José Pedro Silva Granja

Avaliação do Conhecimento e Perceção sobre Cibercrime por Jovens Estudantes Universitários

Universidade Fernando Pessoa

Faculdade de Ciências Humanas e Sociais

Porto, 2022

José Pedro Silva Granja

Avaliação do Conhecimento e Perceção sobre Cibercrime por Jovens Estudantes Universitários

Universidade Fernando Pessoa

Faculdade de Ciências Humanas e Sociais

Porto, 2022

José Pedro Silva Granja

Avaliação do Conhecimento e Perceção sobre Cibercrime por Jovens Estudantes Universitários

O aluno

_____

(José Pedro Silva Granja)

Trabalho apresentado à Universidade Fernando Pessoa, como parte dos requisitos para obtenção do Grau de Licenciado em Criminologia, sob a orientação da Professora Laura M. Nunes.

Resumo

O cibercrime é um problema cada vez mais enraizado na sociedade e em constante desenvolvimento. A galopante evolução tecnológica a partir do final do século XX fez florescer um novo leque de crimes informáticos que apresentam como alvo o estado, a população e especialmente o grupo que melhor acompanha o desenvolvimento das novas tecnologias de informação e comunicação, os jovens.

Desta forma, o principal objetivo deste estudo consiste na avaliação do conhecimento e perceção sobre o cibercrime, pelos jovens estudantes universitários. Para tal, recorreu-se a uma revisão sistemática da literatura existente sobre o conhecimento, as perceções e os comportamentos levados a cabo pelos estudantes relativamente a crimes informáticos que permitiu a elaboração de uma proposta de inquérito por questionário a ser aplicado neste contexto, a sua posterior discussão e a exposição dos resultados esperados.

Palavras-Chave: Cibercrime; Estudantes universitários; Internet; Perceções e conhecimento.

Abstract

Cybercrime is a problem that is increasingly rooted in society and is constantly developing. The galloping technological evolution from the end of the 20th century has given rise to a new range of computer crimes that targets the state, a population and especially the group that best accompanies the development of new information and communication technologies, young people.

Thus, the main objective of this study is to assess the knowledge and perception of cybercrime by university students. To this end, use a systematic review of context knowledge, such as existing perceptions of context knowledge and behaviors carried out by students who consult an interpretation of a proposed inquiry through a survey to be applied to these crimes, their consultation to an interpretation of a proposed inquiry further discussion and presentation of the expected results.

Keywords: Cybercrime; University students; Internet; Perceptions and knowledge.

Agradecimentos

À Universidade Fernando Pessoa pela excelente formação que me proporcionou ao longo destes três anos em especial aos docentes do curso de criminologia por tudo que me transmitiram.

À Professora Doutora Laura Nunes, pelo apoio e pela disponibilidade para esclarecer as dúvidas que iriam aparecendo e as sugestões para melhorar o meu trabalho, que já havia demonstrado no Relatório de Estágio e voltou a assessorar também ao longo deste projeto.

Aos meus pais que me ajudaram em todos os momentos e etapas da minha vida, por isso mesmo devo a eles o homem que sou hoje.

À minha namorada pelo apoio incondicional em todos os momentos.

Índice

Índice de Abreviaturas, acrónimos e siglas

APAV - Associação Portuguesa de Apoio à Vítima

CP - Código Penal

TIC - Tecnologias de Informação e Comunicação

UE - União Europeia

UNESCO - United Nations Educational, Scientific and Cultural Organization

UNODC - United Nations Office on Drugs and Crime

Índice de Anexos

Introdução

O final do século XX, marcou o início da era digital que se caracteriza pelos avanços na área da informática e da tecnologia. Esta evolução operada nas novas tecnologias, culminou no surgimento da Internet que constitui um dos instrumentos mais poderosos na sociedade dado a sua capacidade de distribuir a informação alterando, hoje, a noção de tempo e espaço (Figueiredo, 2014). Enquanto meio de comunicação de partilha de informação, esta ocupa nas nossas vidas um papel cada vez mais central e de maior destaque (Silva, 2016). Todavia, o seu surgimento não trouxe só vantagens uma vez que se projetou também sobre o fenómeno criminal. As práticas e capacidades da informática potenciam exponencialmente a internacionalização da criminalidade, como refere Venâncio (2011).

O Cibercrime, é um fenómeno cada vez mais presente nas sociedades modernas e que pode ser entendido como o conjunto de ofensas que são cometidas através de um computador e de tecnologia eletrónica digital (Yar, 2016). Segundo o Gabinete de Cibercrime (2022), as denúncias deste tipo de crime recebidas por correio eletrónico aumentam consistentemente, de ano para ano, desde 2016 sendo que se verificou um aumento excecional nos últimos dois anos.

Devido ao seu caráter evolutivo e adaptativo, este é um tipo de crime que têm vindo a suscitar uma maior preocupação nas autoridades, nos legisladores e na própria população. A APAV (2021) salienta a importância da consciencialização, do conhecimento e das competências de controlo face ao tipo e à dimensão de informação pessoal partilhada ou partilhável na internet, uma vez que pessoas com níveis mais elevados de controlo percebido face à informação partilhada/partilhável, compartilham de forma mais criteriosa, percecionam-se como mais seguras e apresentam menor probabilidade de serem vítimas de cibercrime.

Assim sendo, a ideia de analisar e avaliar a perceção e conhecimento de jovens estudantes sobre o cibercrime, é sustentada pela necessidade de prevenção da cibervitimação num contexto constituído maioritariamente por jovens, cuja utilização de tecnologias é frequente, estando assim à partida mais exposta a este tipo de vitimação. Posto isto, os objetivos deste projeto de investigação passam por : i) Apurar o nível de conhecimento da população estudantil universitária sobre cibercrime; ii) Capturar a perceção de

ocorrência de cibercrime entre os estudantes universitários; iii) Identificar eventuais indicadores da existência de padrões de cibercrime percecionado;

Como grande questão central da investigação, indaga-se se haverá padrões de cibercrime percebidos como ocorrentes entre a população inquirida.

O presente trabalho é constituído por duas partes fundamentais: Na primeira será feita uma abordagem teórica ao cibercrime, onde se procurará definir este e outros conceitos que lhe estejam associados e abordar algumas tipologias e classificações existentes. Será realizado também um enquadramento legal. Abordar-se-á ainda a vulnerabilidade dos estudantes universitários para este fenómeno, seguido de uma exposição de estudos nacionais e internacionais realizados neste âmbito. Na segunda parte, dedicada à parte empírica, será apresentado o projeto de investigação desenvolvido pelo aluno seguido da enumeração dos métodos, objetivos e procedimentos utilizados para tal, assim como dos resultados que se esperam alcançar.

Parte I.

Enquadramento Teórico

Nesta parte do trabalho apresentar-se-ão algumas definições para cibercrime bem como tipologias, classificações e instrumentos legislativos existentes. Posteriormente, abordar-se-á também a vulnerabilidade apresentada por estudantes universitários para este fenómeno, seguida de uma exposição de estudos nacionais e internacionais realizados neste âmbito.

1.1. Cibercrime: Conceitos Básicos

Segundo Guedes (2021), nos últimos 30 anos têm-se verificado um incontestável crescimento do uso da Internet, de modo que muitas atividades rotineiras do quotidiano foram transferidas para o ciberespaço. Este termo, é entendido por Fernandes (2012) como uma rede de interligações que envolvem infraestruturas tecnológicas, telecomunicações ligadas em rede e sistemas de processamento.

É, desta forma, por volta do final do séc. XX que o fenómeno do cibercrime surge, ainda que nesta altura apenas praticado por pessoas altamente especializadas, conhecidas como "piratas informáticos" e hackers (Vegar, 2010 *cit. in* Vidigal, 2012). No entanto, à medida que a tecnologia evolui, o número de utilizadores aumenta, de maneira que hoje em dia "qualquer" cidadão, mesmo sem vastos conhecimentos informáticos, possa cometer um cibercrime (Vidigal, 2012). É também natural que com a evolução tecnológica surjam novos tipos de cibercrime e novos métodos, o que coloca este tipo de crime em constante evolução e adaptação (Jaishankar, 2011), tornando-o deste modo mais difícil de se conceptualizar.

As novas tecnologias vierem desta forma, proporcionar não só o surgimento de novas formas de criminalidade como ainda também vieram facilitar a prática de crimes já conhecidos, o que vai ao encontro do que salienta Venâncio (2011) "as especificidades da criminalidade informática colocam-se, não só na transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes com elementos caracterizadores de natura digital".

A criminalidade informática, também designada como cibercrime, crime digital, "high techonology crimes" ou "computer related crimes" (Simas, 2014) constitui um tipo de ação criminosa que por si só não é passível de uma única definição. A maioria dos autores

e instituições, que procuram conceptualizar este fenómeno partilham a ideia de que os cibercrimes abrangem todos os atos ilegais, cometidos com recurso a tecnologia sem se referirem a um único tipo de comportamento criminoso.

Exemplo disto é a UNODC (United Nations Office on Drugs and Crime), que considera mais adequado incluir no conceito de cibercrime, não tanto um tipo de atos, mas antes um conjunto de atos ou condutas, que podem ser organizados em categorias com base no objeto do crime ou no modus operandi.

Analogamente, diversos autores tais como Antunes e Rodrigues (2018), descrevem o cibercrime como qualquer crime que ocorre no ciberespaço, incluindo-se no leque de crimes as ações praticadas com recurso à internet, onde se envolvem também os crimes informáticos, aqueles praticados contra os sistemas informáticos, os dados e as informações alojados nos sistemas de informações.

Holt e Bossler (2009) *cit. in* Guedes (2021), propõem de igual forma, uma definição genérica, mas abrangente, de cibercrime, classificando-o como contemplando todos os crimes cometidos com recurso a tecnologia, assim como Yar (2016) que defende que o cibercrime não se refere a um único tipo de comportamento criminoso, mas que em vez disso, abrange uma gama muito ampla de crimes, que compartilham uma importante característica definidora – são cometidos usando tecnologias eletrônicas digitais, como a Internet, redes sociais, e-mail e mensagens.

Também a Comissão Europeia (2007), define como cibercrime "os atos criminosos praticados com recurso a redes de comunicações eletrónicas e sistemas de informação ou contra este tipo de redes e sistemas", não limitando a sua definição a um tipo específico de comportamento criminoso. Assim como a APAV (2021), no Manual ROAR disponibilizado pela instituição que conceptualiza cibercrime como todos os crimes que usam computadores ou outros dispositivos análogos, incluindo redes e outros meios de acesso, referindo-se, portanto, a todo o tipo de ataques contra a disponibilidade, integridade e confidencialidade de sistemas informáticos, sistemas de informação e recursos que os suportam.

1.1.1. Cibercrime: Tipologias e Classificações

Como constatado no ponto anterior, embora se verifiquem semelhanças nas definições apresentadas pelos diversos autores e instituições, é fundamental que haja uma distinção entre os diversos atos criminais praticados, dependendo do alvo ou objeto da ofensa, como faz Furnell (2002) que distingue as ofensas "focadas no computador" que incluem crimes que têm como alvo a infraestrutura eletrónica, ou seja, que abrangem e atingem a própria internet e que sem a existência desta última, a ofensa não poderia ser realizada, das ofensas "assistidas pelo computador", que se refere às ofensas cuja existência é independente da internet, mas que desta forma, encontraram uma nova vida online.

Marques e Martins (2006), analogamente procuraram também tipificar o cibercrime segundo duas categorias, uma primeira em que o computador serve de meio para atingir um objetivo criminoso e uma segunda em que o computador é o alvo simbólico desse ato, passando assim o computador a ser o objeto do crime. Venâncio (2011) distingue de igual modo, dois tipos de cibercrime, aqueles em que " a informática é apenas um meio para a prática do crime e outros em que a informática aparece como um elemento do tipo legal criminalmente punido".

A Comissão Europeia, em 2007, subdividiu também o cibercrime, não segundo duas, mas segundo três categorias: a primeira referente às formas tradicionais de crimes que utilizam agora a internet para a prática de ofensas; uma segunda referente à publicação de conteúdos ilícitos na internet; e uma terceira relativa a crimes exclusivos de redes eletrónicas.

Esta tipificação é fundamental quer para perceber e distinguir quais os crimes que se enquadram nas novas formas de ofensa, sem qualquer semelhança aos crimes praticados no ambiente *offline*, dos crimes já praticados anteriormente, mas, agora com o recurso à tecnologia (Clough, 2010 *cit. in* Martins, 2018).

Holt e Bossler (2016), propuseram uma taxonomia de cibercrimes mais específica, baseada na proposta de Wall (2001), sendo esta constituída por 4 categorias:

i) Ciberinvasão – consiste na invasão de propriedade privada online e incluí crimes como o Hacking ou Cracking e o Malware.

O Hacking ou Cracking podem ser definidos como o acesso não autorizado a sistemas informáticos com intenção criminosa (Maimon & Louderback, 2019 *cit. in* APAV, 2021). Esta atividade poderá incluir a identificação e reconhecimento de sistemas de hardware ou software vulneráveis; a infiltração nos alvos vulneráveis; alterações e redesenho dos sistemas alvo do ataque, incluindo a inserção de vírus e malware que permita acesso privilegiado a informação e dados como dados pessoais, passwords/credenciais de acesso e informação financeira/contas ou mesmo o controlo do próprio sistema; (APAV, 2021).

O Malware, é segundo a APAV (2021) o termo utilizado para se referir a uma variedade de softwares de caráter hostil ou intrusivo, que têm como objetivo causar danos, alterações ou furtar informações em equipamentos.

ii) Ciberfraude – compreende todos os atos de partilha e obtenção ilegal de informações ou materiais online. Exemplos desta prática são as Burlas, o Spam, o Phishing e o Furto de Identidade Online.

Entende-se por Burla, quem visando o enriquecimento próprio ou de terceiro, induzir, através do engano ou erro, outra pessoa a praticar atos que lhe causem ou a outra pessoa prejuízo patrimonial (APAV, 2015). Dentro deste tipo de crime, existem: i) burlas no comércio eletrónico; ii) burlas em leilões na internet; iii) burlas com cartão de crédito; iv) burlas nos relacionamentos íntimos (APAV, 2021).

O Spam, corresponde ao envio de dados e à distribuição massiva de e-mails que anunciam produtos, serviços ou esquemas de investimento, que podem ter um carácter fraudulento e inclusivamente conter malware ou outro anexo de arquivo executável (APAV, 2021). O objetivo deste crime é enganar ou convencer o/a destinatário/a relativamente ao anúncio de produtos, serviços ou esquemas atrativos (APAV, 2021).

Phishing, consiste numa tentativa fraudulenta de aceder a informação pessoal ou financeira, muitas das vezes associada à técnica de Spam. A vítima pode ser abordada por e-mail, chamada telefónica ou mensagem através de uma comunicação aparentemente credível e que remete a fontes oficiais como bancos, onde o atacante lhe solicita dados como password, número do cartão ou códigos de acesso (Dias, 2021).

Furto de identidade online, corresponde à apropriação e uso não consentido dos seus dados pessoais ou financeiros para fins criminosos (Martins, 2021).

iii) Ciberpornografia – corresponde à utilização ilegal de conteúdos pornográficos, incluindo a partilha não autorizada de nudez, revenge porn, grooming, entre outras.

Segundo Guedes (2021), Revenge Porn caracteriza-se pela divulgação pública de nudez do ex-parceiro como forma de vingança após uma separação amorosa.

Já o Grooming Online pode ser definido como um processo de manipulação e uma forma de aliciamento de crianças para que se estabeleça uma relação de confiança com estas, convencendo-as a encontrarem-se pessoalmente com o ofensor, de forma a consumar o abuso sexual (APAV, 2021).

iv) Ciberviolência – corresponde a uma categoria mais abrangente onde estão incluídas todas as situações suscetíveis de causar trauma físico, emocional ou mesmo morte. Alguns exemplos são o cyberbullying, o cyberstalking, os discursos de ódio e a divulgação de material danoso ou perigoso.

Entende-se por Cyberbullying a intenção de agredir verbalmente uma vítima e/ou contribuir para a sua exclusão e isolamento social, por meio da utilização das novas tecnologias de informação e comunicação. O ofensor pode utilizar técnicas como a disseminação de informação falsa com a intenção de difamar a vítima (APAV, 2021).

O Cyberstalking caracteriza-se por um conjunto de condutas persistentes e não desejadas, através do qual um indivíduo, grupo de indivíduos ou organização recorre às TIC com o objetivo de assediar, intimidar ou ameaçar um indivíduo, grupo de indivíduos ou organização (Sani *et alii*, 2018).

Os discursos de ódio, constituem formas de comunicação e expressão que promovem, disseminam, incitam ou justificam o ódio racial, a xenofobia, o antissemitismo e outras formas de ódio baseado na intolerância contra uma pessoa ou grupo de pessoas (APAV, 2021).

1.1.2. Enquadramento Legal

Em 23 de Novembro de 2001, face ao exponencial aumento dos números relativos à criminalidade informática e devido à crescente preocupação por parte dos legisladores, Portugal assinou em Budapeste a Convenção sobre o Cibercrime criada pelo Conselho da Europa.

Esta foi criada com os objetivos e a convicção de que seria necessária "para impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adoção de poderes suficientes para combater eficazmente essas infrações, facilitando a deteção, a investigação e o procedimento criminal relativamente às referidas infrações, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável" (Convenção sobre o Cibercrime, 2001).

Contudo, devido à ineficácia dos instrumentos legislativos disponíveis até à data para fazer face à evolução informática, surge em 2009 a Lei nº. 109/2009 de 15 de Setembro, conhecida como a Lei do Cibercrime, revogando desta forma a Lei nº 109/91, de 17 de Agosto, que vigorava anteriormente. Segundo o que se encontra previsto no artigo 1º da Lei do Cibercrime, esta veio estabelecer as disposições penais materiais e processuais, relativas à cooperação internacional em matéria penal, respeitante ao domínio do cibercrime e da recolha de prova em suporte eletrónico.

No seu capítulo II, a Lei do Cibercrime apresenta as disposições penais materiais onde se encontram tipificados os seguintes crimes informáticos:

i) Falsidade Informática - que consiste na ação de introduzir, modificar, apagar ou suprimir dados informáticos ou, por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, para que estes sejam considerados ou utilizados para finalidades juridicamente relevantes (Lei do Cibercrime Art.º 3, 2009).
ii) Dano Relativo a programas ou outros dados informáticos - caracterizando-se pela ação de apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados

informáticos alheios sem permissão legal ou sem estar autorizado pelo proprietário (Lei do Cibercrime Art.º 4, 2009).

iii) Sabotagem Informática - que consiste em entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, sem permissão legal ou sem estar autorizado pelo proprietário (Lei do Cibercrime Art.º 5, 2009).

iv) Acesso Ilegítimo - que se caracteriza por aceder a um sistema informático, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele (Lei do Cibercrime Art.º 6, 2009).

v) Interceção Ilegítima - que consiste em intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinados ou dele provenientes, através de meios técnicos, sem permissão legal ou sem para tanto estar autorizado pelo proprietário (Lei do Cibercrime Art.º 7, 2009).

vi) Reprodução Ilegítima de Programa Protegido - que se caracteriza pela reprodução, divulgação ou comunicação ao público de um programa informático protegido por lei, de forma ilegítima (Lei do Cibercrime, Art.º 8, 2009).

Porém, como é expectável, a previsão legal de crimes informáticos no ordenamento jurídico português não se cinge apenas aos crimes previstos na Lei do Cibercrime. No Código Penal Português são apresentadas outras condutas que constituem, de igual modo, uma prática criminal deste fenómeno.

No artigo 192.º do CP, encontra-se previsto o crime de devassa da vida privada, que consiste em 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. Incluindo neste ainda a fotografia ou filmagem da vida privada, a observação, escuta ou divulgação de factos íntimos.

No artigo 193.º do CP, encontra-se previsto o crime de devassa por meio de informática, que se traduz em criar, manter ou utilizar ficheiros com dados que identifiquem a origem étnica da vítima, e que refiram as suas convicções políticas, filosóficas e religiosas.

No artigo 194.º do CP, encontra-se previsto o crime de violação de correspondência ou de telecomunicações, que corresponde à abertura de uma encomenda, carta ou outro documento escrito, tomando conhecimento ou divulgando o seu conteúdo, sem a permissão do proprietário.

No artigo 199.º do CP, encontra-se previsto o crime de gravação de fotografias ilícitas, que se traduz em fotografar e filmar uma pessoa, assim como 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.

Por fim, no artigo 221.º do CP, encontra-se previsto o crime de burla informática e nas comunicações, que equivale em intervir, interferir ou utilizar de forma incorreta o tratamento de dados, sem a devida autorização, por forma a obter lucros.

1.2. Cibercrime no Contexto Universitário

1.2.1. Vulnerabilidades dos Estudantes Universitários para o Cibercrime

A entrada no Ensino Superior ocorre por norma numa fase que corresponde à passagem da adolescência para a idade adulta. Nesta, ocorrem mudanças que se traduzem no desenvolvimento, realização e consolidação da identidade pessoal e social do sujeito, que mais tarde culminarão na aquisição do estatuto social de adulto (Andrade, 2006).

Nesta altura de mudança, a internet e as redes sociais são para os jovens, uma maneira de reclamarem espaço privado, que muitas das vezes não o conseguem em qualquer outro lugar, procurando assim conquistar liberdade e autonomia (Vilela, 2019). De acordo com a UNESCO (2005), o grupo mais ativo no ciberespaço, são atualmente os jovens. Estes "contribuem para a atualização de potencial de ferramentas digitais e para a emergência de novas práticas que constituem uma verdadeira cultura digital".

As redes sociais constituem um novo mundo de oportunidades para os jovens, com todas as potencialidades que lhes estão associadas. Exemplo disso são o Facebook, Messenger

e WhatsApp que oferecem uma forma de entretenimento e comunicação especialmente para estudantes universitários (Costa, 2020).

No entanto, a utilização da Internet não é imune a perigos e desfrutar das vantagens da sua utilização, leva também os jovens a conviver com os riscos a ela inerentes. A Comissão Europeia (2012) *cit. in* Vilela (2019) assume que os principais riscos associados à utilização das redes sociais são a violação de privacidade, exposição a conteúdo ofensivo, Ciberbullying, Grooming e Ciberstalking.

Segundo estudos referidos pela APAV (2021) têm-se vindo a verificar um aumento da vitimação por cibercrime, especialmente quando se fala em hacking, malware e phishing, por pessoas com mais hábitos de utilização das redes sociais e das TIC nas suas atividades diárias. A mesma entidade atribui, desta forma, à população mais jovem maior risco de cibervitimação, uma vez que em comparação com os utilizadores mais velhos são aqueles que apresentam índices mais elevados de utilização intensiva das TIC e da Internet.

Este risco, de acordo com Boyd (2008) e com a APAV (2021), deve-se na maioria das vezes ao desconhecimento dos riscos associados a atividades online menos seguras como a disponibilização de dados pessoais que facilitem a invasão da privacidade e que permitam outras pessoas utilizarem a sua identidade, o download de programas de freeware e de músicas, vídeos, filmes e/ou jogos em plataformas não oficiais, a utilização de websites de compartilhamento de arquivos, a aceitação de pedidos de amizade nas redes sociais provenientes de pessoas/perfis desconhecidos entre outros.

Assim, indo ao encontro do objetivo deste projeto de investigação, mostra-se de extrema relevância avaliar o conhecimento e perceção do cibercrime por jovens universitários de forma a prevenir a vitimação, uma vez que estes são considerados os utilizadores mais ativos do ciberespaço e que, portanto, mais expostos estarão a este tipo de criminalidade.

1.2.2. Estudos de Vítimas e Ofensores de Cibercrime em Contexto Universitário Nacional e Internacional

Atualmente, estima-se que cerca de 1 milhão de pessoas em todo o mundo sejam vítimas de cibercriminalidade por dia. Só em 2021, o Gabinete de Cibercrime revela ter recebido em Portugal cerca de 1160 denúncias deste tipo de criminalidade, 516 mais do que no ano anterior.

Em razão disso, o Eurobarómetro desenvolvido pela Comissão Europeia com o objetivo de compreender as experiências e perceções dos cidadãos da UE sobre questões de cibersegurança, criou em 2015 um inquérito que abrangeu mais de 27 000 pessoas em todos os Estados-Membros da UE, onde os inquiridos/as expressaram de igual forma elevados níveis de preocupação com a cibersegurança e com os riscos de cibercrime (APAV, 2021). Mais especificamente, 85% dos/as inquiridos/as referiu concordar com o facto de o risco de cibervitimação estar a aumentar e 73% dos/as inquiridos/as referiu recear que as suas informações pessoais online não sejam mantidas em segurança. Destacou-se além disso a preocupação demostrada por cada inquirido face a diferentes tipos de cibercrime, onde furto de identidade online (68%) se evidenciou.

No que concerne a Portugal, um estudo da Fundação PHC, que se dedica a melhorar a qualidade de vida dos cidadãos, revela que cerca de oito em cada dez portugueses estão preocupados com a criminalidade online e que quase 90% estão preocupados com a segurança dos dados que circulam na internet, sendo que quanto mais jovens maior é a preocupação (Pequenino, 2022). Genericamente, os resultados revelaram que, embora a percentagem de portugueses vitimados por cibercrime estivesse abaixo da média europeia, a preocupação dos cidadãos nacionais em relação a este fenómeno é similar à dos restantes cidadãos europeus (Guedes, 2021).

Apesar de alguns estudos identificarem a experiência de vitimação anterior como um dos fatores que incrementa o risco percebido da população face a este fenómeno, tal não se revela suficiente para explicar os elevados níveis de risco percebido e de preocupação demonstrados nos estudos acima mencionados (Guedes, 2021). Assim sendo, têm vindo a ser apontados outros fatores explicativos, tais como, a ampla cobertura dada pelos media a este tema e a forma como o trata, a vitimação de pessoas próximas e a superficialidade (Bidgoli *et alii*, 2016).

Um estudo realizado por Bidgoli *et alii* (2016) nos Estados Unidos, procurou entender como o cibercrime afeta os estudantes universitários, grupo que este têm como vulnerável devido ao uso extensivo da tecnologia. Outro objetivo deste mesmo estudo foi analisar o conhecimento, as perceções e os comportamentos levados a cabo pelo estudantes em relação aos crimes informáticos. A investigação adotou uma abordagem de métodos mistos, utilizando inicialmente entrevistas semiestruturadas com 10 participantes de

forma a avaliar qualitativamente o tema, sendo de seguida realizada uma pesquisa online com 222 participantes de forma a confirmar resultados.

Após a realização do estudo, foi possível identificar quantos estudantes já foram vítimas de cibercrime, assim como as formas mais recorrentes. Para além disso, os autores chegaram à conclusão de que a maioria dos estudantes adquirem os seus conhecimentos sobre cibercrime predominantemente por meio de pessoas que conhecem pessoalmente e que foram vitimadas por este tipo de crime ou pelos media. Desta forma, concluiu-se que a autoeficácia e o medo, influenciam a tendência dos estudantes a tomar medidas preventivas para evitar comportamentos facilitadores e denunciar crimes cibernéticos às entidades apropriadas.

Nakala e Diunagala (2020), semelhantemente, através do estudo por estes realizado identificaram alguns fatores de risco para a cibervitimação, especificamente direcionados a estudantes universitários. Para tal, averiguaram qual a sua literacia digital, compreensão de segurança online, estatuto socioeconómico e estilo de vida de forma a identificar possíveis fatores de risco para crimes como a criação de contas falsas, hacking, doxing, cyberstalking e fraude pela internet.

No final do estudo, concluiu-se que o pouco contacto com a família, a menor concentração nos estudos, o maior nível socioeconómico, a exposição elevada às redes sociais, simultaneamente com poucas medidas de segurança e privacidade e fraca compreensão informática, constituem fatores de risco para a cibervitimação.

No mesmo âmbito, o estudo realizado por Neazkor *et alii* (2020) procurou avaliar o padrão de conscientização pública sobre o crime cibernético na Nigéria. Para esse propósito, recorreram a questionários e entrevistas realizadas a 1031 funcionários e estudantes de universidades. Os resultados demonstraram que uma fraca consciência do cibercrime, parece estar associada a experiências de vitimação, uma vez que os sujeitos passam a não estar alerta dos perigos das redes sociais, e por consequente, não adotam comportamentos seguros ao utilizar a internet.

Como se têm vindo a constatar, os jovens apresentam uma maior suscetibilidade a experienciarem a cibervitimação. Todavia, diversos estudos têm vindo a demonstrar que a perceção dos jovens relativamente à vitimação por cibercrime não é congruente com esta evidência, uma vez que na maioria das vezes estes vêm outros como mais vulneráveis

a este tipo de crime e percecionam de forma menor os riscos associados à utilização do ciberespaço (Guedes, 2021). Como exemplo do acima referido, o estudo de Conway e Hadlington (2018), na Inglaterra permitiu constatar que na conceção dos jovens, os mais velhos são mais suscetíveis à cibervitimação, não apresentando consciência de que apresentam um risco de vitimação online maior (Guedes, 2021).

As perceções de cibercriminalidade, ou seja, as perceções que os indivíduos têm em relação à criminalidade informática, assumem deste modo um papel fundamental no estudo da cibercriminalidade e cibersegurança, o que justifica a investigação realizada de seguida.

Parte II.

Contribuição Empírica

Nesta parte do trabalho serão apresentados os aspetos relacionados com a investigação a que o aluno se propõe realizar, nomeadamente, o método, os objetivos, o procedimento e os resultados que se esperam alcançar com base na revisão de literatura efetuada. Por fim, apresentar-se-á uma conclusão deste trabalho.

2.1. Método

O estudo que se propõe realizar desenvolver-se-á mediante a utilização de um inquérito por questionário que seguirá um desenho exploratório, observacional, descritivo e transversal. Este deverá ser antecedido por uma primeira parte referente à obtenção de consentimento, explicação dos objetivos de investigação e recolha dos dados sociodemográficos que possibilitarão a caraterização da amostra. Dentro do método, recordaremos os objetivos e a grande questão central da investigação.

Uma vez apresentadas as linhas gerais do método, passam a apresentar-se os objetivos deste trabalho.

2.1.2. Objetivos e Questões de Investigação

Como já referido, a presente investigação têm como objetivo geral apurar o nível de conhecimento da população estudantil universitária sobre o fenómeno do cibercrime, capturando ainda a sua perceção da ocorrência desta forma de criminalidade para que se identifiquem eventuais indicadores da existência de padrões de cibercrime percecionado. Para tal, recolher-se-ão dados tais como o sexo, idade, nível socioeconómico, conhecimento informático, consciência sobre o cibercrime e experiências anteriores de vitimação.

Assim sendo, coloca-se a seguinte questão de investigação: “Existirão padrões de cibercrime percebidos como ocorrentes entre a população inquirida?”.

Para que se desenvolva este trabalho de investigação de maneira adequada, apresentar-se-á de seguido o material e o procedimento utilizado.

2.1.3. Material e Procedimento

Primeiramente, antes de qualquer tipo de recolha de dados, deverá começar-se por obter autorização formal, junto de instituições de ensino superior, para que se recolham os dados necessários dos respetivos alunos. Assim, nesse sentido deverá ser elaborada uma carta ou e-mail, onde se anexar-se-á o protocolo de investigação, ou seja, o respetivo projeto. Após a obtenção formalizada dessa autorização é que se passará à recolha de dados por administração do questionário.

No entanto, para que se recolha a informação necessária junto de cada um dos inquiridos, é fundamental de acordo com os princípios éticos e deontológicos que se proceda preliminarmente i) à obtenção do consentimento informado dos participantes sendo apresentada se for o caso uma declaração de consentimento informado (Anexo A), ii) à garantia de anonimato e confidencialidade e ainda iii) à explicação dos objetivos de investigação.

O questionário será elaborado tendo por base as estatísticas de prevalência do cibercrime na população portuguesa e revisão da literatura. Após a revisão da literatura e considerando a informação obtida, o questionário deverá ser divido em 3 partes: a primeira destinada à caracterização sociodemográfica da amostra onde constarão questões relativas ao sexo, idade, ano curricular que se encontra a frequentar, estado civil, quantos elementos compõe o seu agregado familiar e o seu estatuto socioeconómico; a segunda parte destinada à literacia digital e utilização da internet, onde se procurarão recolher dados acerca da frequência com que os jovens estudantes a utilizam, o propósito da sua utilização, as redes sociais manuseadas, medidas de segurança e de privacidade utilizadas e a sua literacia digital; por fim uma terceira parte destinada à análise da perceção e conhecimento do cibercrime propriamente dita, onde serão aplicadas questões que procurarão avaliar a consciência do cibercrime, experiências anteriores de vitimação por cibercrime e nestes casos recolher dados acerca dos tipos mais recorrentes, exposição através de outros ou dos media, autocontrolo e intenção de denunciar.

Posteriormente, os dados recolhidos serão organizados e registados numa base de dados, a partir da qual, mediante tratamento estatístico, estes serão convertidos em resultados que me permitirão extrair conclusões interpretáveis.

2.2. Resultados Esperados

Neste último ponto espera-se que sejam apresentados os resultados, no entanto, como este se trata de um projeto de graduação, a investigação não se chegou a concretizar o que impede a apresentação de resultados reais sendo desta forma apresentados de seguida no quadro 1 alguns dos resultados esperados com base na revisão de literatura.

Quadro 1

Apresentação dos resultados obtidos nos estudos consultados vs resultados esperados com a investigação

Resultados dos Estudos Consultados	Resultados Esperados
Bidgoli *et alii* (2016) - A exposição ao cibercrime por outros, pelos media e o autocontrolo influenciam as perceções dos estudantes do fenómeno do cibercrime.	Espera-se encontrar uma relação positiva entre a exposição ao cibercrime e a perceção dos estudantes acerca deste fenómeno uma vez que o risco percebido da população face a um determinado problema aumenta quando existe uma maior exposição.
Nalaka e Diunagala (2020) - Cyberstalking foi o crime mais experienciado por estudantes.	No contexto português, considera-se que este não será o tipo de crime mais recorrente, uma vez que segundo as estatísticas nacionais a tipologia mais frequentemente denunciada é o phishing.
Costa (2020) - As vítimas mais frequentes de cibercrime revelam uma literacia digital mais reduzida**.**	Espera-se que os resultados sejam idênticos, uma vez que é referido pela APAV (2015) que quanto menos informado um sujeito está, mais riscos ele corre online.
Bidgoli *et alii* (2016) - As perceções de medo e autoeficácia influenciam os comportamentos dos estudantes em termos de medidas preventivas e comportamentos facilitadores.	Acredita-se que se obtenham resultados semelhantes uma vez que uma pessoa que se percecione em risco de cibervitimação adotará, com maior probabilidade, comportamentos orientados para a sua cibersegurança, o que contribuirá para a redução do risco.
Nzeakor *et alii* (2020) - o sexo masculino apresenta uma maior consciência do cibercrime comparativamente ao sexo feminino, logo estes apresentarão por norma menor risco de vitimação.	Considera-se que a associação entre o sexo feminino e o risco de vitimação feita por este autor não deve ser linear isto porque apesar de alguns estudos apontarem para uma maior probabilidade dos sujeitos de sexo feminino serem vítimas de cibercrime, outros como é o caso do estudo de Costa (2020) revela o oposto. Desta forma, não se possui nenhuma certeza em relação ao sexo que apresentará um maior risco de vitimação.

Considerações Finais

A realização deste estudo, possibilitou aprofundar aquilo que constitui uma das principais ameaças da atualidade, os crimes informáticos. Este tipo de criminalidade que se reflete em características como a atemporalidade, a transnacionalidade, a deslocalização e sobretudo o anonimato na sua prática (Dias, 2012) constitui um fenómeno cada vez mais recorrente e em crescente desenvolvimento, muito devido à dificuldade notada de o definir e especialmente de o prevenir.

Ao longo da revisão de literatura que se efetuou foi possível notar que as perceções e as atitudes dos cidadãos moldam, muitas das vezes, o seu comportamento (Yar, 2010). Daí surge a necessidade de existirem estudos, programas de prevenção e intervenção que tenham em conta essas perceções e atitudes relativamente ao cibercrime para que se mudem comportamentos e atitudes no ciberespaço.

Neste sentido e citando Holt (2016) à criminologia, bem como aos profissionais desta área interessam não só os "crimes velhos" como também os "crimes velhos" praticados com "novos instrumentos" cabendo-lhes assim a sua deteção e prevenção através da elaboração de estudos relacionados com esta problemática.

Relativamente aos objetivos propostos, pensa-se que estes serão alcançáveis, uma vez que, tendo por base estudos já realizados com objetivos idênticos e os resultados por estes alcançados, crê-se que a partir do inquérito por questionário proposto se alcancem resultados idênticos. No entanto, devido à versatilidade e heterogeneidade deste fenómeno pensa-se que poderão existir algumas limitações tais como a utilização de um único instrumento de recolha de dados que poderá se relevar ineficaz devido à natureza diferente de cada tipo de cibercrime.

Concluindo e respondendo à questão central desta investigação, acredita-se que em futuros estudos centrados nesta temáticas se encontrem padrões de cibercrime percebidos como ocorrentes entre a população inquirida, nomeadamente uma elevada exposição diária à Internet e Redes Sociais, a prevalência de um dos sexos, uma débil literacia digital entre outros padrões que se irão descobrir com a realização da investigação.

Referências

Abdulai, M. (2020). Examining the Effect of Victimization Experience on Fear of Cybercrime: University Student's Experience of Credit/Debit Card Fraud. *International Journal of Cyber Criminology*, 14, pp. 157-174.

Amador, N. (2012). Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro. [Em linha]. Disponível em <https://comum.rcaap.pt/handle/10400.26/17168>. [Consultado em 19/06/2022].

Andrade, M. (2006). Antecipação da conciliação dos papéis familiares e profissionais na transição para a idade adulta: estudo diferencial e intergeracional. [Em linha]. Disponível em < https://repositorio-aberto.up.pt/handle/10216/41636>. [Consultado em 03/07/2022].

Antunes, M. e Rodrigues, B. (2018). *Introdução à cibersegurança: A internet, os aspetos legais e a análise digital forense*. Lisboa, FCA - Editora de Informática.

APAV (2015). Folha Informativa Burla. [Em linha]. Disponível em < https://apav.pt/apav_v3/images/folhas_informativas/fi_burla.pdf>. [Consultado em 09/07/2022].

APAV (2021). Manual ROAR - Da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas. [Em linha]. Disponível em < https://apav.pt/publiproj/images/publicacoes/ManualProcedimentosROAR-PT.pdf>. [Consultado em 3/06/2022].

Assembleia da República (2009). Lei n.º 109/2009 de 15 de setembro: Lei do Cibercrime, *Diário da República*, 1.ª série, n.º 179.

Bidgoli, M., Knijnenburg, B. e Grossklags, J. (2016). When Cybercrimes Strike Undergraduates. Paper presented at the 2016 APWG Symposium on Electronic Crime Research (eCrime).

Boyd, D. e Ellison, N. (2008). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13, pp. 210-230.

Carvalho, C. (2011). Ciberstalking: Prevalência na população universitária da Universidade do Minho. [Em linha]. Disponível em < http://repositorium.sdum.uminho.pt/handle/1822/18638>. [Consultado em 16/06/2022].

Código Penal (2020). 9.ª edição. Porto, Porto Editora.

Conselho da Europa (2001). Convenção sobre o Cibercrime. Budapeste, 23 de Novembro de 2001. Disponível em < https://rm.coe.int/16802fa428>. [Consultado em 24/06/2022].

Costa, A. (2020). Cibercrime: Um estudo exploratório da população universitária da Universidade do Porto. [Em linha]. Disponível em < https://repositorio-aberto.up.pt/bitstream/10216/132474/2/446100.pdf>. [Consultado em 04/06/2022].

Dias, P. (2021). Prevenir um ataque de phishing: A importância da formação dos Colaboradores. [Em linha]. Disponível em < https://comum.rcaap.pt/bitstream/10400.26/39283/1/99991939_Paulo_Dias.pdf>. [Consultado em 19/06/2022].

Dias, V. (2012). A problemática da investigação do cibercrime. *Data Venia - Revista Jurídica Digital*, 1(1), pp. 64-71.

Fernandes, J. (2012). Utopia, Liberdade e Soberania no Ciberespaço. *Nação e Defesa*, 1(133), pp. 11-31.

Figueiredo, H. (2014). Cibercrime. *Revista Jurídica UNIGRAN*, 16(32), pp. 90-95.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. London, Addison-Wesley.

Gabinete Cibercrime (2022). Nota Informativa, Cibercrime: Denúncias Recebidas 2021. [Em linha]. Disponível em < https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias-de-cibercrime-25-01-2022.pdf>. [Consultado em 15/06/2022].

Guedes, I. et alii (2021). *Cibercriminalidade Novos Desafios, Ofensas e Soluções.* Lisboa, Pactor.

Holt, T. (2016). Situating the problem of cybercrime in a multidisplinary context. *In:* Holt, T. (Ed.). Cybercrime through an interdisciplinary context. London and New York, Routledge.

Holt, T. e Bossler, A. (2016). *Cybercrime in Progress: Theory and prevention of technology-enabled offenses*. London and New York, Routledge.

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior.* New York, Routledge.

Marques, G. e Martins, L. (2006). *Direito da Informática*. Coimbra, Almedina.

Martins, A. (2018). Sentimento de Insegurança e Vitimação no Ciberespaço: A relação entre variáveis individuais e contextuais. [Em linha]. Disponível em < https://repositorio-aberto.up.pt/handle/10216/119687>. [Consultado em 02/07/2022].

Martins, J. (2021). Preditores do Medo e Vitimação Online: Um Estudo Empírico. [Em linha]. Disponível em <https://repositorio-aberto.up.pt/bitstream/10216/137800/2/515162.pdf>. [Consultado em 18/06/2022].

Nalaka, G. e 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 Criminology*, 14(1), pp. 176-183.

Nzeakor, O., Nwokeoma, B. e Ezeh, P.(2020). Pattern of Cybercrime Awareness in Imo State, Nigeria: An Empirical Assessment. *International Journal of Criminology*, 14(1), pp. 285-299.

Pequenino, K. (2022). Cibersegurança: Oito em cada dez portugueses preocupados com cibercrime. *Jornal Público,* N.º 11678.

Ribeiro, M. (2015). Cibercrime e Prova Digital. [Em linha]. Disponível em < https://comum.rcaap.pt/bitstream/10400.26/28946/1/Cibercrime%20e%20Prova%20Digital.pdf>. [Consultado em 22/06/2022].

Pires, S., Sani, A. e Soeiro, C. (2018). Stalking e ciberstalking: coocorrência e padrões de vitimação em estudantes universitários. *Arquivos Brasileiros de Psicologia*, 70 (2), pp. 5-21.

Santos, S. (2018). Estudo das Perceções de Cibersegurança e Cibercrime e das Implicações na Formulação de Políticas Públicas. [Em linha]. Disponível em < https://www.repository.utl.pt/handle/10400.5/16235?locale=en>. [Consultado em 12/06/2022].

Silva, J. (2016). Cibercrime: O Crime de Pornografia Infantil na Internet. [Em linha]. Disponível em < https://estudogeral.sib.uc.pt/handle/10316/34801>. [Consultado em 21/06/2022].

Simas, D. (2014). O Cibercrime. [Em linha]. Disponível em < https://recil.ensinolusofona.pt/bitstream/10437/5815/1/Tese%20Cibercrime%20-%20Diana%20Simas.pdf>. [Consultado em 07/06/2022].

UNESCO (2005). *Towards Knowledge Societies*. Paris, UNESCO Publishing.

United Nations Office on Drugs and Crime (2013). *Comprehensive Study on Cybercrime*. New York, United Nations.

Venâncio, P. (2011). *Lei do Cibercrime Anotada e Comentada*. Coimbra, Coimbra Editora.

Vilela, B. (2019). Jovens e redes sociais – Efeitos no desenvolvimento pessoal e social. [Em linha]. Disponível em < https://bibliotecadigital.ipb.pt/bitstream/10198/20576/1/Barbara%20Vilela.pdf>. [Consultado em 27/06/2022].

Wall, D. (2001). Cybercrimes and the Internet. *In:* Wall, D. (Ed.). *Crime and the Internet*. London and New York, Routledge.

Wall, D. (2005). The Internet as a Conduit for Criminal Activity. *In:* Pattavina, A. (Ed.). *Information Technology and the Criminal Justice System*. Thousand Oaks, CA: Sage, pp. 77-98.

Wall, D. (2008). Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers and Technology*, 22(1/2), pp. 45-63.

Yar, M. (2010). Public perceptions and public opinion about internet crime. In: Jewkes, Y. and Yar, M. (Eds.). *Handbook of Internet Crime*. Cullompton, Willan Publishing.

Yar, M. (2016). Online Crime. *In:* Pontell, H. (Ed.). *Oxford research encyclopedia of criminology and criminal justice*. Oxford, Oxford University Press.

Anexo A

Declaração de consentimento informado

Designação do Estudo:

"Avaliação do conhecimento e perceção sobre cibercrime por jovens estudantes universitários".

Eu, abaixo-assinado, ----------, compreendi a explicação que me foi fornecida acerca da participação na investigação que se tenciona realizar, bem como do estudo em que serei incluído. Foi-me dada oportunidade de fazer as perguntas que julguei necessárias, e de todas obtive resposta satisfatória. Tomei conhecimento de que da informação ou explicação que me foi prestada versaram os objetivos e os propósitos deste estudo. Além disso, foi-me afirmado que tenho o direito de recusar, a todo o tempo, a minha participação no estudo, sem que isso possa ter como efeito qualquer prejuízo pessoal.

Foi-me ainda assegurado que os registos em suporte papel e/ou digital serão anónimos e confidenciais, sendo utilizados única e exclusivamente para o estudo em causa, e sendo guardados em local seguro durante a pesquisa e destruídos após a sua conclusão.

Por isso, consinto em participar no estudo em causa.

Data: _____/_____/ 2022

Assinatura/Rúbrica do participante no projeto: _____

Assinatura do investigador responsável: _____

(José Pedro Granja)