Universidade Fernando Pessoa
Faculdade de Ciências Humanas e Sociais

Licenciatura em Criminologia

Projeto de Graduação

O crescimento da burla informática em contexto de pandemia de COVID-19 em Portugal

Ana Rita Lopes da Silva
Porto, 2022

Universidade Fernando Pessoa
Faculdade de Ciências Humanas e Sociais

Licenciatura em Criminologia

Projeto de Graduação

O crescimento da burla informática em contexto de pandemia de COVID-19 em Portugal

Ana Rita Lopes da Silva
Porto, 2022

Universidade Fernando Pessoa

Faculdade de Ciências Humanas e Sociais

Licenciatura em Criminologia

Projeto de Graduação

O crescimento da burla informática em contexto de pandemia de COVID-19 em Portugal

A Aluna

_____

(Ana Rita Lopes da Silva)

Projeto de Graduação apresentado à Faculdade de Ciências Humanas e Sociais da Universidade Fernando Pessoa, como parte dos requisitos necessários para a obtenção do Grau de Licenciada do Curso de Criminologia, sob a orientação do Professor Doutor Joaquim Ramalho.

Resumo

Os crimes de teor informático e *online* aumentaram exponencialmente devido ao confinamento social, decorrente do eclodir da pandemia de COVID-19. Este aumento deveu-se à necessidade das pessoas se manterem conectadas ao mundo e de alguns negócios resistirem à crise. Recorrer ao cibermundo foi a estratégia utilizada por indivíduos para fazer compras *online* ou perpetrarem crimes inerentes à *Internet* e à informática.

O presente projeto pretende expor o conceito do cibercrime, mais concretamente das burlas informáticas/*online*, de modo a compreender de que forma são perpetrados estes crimes e porque aumentaram com o aparecimento da pandemia que assolou o mundo, em 2020. Mediante uma proposta de intervenção apoiada num método qualitativo, é esperado a realização de entrevistas a profissionais da área da criminologia e/ou direito, com o intuito de compreender quem são os possíveis envolvidos nestes crimes e quem tem mais probabilidade de se tornar vítima. Para além disso, intenta-se perceber o que um criminólogo faz nestes casos, a nível de prevenção e/ou intervenção, como também compreender os aspetos a ser melhorados para evitar vitimação e a perpetração de burlas informáticas.

Palavras-chave: Burla informática, Cibercrime, COVID-19

Abstract

Computer and online crimes have increased exponentially due to social confinement, stemming from the outbreak of the COVID-19 pandemic. This increase was due to the need for people to stay connected to the world and for businesses to face the crisis. Log onto the cyberworld was the strategy used by individuals to make online purchases or perpetrate crimes inherent to the Internet and computing.

This project aims to expose the concept of cybercrime, more specifically online/informatic scams, to understand how these crimes are perpetrated and why they have increased with the onset of the pandemic that devastated the world in 2020. Through an intervention proposal supported by a qualitative method, it is hoped to conduct interviews with professionals in the area of criminology and/or law, in order to understand who, the possible participants in these crimes are and who is more likely to become a victim. In addition, we intend to understand what a criminologist does in these cases, in terms of prevention and/or intervention, as well as to understand the aspects to be improved to avoid victimization and the perpetration of computer fraud.

Keywords: Online fraud, Cybercrime, COVID-19

Agradecimentos

Quero agradecer à Universidade Fernando Pessoa e a todos os professores com quem me cruzei nestes 3 anos.

Aos meus pais por me terem proporcionado a oportunidade de estudar na UFP, pelo apoio e amor incondicional e por estarem sempre onde eu precisava.

Às minhas amigas mais queridas, Sofia, Bárbara e Bia, por acreditarem em mim e me darem sempre força e por preencherem a minha vida de cor.

À minha família que festeja as minhas conquistas e me ampara nas contrariedades da vida.

Ao Pedro, mesmo já não estando por cá, esteve sempre presente a dar-me motivos para continuar, meu anjo da guarda.

Por fim, agradeço ao orientador, Professor Doutor Joaquim Ramalho, por toda a ajuda e disponibilidade na realização deste projeto.

Índice

Índice de Siglas

CP – Código Penal

STJ – Supremo Tribunal de Justiça

Art. – Artigo

PGR – Procuradoria-Geral da República

OPC – Órgãos de Polícia Criminal

Índice de Anexos

Introdução

O presente projeto de graduação, é intitulado de "O crescimento da burla informática em contexto de pandemia de COVID-19 em Portugal" e foi realizado de modo a obter o grau de Licenciada do curso de Criminologia. A burla informática tem sido um fenómeno cada vez mais debatido devido ao aumento progressivo da sua prática, especialmente durante a pandemia de COVID-19. Em tempo de flagelo, o uso da *Internet* e plataformas *online*, como redes sociais ou lojas *online* aumentou consideravelmente e, portanto, tanto pessoas individuais como empresas foram compelidos a adaptar-se à nova realidade e incluir o cibermundo no seu quotidiano, de modo a manter o normal funcionamento da vida. No entanto, não só aspetos positivos decorreram da nova era tecnológica, uma vez que foram desenvolvidos e/ou aperfeiçoados novos métodos criminais. A burla informática foi um dos crimes mais desenvolvidos e praticados durante os anos de 2020, 2021 e 2022 (até à data), onde houve vários períodos de confinamento social. De acordo com o Boletim do Observatório de Cibersegurança (2021), no ano 2021 houve um aumento de 124% de criminalidade informática em relação ao ano de 2019.

Em virtude do exposto, este Projeto de Graduação está divido em dois capítulos principais. O primeiro é destinado ao enquadramento teórico do tema, começando pelo conceito de cibercrime e burla, que serão o ponto de partida para compreender em que consiste a burla informática e as suas vertentes, terminando na dificuldade em investigar casos de crimes de burla informática e outros crimes *online*. Por outro lado, no segundo capítulo, encontra-se uma proposta de estudo relacionada ao aumento da burla informática em tempo de pandemia de COVID-19, em Portugal. O estudo consiste em compreender de que modo esta interferiu na prática de crimes e permitiu aperfeiçoar os crimes tradicionais e conceber novas tipologias de crimes, em especial da burla informática; quem foram/são as principais vítimas e o tipo de perpetradores. Para além disso, é indispensável entender o papel dos criminólogos em contexto de prevenção e/ou intervenção em caso de crimes de burla informática e outros crimes online, bem como depreender sobre o que deve ser melhorado, para evitar vitimação e a prática destes atos. Num modo geral, o estudo propõe confirmar as afirmações do parágrafo anterior, através de entrevistas.

Deste modo, em contexto metodológico, a proposta apresenta uma perspetiva qualitativa. Destarte, irá ser apresentado os objetivos gerais e específicos da investigação, a metodologia, os participantes, o método utilizado para a recolha dos dados, o procedimento e, por fim, os resultados esperados do estudo.

Parte I – Enquadramento Teórico

1. Cibercrime

O crime informático só se tornou possível no decorrer das últimas décadas, visto que apenas a utilização da *Internet* o permite, uma vez que é uma criação recente. A vida das pessoas tornou-se muito mais facilitada, «ao permitir o acesso, em questão de segundos, em qualquer parte do mundo» (Nunes, 2021, p.11). A partir da ligação a uma rede de *Wi-Fi* é possível obter uma quantidade absurda de informação «armazenada em servidores localizados em todo o Mundo» (Nunes, 2021, p.11), como também é possível estabelecer comunicação instantânea e gratuita entre pessoas que se encontram em polos opostos do globo. Deste modo, para angariar mais consumidores, as empresas tiveram de se adaptar e aderir ao novo mundo *on-line*. De acordo com Duarte Nunes (2021, p.11), a estratégia das empresas focou-se na «monitorização da atividade das pessoas na Internet […] levadas a cabo através de cookies». As empresas acabam por criar perfis de consumo através da informação arrecadada do histórico de navegação dos utilizadores de *Internet*, desenvolvendo assim, publicidade específica e estratégias comerciais eficazes, de modo a criar um mercado rentável (Nunes, 2021, p.11).

No entanto, apesar de todas as benesses da *Internet* e do mundo *on-line*, é necessário compreender que não é um espaço totalmente seguro e podemos até afirmar a sua fragilidade, pelo seu carácter recente, transfronteiriço e ilimitado. O desenvolvimento da tecnologia originou um novo tipo de criminalidade, o cibercrime ou criminalidade informática.

A UNODC (*United Nations Office on Drugs and Crime*), salienta que os crimes informáticos «são uma forma de crime transnacional em expansão», uma vez que ocorrem num espaço sem fronteiras - o ciberespaço -, e levados a cabo cada vez mais assiduamente por organizações criminosas.

Até a atualidade não há um consenso sobre a definição exata do conceito de cibercrime. No entanto, Feliz Gouveia, no *Dicionário Crime, Justiça e Sociedade* (2016, p.78), considera que é todo o «crime que é facilitado, permitido ou amplificado pela *Internet*». Por outras palavras, a informática é um meio para praticar crimes considera-

dos tradicionais, isto é, praticados no mundo físico, como também, foram desenvolvidos outros tipos de crimes inerentes ao uso da tecnologia informática e *Internet*.

O desentendimento em relação à caracterização do crime informático levou vários autores a produzir a sua própria noção. Enquanto por um lado, alguns consideravam "todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é alvo simbólico desse ato ou em que o computador é objeto de crime" (Marques e Martins, 2006 *cit. in* Simas, 2014, p.12), outros acreditam a informática da criminalidade digital é o bem jurídico a ser protegido, onde os crimes informáticos são dispostos em categorias distintas - «crime informático digital próprio/puro ou crime digital impróprio/impuro» (Simas, 2014, p.12).

Sendo assim, é possível distinguir os autores entre «criminalidade informática em sentido amplo e criminalidade informática em sentido estrito» (Nunes, 2021, p.11). No sentido amplo, é possível afirmar que toda a criminalidade «pode ser cometida através de meios informáticos» (Simas, 2014, p.12), mas que segundo Duarte Nunes (2021, p.37), o mesmo crime pode também ser cometido via outros meios, uma vez que a informática/*internet*, são apenas um possível instrumento para a sua prática. Em relação ao conceito estrito, múltiplos autores consideram que apesar do bem jurídico a ser protegido não ser necessariamente digital, o meio informático é parte integradora do tipo legal (Simas, 2014, p.12), por exemplo, burla informática e outros tipos de crimes previstos na Lei n.º 109/2009, de 15 de setembro[1].

Segundo Nelson Amador (2018, p.19) e incluído pela Comissão Europeia no conceito de cibercrime, este foi dividido em três categoria de crimes, sendo a primeira referente aos crimes tradicionais, como a fraude ou a falsificação; no segundo grupo, podemos encontrar a publicação, em meios de comunicação *on-line*, de conteúdos ilegais. Por último, a Comissão Europeia dispôs na terceira categoria todos os «crimes eletrónicos propriamente ditos», por exemplo, pirataria ou ataques aos sistemas informáticos.

[1] Lei n.º 109/2009, de 15 de setembro, *Lei do Cibercrime*. Aprovada relativamente «a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa».

Por outro lado, a Convenção sobre o Cibercrime, no Conselho da Europa (2001), e citando Gouveia no *Dicionário Crime, Justiça e Sociedade* (2016, p.78), estabeleceu quatro grandes grupos para combater o cibercrime: «a) ofensas contra a integridade, a disponibilidade e a confidencialidade dos sistemas informáticos e dos seus dados, b) fraude e falsificação informática, c) produção, disseminação e posse de conteúdos ilegais, e d) violação de direitos de autor e de propriedade intelectual». Estes grupos encontram-se descritos na Doutrina Portuguesa em diferentes documentos legais. Os artigos n.º 193 (*Devassa por meio de informática*) e n.º 221 (*Burla informática e nas comunicações*) do Código Penal Português, referentes à primeira alínea, onde encontramos «os crimes que recorrem a meios informáticos, não alterando o tipo penal comum» (Simas, 2014, p.13). De seguida, encontramos na Lei n.º 58/2019, de 08 de agosto (*Dados pessoais para prevenção, deteção, investigação ou repressão de infrações penais*) e na Lei n.º 69/98, de 28 de outubro (*Regula o tratamento dos dados pessoais e a proteção da privacidade no setor das telecomunicações*), os crimes relacionados à proteção de dados pessoais e proteção da privacidade, contidos na alínea *b)* previamente abordada, e os crimes retratados na alínea *c)* podem ser identificados na Lei n.º 109/2009, de 15 de setembro (*Lei do Cibercrime*), onde a informática é «o elemento próprio do tipo de crime» (Simas, 2014, p.13). Finalmente, os crimes em detrimento do conteúdo, como violações dos direitos de autor, a difusão de pornografia infantil ou a discriminação racial ou religiosa, inserem-se nos artigos 171.º, nº3, alínea *b)* e artigo 176.º do CP (*Abuso Sexual de Crianças*) e artigo 240.º, nº1, alínea *a)* do Código Penal (*Discriminação e incitamento ao ódio e à violência*).

Como dito anteriormente, a Convenção sobre o Cibercrime foi adotada pela Lei n.°109/2009 – *Lei do Cibercrime* –, em Portugal, tipificando seis categorias: «i) Falsidade informática; ii) Dano relativo a programas ou outros dados informáticos; iii) Sabotagem informática; iv) Acesso ilegítimo; v) Interceção ilegítima; vi) Reprodução ilegítima de programa protegido.» (Gouveia *In* Dicionário Crime, Justiça e Sociedade, 2016, pp.78-79). Para além disso, a Procuradoria-Geral da República estabeleceu um Gabinete Cibercrime, em 2011, de modo a efetivar uma aplicabilidade eficiente da Lei do Cibercrime, criando vias eficazes e específicas durante os processos criminais de cibercrime, com o intuito de facilitar a colaboração nas diligências de inquérito entre o «Ministério Público e os órgãos de Polícia Criminal e entre estes e entidades privadas» (Simas, 2014, pp.161-162).

A Convenção sobre o Cibercrime do Conselho da Europa, de acordo com Maria Ribeiro (2015, p.7), estabeleceu três objetivos: «harmonizar legislações e os crimes neles previstos; estender às jurisdições de Estados Membros determinados instrumentos processuais de produção de prova modernos e adequados à investigação da cibercriminalidade; […], pretende facilitar a cooperação internacional e viabilizar investigações»

Lourenço Martins (*cit. in* Maria Ribeiro, 2015, p.8) resumiu brevemente a Convenção sobre o Cibercrime:

> «*Visa prevenir os atentados à confidencialidade, integridade e disponibilidade dos sistemas informáticos, das redes e dos dados, bem como o uso fraudulento de tais sistemas, redes e dados, assegurando-se a incriminação dos comportamentos respectivos (direito penal material); visa ainda a adopção de poderes processuais suficientes para a detecção, investigação e perseguição contra estas infracções penais, quer no plano nacional quer internacional. Dedica particular atenção à pornografia infantil (artigo 9. °) cometida através das redes e às infracções relativas à propriedade intelectual e aos direitos conexos.*
>
> *No direito processual, avultam as medidas para conservação rápida de dados informáticos registados, conservação, divulgação rápida de dados relativos ao tráfico das mensagens, podendo haver injunções para divulgação de dados que estejam na posse ou sob controlo de alguém, nomeadamente de um fornecedor de serviços em rede, busca e apreensão de dados informáticos armazenados, colheita de dados relativos ao tráfico em tempo real, intercepção de conteúdos.*
>
> *Um outro capítulo é dedicado a regras de cooperação internacional, e dentro deste a disposições específicas sobre a conservação de dados informáticos e sua rápida divulgação, e entreajuda respeitante a poderes de investigação.*
>
> *Finalmente, as Partes providenciarão por um ponto de contacto permanente (rede 24/7) para assistência imediata nestas investigações, designadamente recolha de provas sob forma electrónica de uma infracção penal*.».

Deste modo, a Lei n.º 109/2009, de 15 de setembro foi aprovada, em Portugal e transposta para a ordem jurídica interna a Decisão-quadro n.º 2005/222/JAI do Conselho de 24 de fevereiro. Esta última estipulou as «disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional e matéria penal, relativas ao domínio do cibercrime e de recolha de prova ou suporte eletrónico, tendo a mesma como base a Convenção de Budapeste» (Azevedo, 2016, p.19). No entanto, apenas a Lei do Cibercrime é que permitiu encontrar «medidas processuais aplicáveis à investigação criminal do cibercrime», uma vez que prevê tipologias legais de crimes em que a informática aparece como meio para a perpetração do crime (Azevedo, 2016, p.19). Ao contrário do Código Penal, na Lei do Cibercrime, encontramos crimes com bem jurídicos a proteger a incidir sobre a «integridade dos sistemas informáticos» (Azevedo, 2016, p.19). Podemos observar que a Lei do Cibercrime é aplicada na jurisprudência portuguesa:

«A pesquisa no computador dos dados informáticos que dele constam, bem como a apreensão desses dados é regulada na Lei do Cibercrime, em cujo âmbito definido logo no artº 1º se encontram "as disposições penais materiais e processuais (…), relativas ao domínio (…) da recolha de prova em suporte electrónico".»[2]

«O documento obtido através de recolha de prova em suporte eletrónico consubstanciando uma impressão de uma publicação realizada pelo arguido no mural do seu perfil de Facebook, que opera através da internet e no âmbito de um sistema informático é regulado pela lei do cibercrime»[3].

Portugal e o mundo viram o cibercrime crescer com a pandemia de COVID-19, com uma tendência a aumentar o número de incidentes a cada ano. O crime informático aumentou exponencialmente paralelamente «aos momentos de maior confinamento social», sendo fevereiro de 2021, o mês com mais casos registados (190 incidentes) devido ao confinamento (Boletim Observatório de Cibersegurança, 2021). Segundo o

[2] Acórdão 2039/14.0JAPRT.P1 de 07 de julho de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cffe710b2cb8d91e8025800500475ea9?OpenDocument&Highlight=0,inform%C3%A1tica,cibercrime [consultado em 30/09/2022].
[3] Acórdão 471/15.0T9AGD-A.P1 de 13 de abril de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument&Highlight=0,inform%C3%A1tica,cibercrime [consultado em 30/09/2022].

Centro Nacional de Cibersegurança (2022), os casos de crimes informáticos tiveram um aumento muito significativo em 2020 (689 dos incidentes registados) e, em 2021, houve um aumento de 26% (847 dos incidentes registados). O *phishing*/*smishing* foram as tipologias mais registadas contribuindo 40% para o total de crimes informáticos.

2. Burla

Uma das vertentes do cibercrime é a burla informática, no entanto, é necessário compreender no que se fundamenta a burla em si, antes de nos debruçar-nos sobre o tema deste trabalho.

De acordo com José Alfredo (2013, p.15), a burla começa quando um agente com a intenção de obter enriquecimento ilegítimo para si ou para outrem promove com astúcia, factos que pretendam induzir em erro ou enganar outra pessoa, «fazendo-a praticar atos que causem a ela mesma (ou a terceiros) um prejuízo de cariz patrimonial». Sendo assim, é-nos possível afirmar que a característica essencial do crime de burla é a de induzir alguém em erro, «isto é, implica a colaboração da vítima, resultando numa viciação da vontade de que foi objeto» (Azevedo, 2016, p.29). O crime de burla está tipificado no artigo 217.º do C.P. Português[4].

Como é possível verificar, o crime de burla enquadra-se nos crimes contra o património, logo o bem jurídico a proteger é o «património do sujeito passivo globalmente considerado» (Alfredo, 2013, p.15). Isto significa que a burla não é crime contra a propriedade, uma vez que dos crimes contra o património «tem de resultar um prejuízo patrimonial enquanto elemento do crime» (Azevedo, 2016, p.29). O «erro ou engano sobre factos que astuciosamente provocou», no artigo 217.º C.P. Português, referem-se à «provocação de uma falsa representação da realidade», sendo a astúcia o «aproveitamento de uma vantagem cognitiva do agente sobre o burlado que lhe permite manipular

[4] ***Artigo 217.º do CP***
Burla
1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, por meio de erro ou engano sobre factos que astuciosamente provocou, determinar outrem à prática de atos que lhe causem, ou causem a outra pessoa, prejuízo patrimonial é punido com pena de prisão até três anos ou com pena de multa.
2 - A tentativa é punível.
3 - O procedimento criminal depende de queixa.
4 - É correspondentemente aplicável o disposto nos artigos 206.º e 207.º.

a vontade do burlado» (Albuquerque, 2010 *cit. in* Azevedo, 2016, p.31) e meio necessário para enganar ou persuadir. Por outro lado, o erro equivale à «falsa ou nenhuma representação da realidade concreta, que funcione como vício do consentimento da vítima» (Azevedo, 2016, p.31) e o engano corresponde à «simples mentira» (Azevedo, 2016, p.31). O crime de burla, segundo Ana Azevedo (2016, p.32), apenas é consumado se da prática do crime resultar prejuízo patrimonial e, consequentemente, o empobrecimento da vítima ou de terceiros.

De modo a corroborar os parágrafos anteriores, podemos observar alguns exemplos na jurisprudência portuguesa, mostrando como os crimes de burla são julgados:

«I. Há pelo menos sete novos dados a impor a ultrapassagem da fixação da jurisprudência dos acórdãos do STJ quanto ao concurso de crimes de falsificação e burla. II. Uma falsificação de escritos utilizados unicamente como meio de burlar alguém, está em concurso aparente (é consumida pelo) com o crime de burla (crime-fim), devendo a punição deste concurso ser encontrada na moldura penal mais grave, na qual se considerará o ilícito excedente em termos de medida da pena.»[5]

«I - Quando não existe encenação com vista a levar a vítima a desejar fazer o negócio (pensando erradamente que está a fazer um bom negócio), o lucro assim obtido é legítimo, isto é, o vendedor aproveita as regras gerais da concorrência, as regras específicas do mercado de veículos usados e a necessidade do comprador, ganhando dinheiro legitimamente. Quando o lucro é obtido através de engano "astuciosamente provocado" pelo agente (p. ex., viciando o conta-quilómetros), esse lucro, mesmo pequeno, corresponde a um enriquecimento ilegítimo, sendo certo que a ilegitimidade não está em ter tido lucro, mas no modo como o obteve. II – No caso, o prejuízo patrimonial do ofendido traduz-se na diminuição do valor do seu património ao adquirir o veículo por um valor superior, devido à adulteração da quilometragem: o ofendido sofreu com um pre-

[5] Acórdão 4395/03.6TDLSB.L1-5, de 29 de junho de 2010, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d1cf18b34be2a7648025777a00492765?OpenDocument [consultado em 01/10/2022].

juízo equivalente ao valor da diferença entre o que pagou e o valor do bem que recebeu em troca.»[6]

«I - No crime de burla existe, pelo menos, um duplo nexo causal: a acção enganadora (astúcia do agente) tem de ser a causa do erro (engano) e este engano tem de ser a causa da disposição patrimonial (entrega do bem). II – O acto de enganar (astucioso) tem de ser anterior à entrega (ou logo seguido) pois em primeiro lugar tem de existir o convencimento (feito por acção do arguido) do ofendido a fazer a posterior disposição patrimonial, devendo uma (a acção enganosa do arguido) ser causa da outra (entrega/disposição patrimonial pelo ofendido). III - Se o ofendido entrega ao arguido veículos automóveis para que este os venda e lhe entregue o dinheiro acordado das vendas, e este vende os veículos e não lhe entrega o dinheiro, ficando com ele e dele se apropriando, não comete o crime de burla mas o de abuso de confiança. IV - Não é de verificação impossível e nem excessivamente onerosa a condição imposta ao arguido de pagar a indemnização arbitrada, se esta consiste em pagar pouco mais do que a quantia de que se apropriou, tendo já decorrido três anos para fazer essa entrega e não o fez. V - A suspensão da execução da pena de prisão é benesse concedida ao arguido que a deve ver como oportunidade de mudar de vida de modo a que não tenha de ir para a prisão.»[7]

Do artigo n.º 217.º ao artigo n.º 222.º do Código Penal Português defrontamo-nos com as vertentes existentes de crime de burla. No artigo 218.º do CP, a burla qualificada, compreende que se «a) o prejuízo patrimonial for de valor elevado; b) o agente fizer da burla modo de vida; c) o agente se aproveitar de situação de especial vulnerabilidade da vítima, em razão de idade, deficiência ou doença; ou d) a pessoa prejudicada ficar em difícil situação económica», a pena de prisão passa a ser até cinco anos ou uma pena de multa de até 600 dias, ou seja, a pena torna-se agravada pela existência de dolo. Os artigos penais a seguir pertencem ao crime de burla relativa a seguros (artigo 219.º do CP); crime de burla para obtenção de alimentos, bebidas ou serviços (artigo 220.º do

[6] Acórdão 573/14.0T9VLG.P1, de 13 de julho de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/97fbc0f04e943da380258009004b4f7a?OpenDocument [consultado em 01/10/2022].
[7] Acórdão 529/11.5TABGC.P1, de 19 de fevereiro de 2014, disponível em: http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/86a0c32b8287111d80257c9200501b88?OpenDocument [Consultado em 01/10/2022].

CP); crime de burla informática e nas comunicações (artigo 221.º do CP) e, por último, o crime de burla relativa a trabalho ou emprego (artigo 222.º do CP).

3. Burla informática

Os crimes de burla informática compartilham com a burla clássica, o mesmo objetivo, isto é, obter enriquecimento ilegítimo, «causando a outra pessoa prejuízo patrimonial» (Azevedo, 2016, p.37). Não obstante, esta artimanha não necessita recorrer ao erro ou engano de uma pessoa, uma vez que «a máquina não pode ser ludibriada» (Azevedo, 2016, p.37), havendo sim, um erro ou artifício diretamente sobre dados ou aplicações informáticas (Azevedo, 2016, p.37).

Há quem compare crimes de burla informática aos crimes de colarinho branco, não em sentido conceitual, mas no âmbito das semelhanças entre ambas as práticas. De acordo com Ana Azevedo (2016, p.34), podemos considerar ambos como sendo crimes habitualmente cometidos por pessoas com um estatuto social elevado, que não recorrem à violência e com pretensão de obter "lucro financeiro" (Azevedo, 2016, p.34). Para além disso, Azevedo refere um aspeto importante deste tipo de delitos: a «difícil perceção pelo homem comum dado a alta destreza que caracteriza tão bem os criminosos mais sofisticados» e que requer astúcia (Azevedo, 2016, p.34).

Aliás, Maria Morgado e José Vegar (2003, p.33) agruparam os crimes económico-financeiros, ou crimes de colarinho branco, em 3 grupos. A primeira categoria está relacionada aos crimes tributários «que se subdividem em aduaneiros, fiscais e contra a segurança social» (Morgado e Vegar, 2003, p.33). Neste caso, e segundo os autores, o transgressor objetivava a «apropriação fraudulenta das quantias devidas ao Estado como imposto». No segundo grupo e que denotamos como sendo o mais relevante para este trabalho, foram integrados os crimes de burla informática e nas telecomunicações. Os crimes informáticos relacionavam-se ao «acesso indevido a sistemas computadorizados, para obter informações, como no uso do computador e das redes virtuais para a obtenção de lucro ilegal» (Morgado e Vegar, 2003, p.37). Um dos exemplos mais relevantes que Morgado e Vegar nos dão é o da «intrusão em redes sensíveis» que explicado sucintamente sugere que com o propósito de coletar números de cartões de crédito, os infratores procederiam à aquisição de bens e produtos (Morgado e Vegar, 2003, p.37). Ainda

referente ao segundo grupo de crimes de colarinho branco, e ao "nível das telecomunicações e internet" (Morgado e Vegar, 2003, p.37), encontramos a pornografia infantil, e consequente venda na Internet. Por último, na terceira categoria estavam enquadrados os crimes de peculato e corrupção, onde os autores descreveram como sendo «crimes económicos e conexos» (Morgado e Vegar, 2003, p.37), isto é, são crimes económicos com uma correlação entre si. Neste grupo, Morgado e Vegar (2003, p.38) figuraram o branqueamento de capitais e o tráfico de influências, configurando uma «forma contemporânea de assalto».

Ao contrário da burla tradicional, na burla informática não existe intervenção de terceiros «no sentido de não se dirigir à manipulação da vontade de uma pessoa» (Azevedo, 2016, p.35), muito menos há «um ato gerador do prejuízo patrimonial por alguém» (Santos, 2005 *cit. in* Azevedo, 2016, p.35), uma vez que no caso da burla informática o intermediário seria o sistema informático.

Por este motivo, podemos admitir que o computador, sendo apenas um meio de ação para o delito, «não poderá ser alvo de engano ou de comportamentos que classifiquem a particularidade da burla tradicional» (Azevedo, 2016, p.36). É, portanto, um delito contra o património, via manipulação informática com o propósito de obter enriquecimento ilegítimo do agente ou de terceiros, «num processo executivo que não contempla, de permeio, a intervenção de outra pessoa (por isso não comporta o duplo nexo de imputação causal referido no art. 217º)»[8] Podemos afirmar que as características supracitadas explicam «de onde advém a sua especificidade» (Azevedo, 2016, p.35). Sendo assim, a burla informática só acontece quando estão verificadas as condições previstas no artigo 221. ° do CP[9].

[8] Acórdão 1318/02 de 15 de maio de 2002, disponível em: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/0fdd0aa4bad15aff80256bcd00475da3 [consultado em 14/09/2022].

[9] ***Artigo 221.º do CP***
Burla informática e nas comunicações

1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, mediante interferência no resultado de tratamento de dados, estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.

2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos eletrónicos ou outros

Podemos admitir que a burla informática é um crime de resultado cortado ou parcial[10], uma vez que a consumação do ataque se dá com o dano patrimonial da vítima, não levando em conta se houve benefício económico ao infrator ou de terceiros (Azevedo, 2016, p.37). No entanto, esta característica de um delito de resultado parcial/cortado deve-se à intenção de enriquecimento (Azevedo, 2016, p.37).

Em acórdãos relacionados a crimes informáticos, o STJ tem optado por definir como bem jurídico a proteger, não apenas o património, como também «a fiabilidade dos dados e a sua proteção» (Azevedo, 2016, p.36), como podemos ver pelos seguintes excertos dos Acórdãos do STJ:

«No crime de burla informática do art.º 221.º, do C. Penal, o bem jurídico protegido é não só o património – mas concretamente, a integridade patrimonial – mas também os programas informáticos, o respetivo processamento e os dados, na sua fiabilidade e segurança»[11].

«O bem jurídico tutelado pelo crime de falsidade informática é a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório (onde se inclui a segurança nas transações bancárias), afetando, ainda que reflexamente, a integridade dos sistemas informáticos.»[12].

---

meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.

3 - A tentativa é punível.

4 - O procedimento criminal depende de queixa.

5 - Se o prejuízo for:

a) De valor elevado, o agente é punido com pena de prisão até cinco anos ou com pena de multa até 600 dias;

b) De valor consideravelmente elevado, o agente é punido com pena de prisão de dois a oito anos.

6 - É correspondentemente aplicável o disposto no artigo 206.º

[10] A jurisprudência portuguesa explica que um «crime de resultado parcial ou cortado, caracterizado por uma descontinuidade ou falta de congruência entre os correspondentes tipos subjetivo e objetivo, já que se exige intenção de enriquecimento ilegítimo do agente, a consumação não depende desse enriquecimento, mas do empobrecimento (dano) da vítima». Acórdão 0014449, de 03 de maio de 2001, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7f9f1fe8642dc81580256a7f0036b9d3?OpenDocument [consultado em: 14/09/2022].

[11] Acórdão 05P2253, de 06 de outubro de 2005, disponível em: http://www.dgsi.pt/jstj.nsf/-/1E2E4014CF41DC87802570920057EC37 [consultado em 08/09/2022].

[12] Acórdão 1462/16.0PCSNT.S1, de 18 de novembro de 2020, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/526b2874eddd6aeb80258685006f0317?OpenDocument&Highlight=0,cibercrime [consultado em 08/09/2022].

Em 2021, a burla informática e nas telecomunicações foi o crime informático com maior preponderância, cerca de 91% do total (Relatório de Cibersegurança, 2022). Para além disso, 75% dos casos de condenação por crime informático eram relacionados a burla informática. Os crimes informáticos e, em especial, crimes de burla informática e nas telecomunicações veem uma tendência para aumentar, uma vez que crimes relacionados às tecnologias se têm tornado uma das tipologias criminais mais adotadas por criminosos. Consoante o Relatório Anual de Segurança Interna (2021), este crescimento começou a notar-se com o confinamento social, em 2020, devido à pandemia de COVID-19, com 19.855 casos registados e, um aumento de 7,7%, em 2021, para 21.374 incidentes registados.

4. Como se manifesta a burla informática

4.1. *Phishing*

No mundo atual, os criminosos encontraram novas formas de expandir a burla tradicional e ligá-la à cibercriminalidade. Sendo assim, desenvolveram um novo tipo de crime, a burla informática. Deste modo, uma das suas vertentes é o *phishing*.

O *phishing* tornou-se num dos tipos de criminalidade dominante no ciberespaço e é «considerado atualmente a forma mais popular de fraude na *Internet*» (Ferreira e Fávero *In* Dicionário Crime, Justiça e Sociedade, 2016, pp.359-360), sendo o tipo de criminalidade informática mais denunciado ao Gabinete do Cibercrime da PGR, em 2021 (Relatório de Cibersegurança, 2022). Aliás, o *phishing* é uma "técnica decetiva" da engenharia social[13].

Significa, literalmente, «pescar por palavras-passe» (Ferreira e Fávero *In* Dicionário Crime, Justiça e Sociedade, 2016, p.359), dado que se fundamenta no envio de *emails* que redirecionam a vítima a *sites* fraudulentos, que julga ser fidedigno, de uma "empresa com reputação". No entanto, esta página «gerida por terceiros é falsa!» (Azevedo, 2016, p.68). Depois de aceder ao *site*, este induziria as pessoas a revelarem as

[13] De acordo com Ana Azevedo (2016, p.67), na sua dissertação *Burlas Informáticas: Modos de Manifestação*, engenharia social consiste na «prática de recolha de informações por intermédio da exploração de relações humanas de confiança, ou outros métodos que enganem utilizadores e administradores de sistemas».

suas palavras-passe ou dados de cartões bancários, sem que a estas constatassem que estavam a ser vítima de um crime aleivoso (Ferreira e Fávero *In* Dicionário Crime, Justiça e Sociedade, 2016, p.359). Este procedimento é intitulado por «bait and hook», isto é, «isco e gancho» (Emm, 2006 *cit. in* Ferreira e Fávero *In* Dicionário Crime, Justiça e Sociedade, 2016, p.360). Outra técnica do *phishing* relativamente parecida seria (com o mesmo propósito), enviar uma mensagem instantânea com um *link* para um *site* com as mesmas características do método anterior (Ferreira e Fávero *In* Dicionário Crime, Justiça e Sociedade, 2016, p.360).

É-nos possível afirmar que a utilização de dados pessoais sem autorização para obtenção de lucro patrimonial é o objetivo dos delinquentes, através de atos preparatório que, tal como Ana Azevedo (2016, p.69) ilustra são: o «envio de mensagens de conteúdo enganoso e a construção de uma página *web* em tudo idêntica à original». Estes últimos são atos preparatórios do crime da burla informática, logo «não deverão ser punidas individualmente» (Azevedo, 2016, p.69).

4.2. *Smishing*

O *smishing*, variante do *phishing*, serve como propósito para «levar o utilizador a fornecer informação pessoal» (Azevedo, 2016, p.76). A partir de mensagens SMS, o remetente ludibria o «recetor da mensagem a transferir dinheiro da sua conta bancária» (Azevedo, 2016, p.76).

4.3. *Vishing*

Outra variante do *phishing*, o *vishing* utiliza mensagens de voz para obter ilegalmente dados pessoais. Neste caso, a burla é concebida através de chamadas telefónicas em tempo real, o que torna o processo mais rápido e eficaz, ao contrário de outras técnicas assíncronas, como *emails*, que podem nem ser abertos ou lidos. Por outro lado, «é inerentemente mais difícil de analisar o vishing por ser de difícil rasto» (Azevedo, 2016, p.77), uma vez que, como referido anteriormente, é um crime realizado em tempo real.

4.4. *Pharming*

Com a mesma finalidade do *phishing*, o *pharming* consiste no ataque dos servidores ou do router, ou seja, todos os que utilizarem a mesma infraestrutura de comunicação que está a ser alvo de ataque serão «explorados simultaneamente», uma vez que, o invasor tem controlo sobre a rede em que passa informação (Azevedo, 2016, p.77). A única e grande diferença entre *pharming* e *phishing* é que em *pharming* recebe-se *links* genuínos para revelar os seus dados pessoais, pois o *router* é o alvo do ataque. Já no *phishing*, a vítima é redirecionada a *sites* "aparentemente" genuínos (Azevedo, 2016, p.79).

4.5. *Skimming*

Apesar de não ser uma técnica que utiliza *internet* para obter dados pessoais ou bancários, está, no entanto, relacionado à clonagem de cartões bancários. O *skimming* utiliza de um aparelho, *skimmer*, que se entende por um «aparelho de leitura e gravação de bandas magnéticas» (Azevedo, 2015, p.80).

Explicado mais detalhadamente e segundo o Relatório Geral sobre as atividades da Europol de 2010, o *skimming* traduz-se na «cópia da banda magnética de um cartão de pagamento, sem o conhecimento ou o consentimento do titular do cartão, que acontece geralmente quando o cartão de pagamento está a ser utilizado pelo titular numa ATM genuína ou num terminal de um ponto de venda. Os dados são depois escritos (clonados) em novos cartões que são utilizados para fazer levantamentos ilícitos de dinheiro, o que geralmente acontece fora do país de residência do titular do cartão».

Esta técnica tem se tornado cada vez mais apelativa, devido à «simplicidade dos materiais utilizados» (Azevedo, 2016, p.81) para gravar os dados dos cartões bancários e, posteriormente, subtrair dinheiro à vítima.

4.6. *Homebanking*

O *homebanking* ou banco ao domicílio é um serviço prestado pelas instituições financeiras que proporciona aos seus clientes o «pagamento de serviços e compras, consultas de saldos, carregamentos de telemóveis, transferências de valores» (Azevedo, 2016, pp.96-99). Para além de ser possível a sua utilização em qualquer dispositivo

(telemóvel, computador, *tablet*…), qualquer altura ou lugar, desde que com acesso à *Internet*, conferiu, também, uma "descentralização dos serviços prestados" (Guimarães, 1999 *cit. in* Azevedo, 2016, p.96).

Através do *site* ou de uma *app* fidedigna da instituição bancária, é possível aceder aos serviços bancários de forma segura, uma vez que é disponibilizado um serviço encriptado, com canais de autenticação que apenas o usuário tem acesso. Por sua vez, as instituições bancárias estão encarregues de assegurar a total segurança destes serviços, assegurando-se que no final das operações, estas sejam apenas do conhecimento do cliente. Estas condições foram inicialmente acordadas entre «uma instituição bancária e um cliente», de modo a tornar a experiência do *homebanking*, disciplinada e fiável (Azevedo, 2016, pp.96-99).

No entanto, apesar da encriptação de toda a informação, «tudo é falível, até um *site* bancário» (Azevedo, 2016, p.97). Como referido anteriormente, com o surgimento de novos crimes ligados à tecnologia e ao mundo *on-line*, como o *phishing*[14] e o *pharming*[15], «que tem como alvo principal as instituições de crédito» (Azevedo, 2016, p.97), tem-se notado um aumento cada vez maior destes ataques informáticos. Estas práticas são claramente crimes de burla informática e devem ser julgados como tais.

4.7. Fraude no comércio *on-line*

A *Internet* permitiu que se desenvolvesse uma exposição desmesurada de informação, isto é, através das redes sociais e partilha de informação privada, comentários em artigos *on-line*, subscrição de jornais e páginas *on-line* permite a terceiros ter conhecimento destas atividades (Nunes, 2021, p.12). Estes "terceiros" são, na verdade, empresas que monitoram regularmente os elementos supramencionados, das atividades *on-line* do público geral de modo a criar os chamados «perfis de consumo» (Nunes, 2021, p.12). Este acompanhamento de atividades permite «às empresas dirigir publicidade específica e acabam por gerar um mercado altamente lucrativo para as empresas» e «desenvolver estratégias comerciais muito eficazes» (Nunes, 2021, p.12).

[14] O conceito de *phishing* foi abordado previamente nas páginas 19-20 deste trabalho.
[15] O conceito de *pharming* foi abordado previamente na página 21 deste trabalho.

Contudo, devido à eclosão da pandemia de COVID-19, foi necessário que inúmeras empresas recorressem a estratégias de modo a continuar operacionais e evitar crises ou falências. Uma das estratégias foi apostar no comércio *on-line* e, consequentemente, uma «desinstitucionalização dos tradicionais meios de pagamento» (Rocha, 2004 *cit. in* Azevedo, 2016, p.103). Em virtude da comodidade inerente ao poder de compra a partir de qualquer lugar, através de um dispositivo com ligação à *internet* e «maior pesquisa comparativa», foram abertas portas a novos negócios e oportunidades (Azevedo, 2016, p. 104.

O crescimento do comércio electrónico trouxe um «aumento de fraudes associadas ao *e-commerce*» (Azevedo, 2016, p.104). De acordo com Joel Pereira, o crescimento do comércio *on-line* é freado apenas pela «falta de confiança por parte dos clientes na segurança do sistema quanto aos meios de pagamento» (Pereira, 2001 cit. in Azevedo, 2016, p.104), uma vez que neste género de transações comerciais há três elementos envolvidos: o cliente, o comerciante e a empresa bancária (Azevedo, 2016, p.104).

Não só a operação para efetuar o pagamento é uma vulnerabilidade para o roubo de dados pessoais ou bancários, uma vez que é necessário na maior parte das vezes inserir o número do cartão, código de segurança, entre outros dados; existe também «o medo de ser enganado na hora de comprar através da *Internet*» (Azevedo, 2016, p.105).

5. A dificuldade associada à investigação da burla informática

Os crimes *on-line* possuem características como a «volatilidade, fragilidade, perenidade, dificuldade de acesso (por vezes a informação está cifrada), e dificuldade de atribuir um grau de autenticidade…» (Gouveia *In* Dicionário Crime, Justiça e Sociedade, 2016, pp.125-126), o que dificulta os processos de investigação da polícia. Uma das características que mais complexifica o trabalho da polícia judiciária é o facto de as burlas informáticas e outros crimes através da *internet* serem transfronteiriços: «os crimes praticados no ambiente digital têm suscitado problemas resultantes de imaterialidade (...) a localização física dos agentes não é óbvia (...) (in)determinação jurídica» (Verdelho, 2009 *cit. in* Azevedo, 2016, p.110). Deste modo, a investigação da burla informática ou outros crimes informáticos são de grande complexidade e elaboração, pois requer a cooperação de outros ordenamentos jurídicos e «perícias tecnologicamente rigorosas» (Azevedo, 2016, p.109). Esta cooperação é decorrente de

pedidos que demoram anos a obter resposta, isto quando há resposta. Estes pedidos carecem de uma explicação minuciosa e da delineação de um plano para minimizar o risco de invasão de privacidade de terceiros (Azevedo, 2016, p.108).

Outra particularidade é o atraso a nível tecnológico e informático da Polícia Judiciária, em Portugal, que «não se têm adaptado à internacionalização das redes informáticas» (Pereira, 2001 *cit. in* Azevedo, 2016, p.110) e «as normas substantivas (...) não se coadunam com o caráter transfronteiriço e virtual dos atos praticados na *Internet*» (Pereira, 2001 *cit. in* Azevedo, 2016, p.110). Estes entraves prejudicam, de modo crítico, o andamento dos processos, uma vez que a investigação criminal deve ser «dirigida em tempo real» (Gouveia *In* Dicionário Crime, Justiça e Sociedade, 2016, pp.125-126) levando, consequentemente, a desistências no processo.

Ao nível da investigação propriamente dita, há múltiplos obstáculos que determinam a resolução do caso, como a difícil obtenção de provas digitais, devido à frequente eliminação e/ou alteração dos vestígios da prática de crimes informáticos (Azevedo, 2016, p.110). Além do mais, a quantidade de informação obtida no decurso do processo é geralmente imensa, o que para além de impedir uma atuação em tempo real devido ao tempo que seria dispendido pelos investigadores a analisar os dados, também, seria necessário dispender de «muitos recursos de computação, no espaço de armazenamento e na análise das mesmas e na recolha de elementos determinantes para a resolução do caso» (Azevedo, 2016, p.111).

Destarte, a PGR estabeleceu um Gabinete do Cibercrime de modo a tentar colmatar as falhas sentidas[16] e a secção de Investigação da Criminalidade Informática e de Telecomunicações da Polícia Judiciária é a equipa que está a cargo dos crimes informáticos, em Portugal (Gouveia *In* Dicionário Crime, Justiça e Sociedade, 2016, pp.125-126). Apesar destas implementações para combater a criminalidade informática, é necessário ainda, fomentar a cooperação e apoio entre as autoridades de todos os países envolvidos e proporcionar uma «reeducação» (Azevedo, 2016, p.111) dos OPC ao nível de «cibercrime e de investigação, recolha e preservação da prova digital» (Azevedo, 2016, p.111).

[16] Já desenvolvido na página 15 deste trabalho.

Parte II – Proposta de Estudo

Este projeto intenta abordar como a burla informática é uma prática cada vez mais recorrente no mundo tecnológico em que vivemos e tal como Amador (2018, p.15) no seu estudo sobre o cibercrime, é pretendido «perspetivar o futuro deste fenómeno criminal, sem para isso aspirar a qualquer tipo de futurologia». De modo a compreender o tema proposto, foi pensada a realização de entrevistas a professores/as, da área da criminologia e/ou direito.

Objetivos da investigação

a. Gerais

Compreender porque o número de burlas informáticas aumentou com o eclodir da pandemia de COVID-19.

b. Específicos

i. Abrir um debate sobre a burla informática e os perigos de compras e *apps* de pagamento *on-line*;
ii. Alertar e chamar para o perigo da criminalidade económica *on-line*;
iii. Analisar os pontos de vista de diferentes profissionais em áreas relacionadas ao estudo do cibercrime e da burla informática;
iv. Descobrir que cuidados o cidadão comum pode ter para impedir a vitimação por burla informática;
v. Entender o papel dos criminólogos para prevenir e/ou intervir em caso de crimes de burla informática e outros crimes *on-line*.

Participantes

Professores/as de criminologia e/ou direito.

Método utilizado para recolha de dados

O método utilizado neste estudo será qualitativo. Pretende-se fazer entrevistas a professores/as universitários, de criminologia e/ou direito.

Procedimentos

Em primeiro lugar, será necessário garantir o consentimento informado dos professores a ser entrevistados[17]. Realizados todos os passos para garantir um estudo eticamente legítimo, serão realizadas entrevistas, a partir de um guião estruturado[18], a professores/as das áreas da criminologia e/ou direito, com a duração de cerca de 30 a 40 minutos.

Resultados Esperados

No fim das entrevistas, será feita uma análise e dissecação do conteúdo apurado. É esperado pontos de vista diferentes e um dos objetivos é explorar as discrepâncias e concordâncias de respostas. No fim da análise, pretende-se entender quem pode ser vítima de burla informática e/ou cibercrime e quem poderá ser um possível perpetrador deste tipo de crime que Verdelho (2003, *cit. in* Amador, 2018, p.24), divide em três categorias diferenciadas pelas suas características legais e sócio criminais, «o primeiro onde estão englobados os crimes que recorrem a meios informáticos; o segundo relacionado com os crimes referentes à proteção de dados pessoais e o terceiro que inclui os crimes informáticos propriamente ditos». Para além disso, é ambicionado chegar à conclusão de qual o papel de um/a criminólogo/a na prevenção de crimes informáticos e como intervir nestes casos, uma vez que a criminologia é «uma ciência que "*pretende conhecer a realidade criminal, através da observação e da experimentação. Propõe-se descrever e explicar os comportamentos dos atores sociais*"» (Cusson, 2002, *cit. in* Amador, 2018, p.24). Por fim, pretende-se deduzir quais os aspetos da investigação criminal e na prevenção dos crimes informáticos devem ser alterados ou aperfeiçoados, pois segundo Vera Dias (2010, *cit. in* Amador, 2018, p.30), os investigadores deparam-se com as mais variadas dificuldades: «a falta de legislação adequada; a falta de metodologia no tratamento específico deste crime; a interoperatividade dos sistemas; a lentidão da cooperação e a falta de partilha de informações (quer entre entidades nacionais quer a nível internacional».

[17] Anexo A
[18] Anexo B

Considerações Finais

A execução deste projeto permitiu-me uma visão mais compreendida sobre a relevância do estudo do cibercrime e da burla informática, visto serem crimes com cada vez maior incidência e o seu aumento ser paralelo ao desenvolvimento da tecnologia e da informática, bem como do despontar da pandemia de COVID-19.

É possível concluir que ainda há um grande caminho a percorrer no que diz respeito à prevenção da criminalidade económico-informática e é imprescindível apostar na literacia informática do cidadão comum, assim como, numa modernização e internacionalização dos órgãos de polícia criminal responsáveis pela investigação destes crimes, para haver uma melhor resposta na intervenção. De igual modo, vê-se necessário uma maior cooperação entre as organizações internacionais de modo a combater este mal crescente que coloca pessoas individuais, empresas, países e economias em risco.

Por fim, a proposta apresentada na parte II, tem como objetivo, não combater diretamente o cibercrime, mas contribuir para o debate sobre o mesmo e perceber de que forma podemos contribuir para a instrução informática e alertar para os perigos análogos à *Internet*.

Jurisprudência

- Acórdão 0014449, de 03 de maio de 2001, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7f9f1fe8642dc81580256a7f0036b9d3?OpenDocument [Consultado em: 14/09/2022].
- Acórdão 05P2253 de 06 de outubro de 2005, disponível em: http://www.dgsi.pt/jstj.nsf/-/1E2E4014CF41DC87802570920057EC37 [Consultado em 08/09/2022].
- Acórdão 1318/02 de 15 de maio de 2002, disponível em: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/0fdd0aa4bad15aff80256bcd00475da3 [Consultado em 14/09/2022].
- Acórdão 1462/16.0PCSNT.S1 de 18 de novembro de 2020, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/526b2874eddd6aeb80258685006f0317?OpenDocument&Highlight=0,cibercrime [Consultado em 08/09/2022].
- Acórdão 2039/14.0JAPRT.P1 de 07 de julho de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cffe710b2cb8d91e8025800500475ea9?OpenDocument&Highlight=0,inform%C3%A1tica,cibercrime [consultado em 30/09/2022].
- Acórdão 4395/03.6TDLSB.L1-5, de 29 de junho de 2010, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d1cf18b34be2a7648025777a00492765?OpenDocument [consultado em 01/10/2022].
- Acórdão 471/15.0T9AGD-A.P1 de 13 de abril de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument&Highlight=0,inform%C3%A1tica,cibercrime [consultado em 30/09/2022].
- Acórdão 529/11.5TABGC.P1, de 19 de fevereiro de 2014, disponível em: http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/86a0c32b8287111d80257c9200501b88?OpenDocument [Consultado em 01/10/2022].
- Acórdão 573/14.0T9VLG.P1, de 13 de julho de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/97fbc0f04e943da380258009004b4f7a?OpenDocument [consultado em 01/10/2022].

Referências Bibliográficas

- Alfredo, J. (2013). *Algumas questões referentes ao tipo legal de burla* (Dissertação de mestrado, Universidade Lusófona, Porto). Disponível a partir de https://recil.ensinolusofona.pt/bitstream/10437/4957/1/JOS%C3%89%20ATAN%C3%81SIO%20ALFREDO.pdf
- Amador, N. (2018). *Cibercrime em Portugal. Trajetórias e perspetivas de futuro* (1.ª ed.). Lisboa: Chiado Editora.
- Azevedo, A. (2016). *Burlas Informáticas: Modos de Manifestação* (Dissertação de Mestrado, Universidade do Minho, Minho. Disponível a partir de https://repositorium.sdum.uminho.pt/bitstream/1822/44510/1/Ana%20Helena%20Fran%C3%A7a%20Azevedo.pdf
- Centro Nacional de Cibersegurança (2021). *Boletim Observatório de Cibersegurança*. Disponível a partir de https://www.cncs.gov.pt/docs/boletim-observatorio-setembro2021-1.pdf
- Centro Nacional de Cibersegurança (2022). *Relatório de Cibersegurança*. Disponível a partir de https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf
- Código Penal Português
- Conselho da Europa (2001). *Relatório Explicativo da Convenção sobre o Cibercrime*. Disponível a partir de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b
- Gabinete do Secretário-Geral Relatório (2021). *Relatório Anual de Segurança Interna*. Disponível a partir de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNLI0NgcAIUgtZwUAAAA%3d#page40
- Lei n.º 109/2009, de 15 de setembro (2009). Lei do Cibercrime. Procuradoria-Geral Distrital de Lisboa.
- Maia, R. L., Nunes, L. M., Caridade, S., Sani, A. I., … Afonso, L. (2016). *Dicionário Crime, Justiça e Sociedade* (1.ª ed.). Lisboa: Edições Sílabo.

- Morgado, M. J. e Vegar, J. (2003). *O inimigo sem rosto: Fraude e Corrupção em Portugal*. Lisboa: Publicações Dom Quixote.
- Nunes, D. R. (2021). *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime* (2.ª ed.). Coimbra: Gestelegal.
- Ribeiro, M. (2015). Cibercrime e Prova Digital (Dissertação de mestrado, Instituto Superior Bissaya Barreto, Coimbra). Disponível a partir de https://comum.rcaap.pt/bitstream/10400.26/28946/1/Cibercrime%20e%20Prova%20Digital.pdf#page12
- Serviço Europeu de Polícia (2011). *Europol review: Relatório Geral sobre as atividades da Europol*. Disponível a partir de https://www.europol.europa.eu/sites/default/files/documents/pt_europolreview.pdf
- Simas, D. (2014). *O Cibercrime* (Dissertação de mestrado, Universidade Lusófona de Humanidades e Tecnologias, Lisboa). Disponível a partir de https://recil.ensinolusofona.pt/bitstream/10437/5815/1/Tese%20Cibercrime%20-%20Diana%20Simas.pdf
- United Nation Office on Drugs and Crime. *Cybercrime*. Disponível a partir de https://www.unodc.org/unodc/en/cybercrime/index.html

Anexos

Anexo A – Declaração de consentimento

Eu, _____ (nome completo), declaro que autorizo a minha participação no programa intitulado de "O crescimento da burla informática em contexto de pandemia de COVID-19 em Portugal: Proposta de estudo" desempenhado no âmbito da obtenção do grau de licenciada no curso de Criminologia, na Universidade Fernando Pessoa.

Data: ___/___/___

Professor: _____

O investigador responsável: _____

(Ana Rita Lopes da Silva)

Anexo B – Guião das entrevistas

Questões

1. Qual a sua área e estudo?
2. O que é para si o cibercrime?
3. E a burla informática?
4. Porque é que o número de crimes informáticos aumenta exponencialmente nas estatísticas anuais? Quais os fatores que influenciam esta conduta criminal?
5. Decorrente das questões anteriores, quem considera que se pode tornar uma vítima, quais as características gerais das vítimas de burla informática?
6. Sendo assim, no outro polo da atuação criminal, que tipo de características possui o perpetrador de crimes de burla informática?
7. Considera que existe predisposição para a perpetração de burla informática ou é uma questão de oportunidade? Porquê?
8. A investigação de crimes informáticos é considerada uma tarefa bastante trabalhosa e, por vezes, quase impossível. Quais os aspetos que tornam o cibercrime tão complexo e que elementos devem ser melhorados/mudados ao nível da investigação?
9. De modo a prevenir o crime de burla informática e outros crimes *online*, o que deve ser feito?
10. Por fim, qual considera ser o papel do criminólogo tanto na prevenção, como na intervenção da burla informática?
11. Quer adicionar algo que considere importante ao tema?