevenção e estratégias de redução, baseadas em preditores teóricos (Nodeland & Morris, 2020). Tendo em conta que qualquer pessoa pode ser uma potencial vítima de cibercrime, existem inúmeros fatores de risco, tais como guardar documentos importantes em lugares poucos seguros, não os destruir antes de os deitar fora e transportar códigos ou palavras-passe na carteira, não instalar ou atualizar o antivírus do computador, aceder a *links*, responder a e-mails ou atender contactos desconhecidos (APAV, 2015).

Postar fotografias *online*, juntamente com vídeos ou outras informações pode trazer problemas a longo prazo aos utilizadores, mesmo que o conteúdo seja mais tarde retirado (Caetano et al., 2010). Não sabemos quem vai aceder às nossas informações, e estas continuam disponíveis na *internet* mesmo quando são eliminadas (Ferreira & Monteiro, 2009). É comum partilharmos dados como o nosso nome, morada e número de cartão de crédito na *internet*, sem termos a total certeza até onde essa informação pode ir parar, ou ser utilizada (Comissão Europeia, 2020). Não verificar as opções de segurança dos perfis, aceitar pedidos de amizade de pessoas desconhecidas e partilhar fotografias íntimas nas redes socias são outros fatores de risco (APAV, 2015).

De acordo com o IUTICF de 2019, 49.0% dos entrevistados evitou realizar algumas atividades *online*, ou limitou a sua frequência, como medida de segurança e precaução, no que respeita ao fornecimento de dados em aplicações sociais ou de trabalho, aquisição de produtos e serviços e atividades bancárias (INE, 2019). Cerca de 27.6% dos utilizadores relataram ainda ter problemas de segurança na *internet*, no período de 12 meses anterior à 20 entrevista, sendo vítimas de *phishing* (18.2%) e *pharming* (14.9%), (INE, 2019). O acesso ilegítimo às suas redes sociais e e-mail, e divulgação de conteúdos sem conhecimento do

próprio, juntamente com o roubo de identidade atingiram percentagens de 1.6% e 1.1% respetivamente (INE, 2019).

O estudo de Nakala e Diunugala (2020), identificou alguns fatores de risco, especificamente direcionados a estudantes universitários. Os autores mediram a sua literacia digital, compreensão de segurança *online*, estatuto socioeconómico e estilo de vida, e tentaram prever de que forma estes podiam constituir fatores de risco para os crimes de criação de contas falsas, *hacking*, *doxing*, *cyberstalking* e fraude pela *internet*. (Nakala & Diunugala, 2020). Os resultados demonstram que um menor contacto com a família, menor concentração nos estudos, maior nível socioeconómico e um número elevado de horas nas redes sociais, juntamente com poucas medidas de segurança e privacidade e uma fraca compreensão informática, são fatores de risco para o cibercrime (Nakala & Diunugala, 2020). Uma fraca consciência do cibercrime, parece estar, do mesmo modo, associada a experiências de vitimação, pois sem esta, os sujeitos não estão alerta dos perigos das redes sociais, e não adotam comportamentos seguros ao utilizar a *internet* (Neazkor et al., 2020). De acordo com os resultados do estudo de Neazkor et al. (2020), o cibercrime parece ser sensível ao género e à idade, no que respeita à consciência deste, sendo menor no género feminino, e mostrando também que diminuiu quanto mais novo for o sujeito.

# 3. ESTUDO EMPÍRICO

## 3.1. Objetivos e hipóteses de investigação

A presente investigação tem como objetivo descrever o perfil sociodemográfico das vítimas de cibercrime, numa amostra de estudantes da Universidade do Porto. Não pretendemos analisar as suas causas, mas sim identificar comportamentos e padrões existentes nesta população, através da aplicação de um questionário estruturado. Assim, recolhemos dados acerca do sexo, idade, curso, nível socioeconómico, conhecimento informático e consciência sobre o cibercrime e comportamentos nas redes sociais, das vítimas de crimes cibernéticos.

Tendo em conta a revisão da literatura efetuada, particularmente as investigações de Nakala e Diunugala (2020) e Neazkor et al. (2020), previmos que o perfil da vítima de

cibercrime seja maioritariamente um individuo do sexo feminino, de cursos sociais e humanísticos, dos primeiros três anos letivos, e menos envolvido nos estudos. Previmos também que seja de maior estatuto socioeconómico e a morar sem a família, passando muitas horas *online* para fins de comunicação e entretenimento, em diversas redes sociais e com pouca literacia digital (H1).

Sugerimos que uma maior utilização de medidas de privacidade e segurança nas redes sociais, se traduza numa menor probabilidade de ser vítima de um cibercrime (H2), e que uma maior consciência do cibercrime e das suas tendências, diminua a probabilidade de experienciar um cibercrime (H3). A adoção eficaz de medidas de segurança e privacidade, e compreensão do cibercrime, leva a que o indivíduo esteja mais atento aos perigos *online*, e que adote comportamentos seguros de utilização das redes socias (Nakala e Diunugala, 2020). Por fim, previmos que os cibercrimes mais frequentes sejam os de *cyberstalking*, fraude, *doxing*, *hacking*, utilização de contas falsas (H4), de acordo com os resultados do estudo de Nakala e Diunugala (2020).

## 3.2. Metodologia

### 3.2.1. Participantes

A amostra final desta investigação é constituída por 144 jovens, 88 do sexo feminino e 56 do sexo masculino, e com idades entres os 18 e 27 anos ($M$ = 21.34, $DP$ = 1.80). Todos são estudantes da Universidade do Porto, de todas as faculdades, à exceção da Faculdade de Ciências da Nutrição e Faculdade de Farmácia. As três mais representadas são a Faculdade de Ciências Biomédicas ($n$ = 25), Faculdade de Ciências ($n$ = 30) e a Faculdade de Psicologia e de Ciências da Educação ($n$ = 39). Da amostra, 25.7% dos estudantes frequenta do 5º ano, 25% do 4º ano, 22.9% do 3º ano, 16% do 2º ano, 8.3% do 6º ano e 2.1% do 1º ano. Em relação ao seu rendimento familiar mensal, cerca de 23.6% dos sujeitos da amostra possuem um rendimento entre os 1500€ e 2000€, 21.5% superior a 2500€, 20.8% entre os 1000€ e 1500€, 13.9% entre os 500€ e 1000€ e 4.2% com rendimentos inferiores a 500€. A maioria destes estudantes (72.9%) vive com a família, 20.1% com colegas ou amigos e 6.9% mora sozinho. Quando questionado o seu conhecimento sobre o cibercrime, 86.8% dos sujeitos já conheciam o termo, e 54.2% tinham consciência dos crimes dependentes da *internet*. No que diz respeito à sua literacia digital, 85.4% sabe o que o que são *cookies* e *spam*.

### 3.2.2. Instrumento

O instrumento utilizado para a recolha de dados foi um questionário estruturado em três partes. A primeira é destinada à obtenção do consentimento informado dos participantes, garantia de anonimato, explicação dos objetivos de investigação e de algumas definições cruciais para o seu preenchimento, juntamente com o tempo estimado de resposta e possibilidade de desistir a qualquer momento sem perdas ou ganhos financeiros.

A segunda parte é constituída por dois grupos de questões: características sociodemográficas e comportamentos nas redes sociais. As características sociodemográficas contêm as questões "sexo", "idade", "faculdade", "ano curricular"; "rendimento familiar mensal", "com quem vive?"", "consciência do cibercrime" e "literacia digital"; os comportamentos nas redes sociais contêm as questões "redes socais utlizadas", "motivos de utilização", "medidas de privacidade" e "medidas de segurança". As variáveis escolhidas para a criação deste questionário foram baseadas nos estudos de Nakala e Diunugala (2020), e Nzeakor et al., (2020), juntamente com uma revisão da literatura acerca dos comportamentos dos jovens nas redes sociais e seus comportamentos de risco

A última parte do questionário possui apenas uma questão, uma lista da qual o participante deve escolher os crimes do qual foi vítima, ou selecionar que não foi vítima de nenhum. A terceira parte deste questionário foi elaborada tendo em conta estatísticas de prevalência do cibercrime e revisão da literatura.

### 3.2.3. Procedimento

O questionário utilizado para a recolha de dados foi construído com recurso à plataforma *online Google Forms*, e o seu *link* foi partilhado nas redes sociais *Facebook* e *Instagram*. Devido a isso a nossa amostra não é probabilística, mas sim de conveniência pois qualquer pessoa com acesso aos seus meios de divulgação podia responder ao questionário.

### 3.2.4. Método de análise de dados

Os dados obtidos com a recolha dos questionários foram analisados com recurso ao programa IBM SPSS *Statistics* (*Statistical Package for Social Sciences*), versão 26. Foram pedidas frequências e percentagens, para avaliar a distribuição dos dados na nossa amostra, e foram utilizados testes de Qui-Quadrado, que permitem averiguar diferenças significativas entre variáveis categóricas.

## 3.3. Resultados

O interesse principal deste estudo é a descrição do cibercrime na população universitária do Porto. Assim, mesmo tendo recolhido questionários de participantes que não foram vítimas deste fenómeno, iremos debruçar-nos sobre a subamostra de estudantes que relataram ter sido vítimas. É igualmente do nosso interesse perceber se uma maior consciência do cibercrime, e uma maior adoção de medidas de privacidade e de segurança nas redes sociais possuem alguma relação com a sua diminuição, pelo que também apresentaremos esses resultados. Assim será possível para nós traçar um perfil vitimológico das vítimas mais comuns deste crime, e entender a sua frequência nesta população.

### 3.3.1. Vitimação por cibercrime

No total de 144 participantes da nossa amostra, foi possível verificar que 101 (70.6%) não foram vítimas de qualquer cibercrime, sendo que apenas 43 (29.4%) o foram.

Quadro 1. Frequências de cibercrimes relatados para homens e mulheres

| Cibercrimes | Homens | Mulheres |
|---|---|---|
| Pharming | 0 | 3 |
| Phishing | 3 | 7 |
| Hacking | 1 | 3 |
| Fraude ou Burla *Online* | 4 | 2 |
| Cyberbullying | 0 | 3 |
| Cyberstalking | 3 | 5 |
| Sextortion | 0 | 4 |
| Partilha e Divulgação Ilegítima de Material Fotográfico e Videográfico | 2 | 4 |
| Assédio nas Redes Sociais | 6 | 15 |
| Acesso Ilegítimo a Redes Sociais | 4 | 9 |
| Criação de Perfis Falsos nas Redes Sociais | 3 | 4 |
| Doxing | 0 | 0 |

**Tipos de Cibercrime.** O Quadro 1 mostra as frequências de cibercrimes registados pelos nossos participantes, para homens e mulheres. Assim, podemos destacar como os quatro mais frequentes os crimes de assédio nas redes sociais (*n* = 21), acesso ilegítimo a redes sociais (*n* = 13), *phishing* (*n* = 10), e *cyberstalking* (n = 8). Em todas as categorias de cibercrime, o sexo feminino registou números superiores, à exceção de burla e fraude *online*, em que os homens relataram 4 casos e as mulheres 2. Os homens não registaram qualquer crime de *pharming*, *cyberbullying* e *sextortion*, e não foi relatado nenhum caso de *doxing* para ambos os sexos. Assim, apenas verificamos parte da H4.

**Vítimas de Cibercrime.** O número total de vítimas da nossa amostra é de 43, correspondendo a 29.9% da nossa população total. Desta subamostra 26 elementos são do sexo feminino, com idade compreendidas entre os 19 e 24 anos (*M* = 21.22, *DP* = 1.48), e 17 são do sexo masculino, com idades entre os 19 e 27 anos (*M* = 21.51, *DP* = 2.23). As mulheres da subamostra correspondem a 29.5% da amostra feminina total, e os homens a 30.4% da amostra total masculina.

A fim de verificar as diferenças entre homens e mulheres para as diferentes tipologias de cibercrime, foi realizado um teste de Qui- Quadrado. Este apenas demonstrou valores significativos para o crime *sextortion*, $\chi^2 = 4.01$, $p = .045$, o que demonstrou uma relação positiva entre este crime e ser do sexo feminino (mulheres vítimas, 2.4%, e homens vítimas, 1.6%). Assim, apenas confirmamos parte da nossa H1, pois as mulheres são vítimas mais frequentes apenas para o cibercrime de *sextortion*.

**Ano Curricular.** Para avaliar a relação entre o ano curricular dos participantes e a experiência de cibercrime, foram criados dois grupos: o primeiro constituído pelo 1º, 2º e 3º ano curricular, e o segundo pelo 4º, 5º e 6º ano. O teste de Qui-Quadrado não mostrou diferenças significativas entre os estudantes que não foram vítimas e os que foram, no entanto registou um valor de $\chi^2 = 4.29$, p = 0.38, para *hacking*. Estes valores representam uma relação significativa entre ser do 4º, 5º e 6º ano e ser uma vítima mais frequente de *hacking* (vítimas do 1º, 2º e 3º ano, 0%, e vítimas do 4º, 5º e 6º ano, 4.7%). Estes valores não estão de acordo com a nossa H1, em que prevemos que as vítimas mais frequentes de cibercrime sejam alunos dos três primeiros anos curriculares.

**Curso.** Ao analisar a nossa amostra, verificamos que Psicologia e Ciências da Educação é a faculdade representada em maior número (27.1%), seguida de Ciências

(20.8%), Ciências Biomédicas (17.4%) e Medicina (9.7%). Engenharia constitui também, 8.3% da nossa amostra, Medicina Dentária, 4.2%, Desporto, 3.5%, e Economia e Gestão e Belas Artes, 2.8%. Por fim, as faculdades representadas em menos número foram Letras (2.1%), Direto (0.7%) e Arquitetura (0.7%).

Os diferentes cursos da nossa amostra foram agrupados em três grupos diferentes: cursos socio humanísticos, constituídos por letras, direito e psicologia e ciências da educação, cursos técnico científicos, constituídos por ciências, ciências biomédicas, desporto, economia e gestão, medicina, medicina dentária e engenharia, e cursos artísticos, formados por belas artes e arquitetura. Farmácia e ciências da nutrição não estão inseridos em nenhum grupo, pois não houve registo de nenhum participante a frequentar estes cursos.

Ao realizar o teste de Qui-Quadrado, não foram encontradas diferenças significativas entre os estudantes que não experienciaram qualquer cibercrime, e os que foram vitimados. Mesmo assim, foram encontrados valores significativos para o crime de *sextortion*, $\chi^2 = 9.52$, $p = .008$. Assim, existe uma relação significativa entre frequentar um curso socio humanístico e ser vítima de *sextortion* (vítimas de cursos socio humanísticos, 8.9%, vítimas de cursos técnico científicos, 0%, e vítimas de cursos artísticos, 0%).

**Literacia Digital.** Ao avaliar as diferenças entre o sexo masculino e feminino, com um teste de Qui- Quadrado encontramos valores de $\chi^2 = 4.07$, $p = .044$, o que tendo em conta as percentagens de 92.9% e 80.7%. Isto significa que existe uma relação significativa entre o sexo feminino e uma maior literacia digital (homens, 42.3% e mulheres, 57.7%), ao contrário do que previu (Nzeakor et al., 2020).

Comparando a amostra que foi vítima, com a que não foi vítima, não encontramos quaisquer diferenças com o teste de Qui- Quadrado. No entanto, são encontradas relações significativas para os crimes de *pharming*, $\chi^2 = 4.33$, $p = .037$, e para assédio nas redes sociais, $\chi^2 = 5.71$, $p = .017$. Concluímos então que existe uma relação significativa entre saber o que são *cookies* e *spam* e não ser vítima de *pharming* (vítimas, 0.8%, e não vítimas, 99.2%), e assédio nas redes sociais (vítimas, 11.4%, e não vítimas, 88.6%).

**Local de Residência.** Observando os estudantes da nossa amostra, verificamos que 72.9% moram com a família, 20.1% com colegas ou amigos, e 6.9% moram sozinhos.

Para analisar estes dados foram criados dois grupos: estudantes a morar com a família, e estudantes a morar sem a família, onde se inserem os que moram com colegas ou amigos, e sozinhos.

Através do teste Qui- Quadrado não encontramos diferenças significativas entre os participantes que não foram vítimas e os que foram. O teste de Qui- Quadrado regista no entanto valores de $\chi^2 = 3.88$, $p = .049$, para o crime de burla ou fraude *online*. Existe então uma relação significativa entre viver com a família e não ser vítima deste cibercrime (vítimas, 5.7%, e não vítimas, 94.3%).

**Rendimento Familiar Mensal.** Ao verificar o rendimento familiar mensal dos estudantes da nossa amostra, observamos que 23.6% possui um rendimento entre os 1500€ e 2000€, 21.5% tem um rendimento superior a 2500€, 20.8% entre os 1000€ e 1500€, 16% entre os 2000€ e 2500€, 13.9% entre os 500€ e 1000€, e 4.2% possui rendimentos inferiores a 500€.

Para analisar a relação entre o rendimento familiar mensal e a vitimação por cibercrime, foram criados três grupos: rendimento baixo, com os rendimentos inferiores a 500€ e entre os 500€ e 1000€, rendimento médio, com rendimentos entre os 1000€ e 1500€, e os 1500€ e 2000€, e rendimento alto, entre os 2000€ e 2500€, e superior a 2500€.

Ao realizar o teste de Qui-Quadrado não são encontradas diferenças significativas entre os estudantes que não foram vítimas de cibercrime e os que foram. O teste de Qui-Quadrado registou um valor significativo para *cyberbullying*, $\chi^2 = 10.56$, $p = .005$, o que representa uma relação positiva entre possuir um rendimento familiar mensal baixo e ser vítima deste cibercrime (rendimento baixo, 100%, rendimento médio, 0% e rendimento alto, 0%). Estes resultados não estão de acordo com a nossa H1, em que prevemos que os estudantes com rendimentos mais altos sejam vítimas mais frequentes de cibercrime.

### 3.3.2. Comportamentos nas Redes Sociais

**Redes Sociais Utilizadas.** Ao analisar as redes sociais utilizadas pelos participantes do nosso estudo, verificamos que todos eles as utilizam. As redes sociais com maior utilização foram o *Messenger* (97.9%), *Facebook* (95.1%), *WhatsApp* (93.8%) e o *Youtube* (92.4%). O *Instagram* registou uma utilização de 88.9% e *Twitter*, 38.9%, *Tik Tok*, 18.1%. As aplicações de namoro virtual, *Tinder* e *Badoo*, registaram a menor utilização, com uma percentagem de 9% e 0.7%, respetivamente. Apenas três dos nossos participantes referiram

que utilizavam outra aplicação para além das enumeradas, sendo estas o *Discord*, *Reddit* e *Wattpad*, com uma percentagem de utilização de 0.7% cada uma.

Para avaliar a relação entre o número de redes sociais utilizadas pelos estudantes, e a experiência de cibercrime, foram constituídos três grupos: os estudantes que utilizam poucas aplicações, que utilizam 3 ou menos, os que utilizam algumas, 4 a 6, e os estudantes que utilizam muitas, pois utilizam entre 7 a mais de 9 redes sociais. Ao analisar estes grupos, verificamos que 80.6% da nossa amostra utiliza entre 4 a 6 redes sociais, 13.9% utiliza entre 7 e mais de 9, e apenas 5.6% dos nossos participantes utilizam 3 ou menos redes sociais.

Com o teste de Qui-Quadrado não foram encontradas diferenças entre os participantes que não foram vitimados e os que foram, mas foi registado um valor de $\chi^2 = 6.60$, $p = .037$, para o cibercrime de acesso ilegítimo a redes sociais. Assim, existe uma relação significativa entre utilizar muitas redes sociais e ser vítima deste crime (vítimas que utilizam poucas redes sociais, 0%, e vítimas que utilizam muitas, 25%).

**Motivos de Utilização.** Ao analisar os comportamentos da nossa amostra nas redes socais, verificamos que comunicar com os amigos (98.6%), ver vídeos e filmes (91%), entretenimento (90.3%) e realizar pesquisas (84.7%) são os principais motivos da sua utilização. Os motivos menos comuns para a utilização das redes sociais são a partilha de informações bancárias (1.4%), revelar informações pessoais, como o nome completo, idade, morada e número de telemóvel (3.5%), partilhar fotografias e vídeos íntimos (4.9%), e marcar encontros com desconhecidos (5.6%). Em relação aos restantes motivos, fazer trabalhos regista uma percentagem de 79.2%, marcar encontros com amigos, 78.5%, comunicar com a família, 72.2%, publicar fotografias e vídeos, 68.1%, fazer compras *online*, 54.2%, participar em petições e questionários, 46.5%, tirar dúvidas com os professores, 12.5%, comunicar com desconhecidos, 11.1%, e partilhar informações privadas, 6.9%.

Foi também incluída a opção "outra", neste ponto do nosso questionário, e apenas três participantes referiram outros motivos de utilização das redes sociais, sendo estes "comunicação interna entre os alunos da faculdade", "pedir orientações no *google maps*", e "publicitar serviços de vendas".

Recorrendo ao teste de Qui-Quadrado, apenas encontramos diferenças significativas entre o grupo que não foi vítima e o que foi vítima de cibercrime, para os motivos de publicar fotografias e vídeos, para partilhar fotografias e vídeos íntimos, e realizar pesquisas, com valores de $\chi^2 = 9.22$, $p = .003$, $\chi^2 = 5.42$, $p = .018$, e $\chi^2 = 5.02$, $p = .025$, respetivamente. Assim, existe uma relação significativa entre não publicar fotografias e vídeos (vítimas que

publicam, 13%, e não vítimas que não publicam, 87%), não partilhar fotografias e vídeos íntimos (vítimas que partilham, 71.2%, e não vítimas que não partilham, 72.3%), e realizar pesquisas (vítimas que não fazem pesquisas, 26.2%, e não vítimas que fazem pesquisa 73.8%), e não ser vítima de cibercrime.

Em relação aos restantes cibercrimes, foram registados valores significativos para criação de perfis falsos, *pharming*, *cyberbullying*, partilha e divulgação ilegítima de material fotográfico e videográfico, fraude e burla *online*, e *cyberstalking*. Para o crime de criação de perfis falsos, foram observados valores significativos de $\chi^2 = 4.69$, $p = .030$, $\chi^2 = 4.29$, $p = .038$, $\chi^2 = 5.55$, $p = .018$, e $\chi^2 = 8.88$, $p = .003$, para os motivos de comunicar com a família, tirar dúvidas, publicar fotografias e vídeos, e fazer compras *online*, respetivamente. Desta forma, existe uma relação significativa entre comunicar com a família (vítimas que comunicam, 6.7%, e vítimas que não comunicam, 0%) e tirar dúvidas (vítimas que tiram dúvidas, 16.7%, e vítimas que não o fazem 3.2%), e uma redução deste cibercrime. Existe também uma relação entre publicar fotografias e vídeos (vítimas que partilham, 6.1%, e vítimas que não partilham, 0%), e fazer compras *online* (vítimas que compram online, 9%, vítimas que não compram *online*, 0%), e ser vítima do crime de criação de perfis falsos.

O cibercrime de partilha e divulgação ilegítima possui uma relação positiva com a publicação de fotografias e vídeos, participação em inquéritos e questionários e compras *online*, com valores de $\chi^2 = 4.74$, $p = .029$, $\chi^2 = 9.48$, $p = .002$, e $\chi^2 = 7.57$, $p = .006$, respetivamente. Estes valores representam uma relação significativa entre partilhar fotografias e vídeos (vítimas que partilham, 6.1%, e vítimas que não partilham, 0%), participar em petições e questionários (vítimas que participam, 9%, e vítimas que não participam, 0%), e fazer compras pela *internet* (vítimas que fazem compras, 7.7%, e vítimas que não fazem compras, 0%), e ser vitima de divulgação e partilha ilegítima.

São registadas relações significativas entre o crime de *cyberstalking* e a publicação de fotografias e vídeos, $\chi^2 = 6.37$, $p = .012$, fazer trabalhos, $\chi^2 = 3.86$, $p = .049$, e fazer compras online, $\chi^2 = 4.32$, $p = .038$. Desta forma, verificamos uma relação significativa entre publicar fotografia e vídeos (vítimas que partilham, 8.2%, e vítimas que não partilham, 0%), fazer trabalhos (vítimas que fazem trabalhos, 7%, e vítimas que não fazem trabalhos, 0%), e fazer compras online (vítimas que fazem compras, 9%, e vítimas que não, 1.5%), e nãos ser uma vítima frequente deste cibercrime.

Encontramos também uma relação significativa entre o crime de *pharming* e tirar dúvidas com os professores, $\chi^2 = 4.94$, $p = .026$, o que representa uma relação entre tirar

dúvidas e ser uma vítima mais frequente desse crime (vítimas que tiram dúvidas, 11.1%, e vítimas que não tiram dúvidas, 0.8%). Para o crime de fraude e burla, são registados valores de $\chi^2 = 4.20$, p =m .040, para a realização de pesquisas, o que representa uma relação significativa entre não fazer pesquisas e ser vítima de fraude e burla na *internet* (vítimas que não fazem pesquisas, 13.6%, e vítimas que o fazem, 2.5%). Por último, são registados valores de $\chi^2 = 4.66$, $p = .031$, para a relação entre participar em petições e questionários e cyberbullying. Assim, existe uma relação significativa entre participar em questionários e petições *online* e ser vítima de *cyberbullying* (vítimas que participam, 4.5%, vítimas que não participam, 0%).

**Número de Horas *Online*.** Para analisar a relação entre o número de horas *online* e a vitimação por cibercrime, foram criados três grupos: os estudantes que passam poucas horas *online*, que utilizam as redes sociais por menos de 1h ou entre 1h e 1h30, os que passam algumas horas, entre 1h30 e 2h ou entre 2h e 2h30, e os que passam muitas horas, entre 2h30 e 3h ou mais de 3h *online*. Ao avaliar os nossos participantes, verificamos que 44.4% passam algumas horas nas redes sociais, 35.4% passam muitas horas, e 20.1% passa poucas horas na *internet*.

Ao realizar o teste de Qui-Quadrado não são registadas diferenças significativas entre os estudantes que não foram vítimas e os que foram. O teste de Qui-Quadrado registou um valor de $\chi^2 = 7.29$, p = .026, para o crime de acesso ilegítimo a redes sociais, o que mostra uma relação significativa entre passar algumas e muitas horas *online* e ser vítima deste cibercrime (vítimas que passam algumas horas *online*, 14.1%, vítimas que passam muitas horas, 7.8%, vítimas que passam poucas horas, 0%). Isto está de acordo com a nossa H1, em que prevemos que as vítimas mais frequentes de cibercrime passei algumas a muitas horas nas redes sociais.

### 3.3.3. Consciência do cibercrime

Analisando as diferenças entre homens e mulheres com um teste de Qui- Quadrado, verificamos que estas apenas existem para "conhecia os crimes dependentes da *internet*", com $\chi^2 = 6.91$, $p = .009$. Isto mostra que existe uma relação significativa entre o sexo feminino e uma menor consciência dos crimes dependentes da *internet*, pois 72.7% das mulheres não os conheciam, em comparação com 27.3% dos homens não tinham consciência destes.

Verificando os participantes que não foram vítimas e os que foram, não encontramos qualquer diferença significativa. Apenas para o crime de *pharming* se verificou uma relação positiva com a consciência do cibercrime, para o conhecimento de crimes dependentes da *internet.* O teste de Qui- Quadrado mostrou valores de $\chi^2 = 4.75$, $p = .029$, o que representa uma relação positiva entre o conhecimento destes crimes e uma menor experiência de vitimação por *pharming* (vítimas, 0%, e não vítimas, 100%).

### 3.3.4. Medidas de segurança e de privacidade nas redes sociais

Ao analisar as medidas de segurança adotadas pelos participantes da nossa amostra, verificamos 74.3% tem um antivírus instalado no seu computador, telemóvel ou tablet, mas que apenas 48% o atualiza quando necessário. Cerca de 90.3% não termina a sessão nas suas redes sociais, e 18.8% tem as suas credenciais de acesso escritas em papel. Quanto à partilha das suas credenciais de acesso, nenhum estudante as partilhou com desconhecidos, e 9% partilhou-as com familiares ou amigos. Verificando as medidas de privacidade adotadas pelos estudantes, averiguamos que 72.2% possui os seus perfis privados, e que apenas 6% possui a sua morada, número de telemóvel e e-mail disponíveis nas suas redes sociais. Da nossa amostra 65.3% dos participantes apenas permitem que pessoas autorizadas vejam os seus vídeos e fotografias, no entanto 59.7% permitem que qualquer pessoa os contacte nas redes sociais.

**Medidas de Segurança.** A fim de averiguar as diferenças entre homens e mulheres, em relação às medidas de segurança, foi realizado um teste de Qui- Quadrado. Apenas foram encontradas diferenças significativos para "credenciais de acesso escritas", $\chi^2 = 4.13$, $p = .042$, o que significa que existe uma relação significativa entre se o sexo feminino e ter as credenciais escritas (homens, 22.2% e mulheres, 77.8%).

Ao analisar as diferenças entre os estudantes que não foram vítimas e os que foram, não observamos qualquer diferença significativa. No entanto, ao observar a população vitimada, reparamos que existem diferenças significativas para o crime de *cyberbullying* e a medida de segurança "atualizo o antivírus com frequência", com $\chi^2 = 6.72$, $p = .010$. Existe então uma relação significativa entre utilizar esta medida de segurança e ser vítima de *cyberbullying* (vítimas que atualizam o antivírus, 6.3%, e vítimas que não atualizam, 0%). Por último, encontrámos diferenças significativas entre o crime de criação de perfis falsos nas redes sociais, e a medida de segurança "termino a minha sessão nas redes sociais", com

$\chi^2 = 5.71$, $p = .017$. Assim, podemos concluir que existe uma relação significativa entre terminar a sessão nas redes sociais e ser vítima deste crime (vítimas que terminam a sessão, 21.4%, e vítimas que não terminam, 3.1%).

Estes resultados estão contra parte da nossa H2, em que prevemos que uma maior adoção de medias de segurança possua uma relação positiva com uma redução na experiência de vitimação.

**Medidas de Privacidade.** Foi realizado um teste de Qui- Quadrado, para verificar as diferenças entre homens e mulheres, mas este não mostrou qualquer diferença significativa para as medidas de privacidade.

Ao analisar a relação entre os participantes quem não foram vítimas de cibercrime e os que foram, através de um teste de Qui- Quadrado, não foram observadas diferenças significativas entre os grupos. Utilizando novamente o teste de Qui-Quadrado, encontramos apenas duas relações significativas, para o crime de divulgação e partilha ilegítima de material videográfico e fotográfico, para a medida "perfis privados" e "apenas pessoas autorizadas podem ver as minhas fotografias e vídeos. Respetivamente, obtemos valores de $\chi^2 = 4$, $p = .045$ e $\chi^2 = 5.25$, $p = .022$. Desta forma os resultados indicam que existe uma relação significativa entre ter os perfis privados e não ser vítima deste crime (vítimas, 4.3% e não vítimas, 99.7%), e entre apenas permitir que pessoas autorizadas tenham acesso aos nossos vídeos e fotografias e não ser vítima deste cibercrime (vítimas, 3.9% e não vítimas, 93.6%).

Assim confirmamos parte da nossa H2, em que prevemos que existe uma relação positiva entre a não experiência de vitimação e a adoção de medidas de privacidade nas redes sociais, para este cibercrime e para estas duas medidas em específico.

## 4. Discussão

O nosso estudo tinha por objetivo caracterizar as vítimas de cibercrime, numa amostra de estudantes universitários, bem como verificar os cibercrimes mais frequentes, e a influência da literacia digital, consciência do fenómeno, adoção de medidas segurança e

privacidade na experiência de vitimação. Desta forma, a análise dos dados foi dividida em três secções, a vitimação por cibercrime, comportamentos nas redes sociais, e a consciência do cibercrime. Foram também estabelecidos dois grupos, os estudantes que não foram vítimas de cibercrime, e os estudantes que o experienciaram, a fim de comparar os resultados obtidos, verificando também diferenças relativas ao género.

A nossa primeira hipótese prevê que as vítimas mais frequentes sejam do sexo feminino, no entanto os autores e estatísticas não possuem uma opinião comum. De acordo com a APAV (2015), as vítimas mais comuns são homens, mas com estabilidade financeira. De acordo com os resultados da investigação de Nzeakor et al. (2020), as mulheres estão em maior risco de serem vítimas, pois parecem possuir menos literacia digital, fator que por si só constitui um risco. No entanto os nossos resultados demonstraram que as raparigas possuíam uma maior literacia digital que os rapazes. Recentemente, com a situação global causada pelo COVID-19 o cibercrime contra as mulheres aumentou. Na índia, entre 25 de Março e 25 de Abril, foram registadas 412 queixas por mulheres, devido a abuso, exposição indecente e fotografias não solicitadas, *sextortion*, *phishing* e ameaças e chantagem, acreditando os especialistas de que se trata de uma ínfima porção da situação real (NDTV, 2020). Os resultados da nossa investigação demonstram que as raparigas são vítimas mais frequentes de cibercrime,mas apenas para *sextortion*, o que está de acordo com as tendências atualmente registadas.

Como agora referido, uma reduzida literacia digital, por si só, constitui um fator de risco para a vitimação por cibercrime, pois quanto menos informado um sujeito está, mais riscos ele corre *online* (APAV, 2015). Os nossos resultados demonstraram que as vítimas mais frequentes na nossa amostra não sabiam o que eram *cookies* ou *spam*, possuindo assim uma reduzida literacia digital. Estes resultados estão de acordo com os estudos de Nzeakor et al. (2020), e Nakala e Diunugala (2020), os dois últimos com um estudo especificamente direcionado para estudantes universitários. Na mesma linha de pensamento, considerámos que os participantes de cursos socio humanísticos seriam vítimas mais frequentes, por não possuírem conhecimentos informáticos tão elevados como os participantes de cursos técnicos, teoria que confirmamos com os nossos resultados. De acordo com Nzeakor et al., (2020), o cibercrime parece ser sensível à idade, pelo que considerámos os alunos dos três primeiros anos curriculares como possíveis vítimas mais frequentes. Contrariamente às nossas expectativas, os alunos do 4º, 5º e 6º ano curricular relataram um maior número de experiências de vitimação. Assim, não confirmamos esta parte da nossa primeira hipótese, relativa ao perfil das vítimas. Não confirmamos a hipótese segundo a qual as vítimas mais

comuns possuíssem rendimentos familiares mensais mais elevados, tal como prevê a investigação de Nakala e Diunugala (2020). Em vez disso, os nossos resultados demonstraram que as vítimas mais comuns possuíam rendimentos familiares baixos. É curioso notar, no entanto, que estes valores foram significativos para os crimes de *cyberbullying*, pois a maior parte das investigações encontradas prevê que as vítimas de meio socio económicos mais elevados sejam vitimadas mais frequentemente, mas para crimes de *phishing*, *pharming* e *doxing*. Sendo o cibercrime um fenómeno tão heterogéneo, surge a ideia de que cada uma das suas manifestações deve ser avaliada de maneria independente, e tendo em conta diferentes fatores.

Continuando a avaliar o perfil das vítimas mais frequentes de cibercrime, na nossa amostra, verificamos que estas não moram com a família e que utilizam muitas redes sociais, e por muitas horas, tal como tínhamos previsto. A família funciona como um fator de proteção, devido à vigilância que exerce sobre o sujeito, e viver sem esta coloca o estudante em maior risco de ser vitimado (Nakala & Diunugala, 2020). A exposição à *internet* por si só basta para colocar o individuo em risco (APAV, 2015), quanto mais quando este utiliza muitas redes sociais e por número elevado de horas (Nakala & Diunugala, 2020).

A forma como os participantes utilizam a *internet* é também relevante, sendo que estes a utilizavam principalmente para partilhar fotografias e vídeos, alguns de cariz íntimo, fazer compras *online*, comunicar com a família, tirar dúvidas com os professores, participar em inquéritos e questionários e fazer trabalhos. A partilha de vídeos e fotografias está de acordo com o que esperávamos, pois constitui um fator de risco (Caetano et al., 2020), juntamente com as compras *online*, mas os restantes comportamentos não eram de esperar. De acordo com Nakala e Diunugala, a concentração nos estudos e a comunicação com a família são fatores de proteção, pois o estudante não se aventura em *sites* duvidosos. Esta tendência poderá ser explicada pelo aumento de horas na *internet*, com as info aulas, e pelas reuniões de trabalhos de grupo *online*, pois um elevado número de horas nas redes sociais constitui um risco (Nakala & Diunugala, 2020). A possibilidade do estudante carregar em *links* falsos e enganosos aumenta nesta fase, o que está de acordo com o aumento dos casos de *phishing*, devido à pandemia de COVID-19 (NDTV, 2020). No entanto, não o podemos afirmar com certezas, pois este estudo é meramente exploratório.

Em relação à nossa segunda hipótese confirmamos as nossas expetativas, mas com uma exceção. A adoção de medidas de privacidade e de segurança nas redes sociais possui um efeito significativo na redução da experiência de vitimação, (APAV, 2015), mas adotar a medida de segurança "termino a sessão nas redes sociais", colocou os participantes em

risco de ser alvo de criação e perfis falsos nas redes sociais. Não existe literatura que suporte estes resultados, pelo que pode ser uma falha do estudo em si, ou de um contexto muito específico dos nossos participantes. Confirmamos também a nossa terceira hipótese, pois uma maior consciência do cibercrime apareceu relacionada com uma vitimação reduzida por cibercrime, tal como defende Nakala e Diunugala (2020).

Para terminar, previmos na nossa quarta hipótese que os cibercrimes mais comuns seriam o *cyberstalking*, fraude ou burla, *doxing*, *pharming* e criação de contas falsas, devido às estatísticas nacionais existentes. Os crimes mais frequentes na nossa amostra foram o assédio nas redes sociais, acesso ilegítimo a redes sociais, *cyberstalking* e *phishing*, sendo que não confirmamos a nossa quarta hipótese. Estes resultados não estão de acordo com as estatísticas, nem com a literatura encontrada, mas estas foram regidas num contexto pré-pandemia. Como podemos verificar, a pandemia vivida provocou uma alteração nos nossos hábitos e o cibercrime encontrou novas formas de atuar. As mulheres parecem ser os principais alvos, vítimas de crimes de cariz sexual e de assédio, e os crimes de *phishing* aumentaram, devido à criação de *links* maliciosos relacionados com o COVID-19 (NDTV, 2020).

## 5. Conclusões

A presente investigação constitui um estudo exploratório, para a caracterização do perfil das vítimas mais comuns de cibercrime, numa população de estudantes universitários, e visando a influência da consciência deste fenómeno e a tomada de medidas de segurança e privacidade, para a redução na experiência de vitimação.

Sendo o cibercrime um fenómeno versátil e difícil de detetar, muitos indivíduos nem imaginam que foram vítimas (Abdulai, 2020; Nzeakor et al., 2020), sendo os efeitos apenas sentidos mais tarde. Desta forma, quando questionamos os nossos participantes sobre se estes foram vítimas de algum cibercrime, existe a possibilidade dos próprios não estarem conscientes de que o foram. Este facto por si só constitui uma barreira ao estudo do cibercrime, pois sem mecanismos que permitam averiguar com total veracidade uma experiência de vitimação, contamos com o testemunho da nossa amostra para prosseguir com a nossa investigação.

Desta forma, o primeiro desafio que esta investigação encontrou foi a versatilidade do próprio fenómeno, e o seu caráter heterogéneo. A *internet* e as redes sociais são ferramentas relativamente recentes na nossa história, e os cibercriminosos sabem tirar partido da nossa ingenuidade ao utilizá-las. Por se tratar de um crime que não provoca danos imediatos e visíveis, este ainda não é olhado com total atenção, e nem a justiça ou forças policiais estão preparadas para lidar com as vítimas, e possível recolha de provas.

Assim, a literatura existente é ainda insuficiente, e muito dispersa, cada uma focando-se nas diferentes componentes deste fenómeno. Como vimos, existem crimes especificamente relacionados com a *internet*, como o *phishing* ou *doxing*, estes difíceis para a vítima de detetar, e encontramos também crimes que tradicionalmente não eram realizados com recurso à *internet*, mas que utilizam agora este meio para mais facilmente aceder às suas vítimas, como o *cyberbulying* e assédio nas redes sociais.

O facto de cada um destes cibercrimes ter uma natureza diferente, inerente a cada um, torna complexa a análise deste fenómeno, dificuldade que encontrámos neste estudo. Os crimes de *pharming* e *phishing* possuem uma natureza financeira, em que o objetivo do criminoso é enriquecer, ao passo que um crime de assédio possui um caráter difamatório, com o objetivo de controlar e humilhar a vítima. A nossa investigação não teve em consideração as especificidades de cada vertente deste fenómeno, analisando todas elas num único estudo. Devido a isso, acreditamos que o contributo deste estudo exploratório é demonstrar que o cibercrime merece uma análise aprofundada, e que cada um dos cibercrimes deve ser avaliado de acordo com fatores e populações especificas para cada um.

Outra limitação do nosso estudo, foi o facto da amostra ser de conveniência, e de não existir um equilíbrio entre o número de alunos de cada faculdade, e entre a população masculina e feminina. O nosso questionário não foi distribuído por e-mail dinâmico entre as várias faculdades, por limitações temporais, contanto apenas com as redes sociais para o distribuir. Uma grande parte da amostra foi constituída por alunos da Faculdade de Psicologia e de Ciências da Educação, pois contámos com a participação de pessoas conhecidas e de um "passa a palavra", para o preencher.

Para terminar, o próprio instrumento de recolha de dados possuí alguns erros, que apenas foram apontados no processo de recolha de dados. Especificamente, quando interrogados sobre se os sujeitos partilhavam informações com desconhecidos, ou marcavam encontros com desconhecidos, a questão estaria melhor formulada se tivéssemos utilizado a expressão "conhecer pessoas novas", ou "partilhar informações com pessoas novas". Alguns dos participantes apontaram que automaticamente não escolheriam essa opção devido a

expectativas morais, ou para não transparecer uma imagem de irresponsabilidade aos investigadores.

Para concluir, mesmo com as suas falhas e limitações, acreditamos que este estudo foi um contributo positivo para a investigação do cibercrime, e permitiu entender que é necessário adotar uma perspetiva muito mais complexa, para o entender na sua totalidade.

## 6. Referências Bibliográficas


Abdulai, M. A. (2020). Examining the effect of victimization experience on fear of cybercrime: university students' experience of credit/debit card fraud. *International Journal of Cyber Criminology*. *14*(1), 157–174. https://doi.org/10.5281/zenodo.3749468

Alves, A. J. M. (2009). *Criador e Criatura: o papel das tecnologias da informação e comunicação no novo contexto das tecnologias emergentes.* (Dissertação de Doutoramento). Faculdade de Ciências Sociais e Humanas Universidade Nova de Lisboa, Portugal.

Angelo, E. (2016). Redes sociais virtuais na sociedade da informação e do conhecimento: economia, poder e competência informacional. *Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação*, *21*(46), 71-80. https://doi.org/10.5007/1518-2924.2016v21n46p71

APAV. (2015). A realidade do cibercrime. Disponível em: https://apav.pt/cibercrime/

APAV. (2019). Relatório Anual 2019. APAV. https://apav.pt/apav_v3/images/pdf/Estatisticas_APAV - Relatorio_Anual_2019.pdf

Barómetro APAV INTERCAMPUS (2013). Perceção da População Portuguesa sobre Stalking, Cyberstalking, Bullying e Cyberbullying. APAV. https://apav.pt/apav_v3/images/pdf/Barometro_APAV_Intercampus_5_VEC_2013.pdf

Brito, B. J. Q., Gordia, A. P., & Quadros, T. M. B. (2016). Estilo de vida de estudantes universitários: estudo de acompanhamento durante os dois primeiros anos do curso de graduação. *Medicina (Ribeirão Preto)*, *49*(4), 293-302. 24

Caetano, H., Miranda, G. L., & Soromenho, G. (2010). Comportamentos de risco na internet: um estudo realizado numa escola do ensino secundário. *Revista Latinoamericana de Tecnología Educativa - RELATEC, 9*(2), 167-185.

Campos, L., & Canavezes, S. (2007). *Introdução à globalização*. Retirado de: https://dspace.uevora.pt/rdpc/handle/10174/2468

Conradie, L., Pitchford, M., Myers, E., Barnes, J., & Short, E. (2020). Cyberharassment awarness course (cybac): influences from domestic abuse perpetrator programmes for its design and function. *International Journal of Cyber Criminology, 14*(1), 220–235. https://doi.org/10.5281/zenodo.3750140

Comissão Europeia (2020). Digital Privacy. European Commission. https://ec.europa.eu/digitalsingle-market/en/policies/online-privacy

Diário da Républica. Decreto-Lei nº48/95 de 15 de Março.

Dias, A. C. G., & Teixeira, M. A. P. (2008). Auto-revelação na Internet: um estudo com estudantes universitários. *Aletheia, 27*(1), 23-35.

Ferreira, P., & Monteiro, A., F. (2009). Riscos da utilização das TIC. *Revista de educação, 1*(1), 88-99.

Gabinete Cibercrime. (2013). Relatório de Atividades de 2013. Ministério Público. http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorioda-atividade_cibercrime_2013.pdf

Giaretta, J. B. Z., & Di Giulio, G. M. (2018). O papel das tecnologias de comunicação e informação (TIC) no urbano do século XXI e na emergência dos novos movimentos sociais: reflexões a partir de experiências na megacidade de São Paulo. *Rev. BRas. estud. uRBanos Reg. 20*(1), 161-179.

INE. (2019). Sociedade da informação e do conhecimento Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias. INE.

https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=354447153&DESTAQUESmodo=2 25

Lee, S. Z. (2020). A basic principle of physical security and its link to cybersecurity. *International Journal of Cyber Criminology, 14*(1), 203–219. DOI: 10.5281/zenodo.3749780

Lei do Cibercrime – Lei nº 109/2009 – Ministério da Justiça.

Lima, G. A. B. O., Pinto, L. P., & Laia, M. M. (2002). Tecnologia da informação: impactos na sociedade. *Inf.Inf., Londrina, 7*(2), 75- 94.

Mendes, J. M. (2015). Ulrich Beck: a imanência do social e a sociedade do risco. *Análise Social, 214*, 211-215.

Meşe, C., & Aydin, G. C. (2019). The use of social networks among university students. *Academic Journals, 14*(6), 190-199. https://doi.org/ 10.5897/ERR2018.3654

Mira, J. E., & Bodoni, P., S., B. (2011). Os impactos das redes sociais virtuais nas relações de jovens e adultos no ambiente académico nacional. *Revista de Educação, 14*(17), 103-115.

Nakala, S., & Diunugala, H. (2020). Factors Associating with Social Media related Crime Victimization: Evidence from the Undergraduates at a Public University in Sri Lanka. *International Journal of Cyber Criminology*, *14*(1), 174–184. https://doi.org/10.5281/zenodo.3748685

NDTV. (2020). "Significant" Increase In Cyber Crimes Against Women During Lockdown: Experts. NDTV. https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-during-lockdown-experts-2222352

Nodeland, B., & Morris, R. (2020). The Impact of Low Self-control on Past and Future Cyber Offending. *International Journal of Cyber Criminology, 14*(1), 106–120. https://doi.org/10.5281/zenodo.3742075.

Nogueira, M. J. C. (2017). *Saúde mental em estudantes do ensino superior: fatores protetores e fatores de vulnerabilidade*. (Dissertação de Doutoramento). Universidade de Lisboa, Portugal.

Nzeakor, O. F., Nwokeoma, B. N., & Ezeh, P., J. (2020). Pattern of Cybercrime Awareness in Imo State, Nigeria: An Empirical Assessment. *International Journal of Cyber Criminology, 14*(1), 283–299. https://doi.org/10.5281/zenodo.3753223

Oliveira, E. S. G. (2017). Adolescência, internet e tempo: desafios para a Educação. *Educar em Revista, 64,* 283-298. 26

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: an examination. *International Journal of Cyber Criminology, 14*(1), 81–105. https://doi.org/10.5281/zenodo.3741131

Saha, S. R., & Guha, A. K. (2019). Impact of social media use of university students. *International Journal of Statistics and Applications, 9*(1), 36-43 https://doi.org/10.5923/j.statistics.20190901.05

Saldanha, J. M. L., Brum, M. M., & Mello, R. C. (2016). As novas tecnologias de informação e comunicação entre a promessa de liberdade e o risco de controle total: estudo da jurisprudência do sistema interamericano de direitos humanos. *Anuario Mexicano de Derecho Internacional, 16,* 461-498.

Santos, V. L. C., & Santos, J. E. (2014). As redes sociais digitais e a sua influência na sociedade e educação contemporâneas. *Holos, 6*, 307-328.

Sousa, C. H. M., & Cardoso, C. (2011). As redes socais digitais: um mundo em transformação. *Agenda Social, 5*(1), 65 – 78.

Schreuders, Z. C., Cockcroft, T., Elliott, J., Butterfield, E., Soobhany, A., R., & Shan-AKhuda, M. (2020). Needs Assessment of Cybercrime and Digital Evidence in a UK

Police Force. *International Journal of Cyber Criminology, 14* (1), 316- 340. https://doi.org/10.5281/zenodo.3757271

Silva, R. M., Costa, E. S., & Oliveira, M. R. (2019). A influência das redes sociais sob a construção da subjetividade humana. Disponível em: https://www.psicologia.pt/artigos/ver_artigo.php?a-influencia-das-redes-sociaissob-a-construcao-da-subjetividade-humana&codigo=A1365

Vermelho, S. C., Velho, A. P. M., Bonkovoski, A., & Pirola, A. (2014). Refletindo sobre as redes sociais. *Educ. Soc., 35*(126), 179-196.

# ANEXOS

**Anexo 1.**

Cibercrime

Parte 1

Venho por este meio solicitar a sua participação no preenchimento deste questionário, com a duração aproximada de 10mn. Este é destinado à realização da minha dissertação de mestrado, orientada pelo Professor Doutor Jorge Negreiros, para obtenção do grau de mestre pela Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto. O nosso objetivo é fazer uma caracterização do perfil sociodemográfico das vítimas de cibercrime, na população universitária da Universidade do Porto.

Para o preenchimento do questionário não será pedida a sua identidade, pelo que garantimos o seu anonimato. Este estudo não lhe trará nenhum gasto/ganho financeiro e é livre de desistir a qualquer momento.

**Termos chave:**

**assédio:** qualquer comportamento indesejado com o objetivo de perturbar, constranger ou afetar a dignidade, baseado em fatores discriminatórios | **cibercrime:** qualquer crime cometido com o uso da internet, ou facilitado por qualquer meio tecnológico digital | ***cyberbullying:*** manifestação das práticas de *bullying* através da *internet* | ***cyberstalking:*** comportamentos constantes de perseguição e ameaça realizados através da internet | ***doxing:*** pesquisa e transmissão de dados privados de um indivíduo ou instituição | ***pharming:*** instalação de um vírus no computador de um usuário, para o desviar para páginas falsas, e roubar informações pessoais e financeiras | ***phishing:*** envio de mensagens eletrónicas que contêm ligações para páginas de internet falsas, semelhantes a outras existentes, para recolher informações de contas bancárias e cartões | ***sextortion:*** quando se ameaça revelar informações da vida privada ou confidenciais, caso não forneçam imagens de caracter sexual, favores sexuais ou dinheiro.

Obrigada pela colaboração!

Ana Filipa Bettencourt

Consciente do acima referido:

Concordo em participar neste estudo □

Não concordo em participar neste estudo □

Parte 2

Fatores Demográficos:

1. Sexo: Masculino □  Feminino □

2. Idade (escreva apenas o número): _____

3. Faculdade:

Arquitetura □

Belas Artes □

Ciências □

Ciências Biomédicas □

Ciências da Nutrição e da Alimentação □

Desporto □

Direito □

Economia e Gestão □

Engenharia □

Letras □

Medicina □

Medicina Dentária □

Farmácia □

Psicologia e Ciências da Educação □

4. Ano curricular:

1º ano □

2º ano □

3º ano □

4º ano □

5º ano □

6º ano □

5. Rendimento familiar mensal:

Inferior a 500€ □

Entre 500€ e 1000€ □

Entre 1000€ e 1500€ □

Entre 1500€ e 2000€ □

Entre 2000€ e 2500€ □

Superior a 2500€ □

6. Com quem vive?:

Com a família □

Em apartamento com colegas ou amigos □

Sozinho □

7. Consciência do cibercrime (assinale apenas se a resposta for "SIM"):

Já conhecia o termo "cibercrime" □

Já conhecia crimes dependentes da internet (e.g. hacking, phishing, pharming, doxing) □

8. Literacia digital (assinale apenas se a resposta for "SIM"):

sei o que são cookies e spam □

Comportamentos nas redes sociais

1. Redes sociais utilizadas: Badoo □ Facebook □ Instagram □ Tinder □ Tik Tok □ Twitter □ WhatsApp □ Youtube □ Nenhuma □ Outra □_____

2. Média de tempo gasto por dia:

Menos de 1h □

Entre 1h e 1h30 □

Entre 1h30 e 2h □

Entre 2h e 2h30 □

Entre 2h30 e 3h □

Mais de 3h □

3. Motivos de utilização:

Comunicar com os amigos □

Comunicar com a família □

Comunicar com desconhecidos □

Marcar encontros com amigos □

Marcar encontros com desconhecidos □

Publicar fotografias e vídeos □

Partilhar fotografias e vídeos íntimos □

Partilhar informações privadas □

Partilhar informações bancárias □

Revelar informações como nome completo, idade, morada e número de telemóvel □

Realizar pesquisas □

Participar em petições/questionários □

Entretenimento □

Ver vídeos ou filmes □

Fazer compras online □

3. Medidas de privacidade (assinale apenas se a resposta for "SIM"):

Os meus perfis nas redes sociais são privados □

Só pessoas autorizadas podem ver a minha informação, fotografias, vídeos e comentários nas redes socais □

Apenas pessoas autorizadas me podem contactar nas redes sociais □

Tenho informações como a minha morada, número de telemóvel e e-mail disponíveis nas redes sociais □

4. Medidas de segurança (assinale apenas se a resposta for "SIM"):

Tenho um antivírus instalado no telemóvel, computador ou tablet □

Atualizo com frequência o antivírus do meu telemóvel, computador ou tablet □

Termino sempre a sessão das minhas redes sociais no meu telemóvel, computador ou tablet □

Partilho as minhas credenciais de acesso com amigos ou familiares □

Partilho as minhas credências de acesso com desconhecidos □

Tenho as minhas credências de acesso escritas em papel ou noutro lugar □

Parte 3

1. No período de 1 ano até à realização deste questionário assinale os cibercrimes dos quais foi vítima (pode assinalar mais do que uma opção):

Criação de perfis falsos nas redes sociais □

Acesso ilegítimo às minhas redes sociais □

Assédio nas redes sociais □

Partilha e divulgação ilegítima de material fotográfico e videográfico nas redes sociais □

*Sextortion* □

C*yberstalking* □

*Cyberbullying* □

Fraude ou burla *online* □

*Hacking* □

*Phishing* □

*Pharming* □

*Doxing* □

*Nenhum* □

Chegou ao fim do questionário, obrigada pela sua colabiração!