O CRIME DA BURLA (ESTELIONATO) ELETRÔNICO: UMA VISÃO LUSO-BRASILEIRA À LUZ DO AVANÇO TECNOLÓGICO

Márcio Roberto Hasson Sayeg

Dissertação de Mestrado em Direito

Especialização em Ciências Jurídico-Políticas

Orientação: Prof. Ana Rita Alfaiate

Setembro, 2021

UNIVERSIDADE PORTUCALENSE

Do conhecimento à prática.

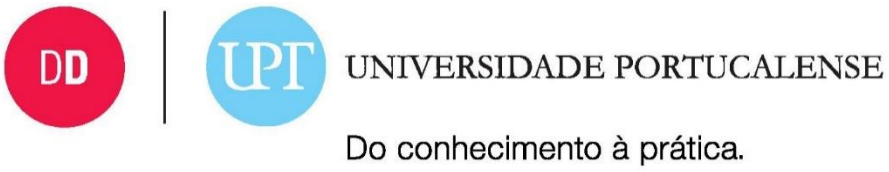
IMP.GE.84.1

Márcio Roberto Hasson Sayeg

O CRIME DA BURLA (ESTELIONATO) ELETRÔNICO: UMA VISÃO LUSO-BRASILEIRA À LUZ DO AVANÇO TECNOLÓGICO

Dissertação de Mestrado apresentada à Universidade Portucalense Infante D. Henrique para obtenção do grau de Mestre em Direito especialização em Ciências Jurídico-Políticas, sob a Orientação da Professora Doutora Ana Rita Alfaiate.

Departamento de Direito
Setembro, 2021



Dedico essa tese de mestrado a todas as pessoas que me apoiaram durante esse processo. A meus pais que sempre me incentivaram a estudar e seguir em frente. A minha família por ser meu alicerce em todas as fases da minha vida. A minha esposa por todo amor, apoio e compreensão em dias turbulentos. Dedico finalmente esse título a todos que estarão presentes em todas minhas próximas conquistas!

AGRADECIMENTOS

Agradeço minha tese de mestrado a meu falecido Pai, que me ensinou tanto e tornou possível a realização deste grande sonho em minha vida.

Agradeço aos professores do mestrado, por todo conhecimento transmitido durante o curso e pela convivência agradável no dia-a-dia.

Agradeço a universidade e quero deixar uma palavra de gratidão por ter me recebido de braços abertos e com todas as condições que me proporcionaram dias de aprendizagem muito ricos.

Agradeço também ao meu irmão, que além de estar ao meu lado em todos os momentos da vida, é o meu melhor amigo e minha inspiração.

Finalmente agradeço a minha esposa e meus filhos, que se fizeram muito presentes em todo o processo de elaboração desta tese, minha cúmplice e meus parceiros.

O CRIME DA BURLA (ESTELIONATO) ELETRÔNICO: UMA VISÃO LUSO-BRASILEIRA À LUZ DO AVANÇO TECNOLÓGICO

RESUMO

O presente trabalho abordou a questão do crime conhecido como burla em Portugal e estelionato no Brasil na esfera tecnológica, a qual conferiu a este tipo de crime um alcance de poder nunca antes visto. Assim, o estudo teve o mérito de ser feito tendo o fato de que milhões (senão bilhões) de pessoas ao redor do mundo se valem do comércio eletrônico, o qual, além de trazer comodidade e agilidade nos negócios online, também abriu novas portas para o crime, dentre eles a burla/estelionato eletrônico, o qual passou a não mais conhecer fronteiras geográficas, além também de novas modalidades para perpetração deste tipo de delito. Assim, o objetivo principal do presente estudo foi o de elucidar as soluções legais adotadas tanto por Portugal como pelo Brasil frente ao crime de burla/estelionato eletrônico. Para tanto, empregou-se como procedimento metodológico a pesquisa em materiais secundários compostos fundamentalmente de teses, dissertações, artigos e monografias obtidos em repositórios acadêmicos, além de livros, leis e jurisprudências aplicados nos 2 países, os quais foram obtidos empregando-se como termos chaves de pesquisa: burla eletrônica, burla qualificada, estelionato eletrônico, estelionato digital, crimes digitais, crimes informáticos, tipificação dos delitos informáticos, frades no ecommerce, restringindo à busca as legislações aplicadas no Brasil e em Portugal. Desta forma, foi possível concluir tanto no Brasil como em Portugal, a modalidade de crime patrimonial ganhou novo fôlego com a era digital, o que se refletiu na quantidade de reclamações feitas em ambos os países, os quais caracterizam esse crime como a obtenção de vantagem ilícita e que causa dano patrimonial perpetrado por meio de engano e meio malicioso e que está no rol dos crimes cibernéticos abertos, sendo considerado um crime material em ambos os países, exigindo-se a produção do resultado e, mesmo que esse seja bem sucedido, precisa também ser denunciado pela vítima. Importante destacar que frente a este ilícito de alcance global, é necessária uma cooperação entre países para a investigação e punição dos criminosos, investigação essa que requer profissionais especializados em cyber segurança e cooperação entre países para que os mesmos sejam extraditados e julgados se for o caso.

Palavras-chaves: burla eletrônica; estelionato eletrônico; fraude; internet.

THE CRIME OF THE SURPRISE / ELECTRONIC ESTELIONATO: A LUSO-BRAZILIAN VISION IN THE LIGHT OF TECHNOLOGICAL ADVANCE

ABSTRACT

This work addressed the issue of crime known as fraud in Portugal and embezzlement in Brazil in the technological sphere, which gave this type of crime a reach of power never seen before. Thus, the study had the merit of being carried out considering the fact that millions (if not billions) of people around the world use electronic commerce, which, in addition to bringing convenience and agility to online businesses, also opened new doors for crime, including fraud/electronic embezzlement, which no longer knows geographic borders, as well as new modalities for the perpetration of this type of crime. Thus, the main objective of the present study was to elucidate the legal solutions adopted by both Portugal and Brazil against the crime of fraud/electronic embezzlement. For that, it was used as a methodological procedure the research in secondary materials composed mainly of theses, dissertations, articles and monographs obtained in academic repositories, in addition to books, laws and jurisprudence applied in the 2 countries, which were obtained using as terms search keys: electronic fraud, qualified fraud, electronic fraud, digital fraud, digital crimes, computer crimes, classification of computer crimes, friars in ecommerce, restricting the search to the laws applied in Brazil and Portugal. In this way, it was possible to conclude both in Brazil and in Portugal, the modality of patrimonial crime gained new breath with the digital age, which was reflected in the number of complaints made in both countries, which characterize this crime as obtaining an advantage illegal and that causes property damage perpetrated through deception and malicious means and which is on the list of open cyber crimes, being considered a material crime in both countries, requiring the production of the result and, even if it is successful, it also needs to be denounced by the victim. It is important to highlight that in view of this global scope, cooperation between countries is needed to investigate and punish criminals, an investigation that requires professionals specialized in cyber security and cooperation between countries so that they are extradited and tried, if applicable.

Keywords: electronic scam; electronic embezzlement; fraud; Internet.

SUMÁRIO

LISTA DE SIGLAS E ABREVIATURAS

ABCOMM - Associação Brasileira de Comércio Eletrônico
ACEPI - Associação da Economia Digital
APAV - Associação Portuguesa de Apoio à Vítima
APED - Associação Portuguesa das Empresas de Distribuição
CC - Código Civil
CP - Código Penal
CPC - Código de Processo Civil
CPP - Código de Processo Penal
DEIC - Departamento Estadual de Investigações Criminais
ECOMMERCE - Comércio eletrônico
ENSC - Estratégia Nacional de Segurança do Ciberespaço
EUA - Estados Unidos da América (
GNR - Guarda Nacional Republicana
IC - Infraestruturas críticas
IDC - *Internacional Data Corporation*
OPC - Órgão de Polícia Criminal
PIB – Produto interno bruto
PJ - Polícia Judiciária
RCM - Resolução do Conselho de Ministros
RGIT - Regime Geral das Infrações Tributárias
RJIFNA - Regime Jurídico das Infrações Fiscais Não Aduaneiras
STJ - Supremo Tribunal de Justiça
TIC - Tecnologia da informação e comunicação
TRF - Tribunal Regional Federal
UNCTAD - *United Nations Conference on Trade and Development*

1 INTRODUÇÃO

O advento do avanço tecnológico ao longo da história e a invenção da Internet no século 20 tornaram a sociedade mais conectada online. Esta ferramenta de integração global está presente em atos do dia a dia, como transações monetárias ou redes sociais. Essa evolução traz muitos benefícios para o homem, incluindo a facilitação na comunicação. No entanto, também abre a possibilidade de praticar muitos comportamentos socialmente inaceitáveis, tornando mais fácil a prática de diversos ilícitos, inclusive com um alcance global.

É aqui que os e-commerces, ou comércios eletrônicos (como são conhecidos em marketing), revolucionaram a forma como os indivíduos e os usuários da Internet compram. Todo o processo e atendimento é realizado virtualmente, o que garante mais comodidade e praticidade ao consumidor.

Refere-se às vendas realizadas por meio de equipamentos eletrônicos, como laptops, tablets, smartphones, telefones comuns, totens e outros aparelhos não estão conectados necessariamente à internet. Todo o comércio realizado via internet pode ser considerado comércio eletrônico, pois requer o uso dos dispositivos acima. Este tipo de comércio também é conhecido como "negócio online".

Nesse contexto, as empresas tiveram que se adaptar às restrições impostas pela pandemia Covid-19. Isso se deveu em parte à adoção do comércio eletrônico, que permite aos consumidores acessar informações de suas casas e de qualquer lugar.

Assim, a população tem aumentado a prática de compras online por meio de sites e aplicativos. Muitas empresas já adicionaram o comércio eletrônico às suas estratégias ou migraram para o comércio eletrônico. O e-commerce traduz-se numa loja virtual que oferece muitas oportunidades e nichos de atuação.

A expectativa é de que essa área cresça por ser grande e oferecer mais comodidade ao consumidor, além de preços mais competitivos. O empreendedor tem muitas vantagens, incluindo alcance global, economia e capacidade de vender 24 horas por dia.

No entanto, os empreendedores virtuais precisam entender de logística para ter sucesso. A logística é um conceito universal. No entanto, a logística de varejo virtual exige muito aprendizado para todos os envolvidos. Isso inclui transportadoras, fornecedores e operadores logísticos, bem como empresas de varejo virtual.

É importante lembrar que a loja virtual estará aberta 24 horas por dia e todos os dias da semana. A loja oferece uma grande variedade de informações, incluindo a localização do produto, identificação, comentários dos clientes e informações sobre

prazos de envio e entrega. Com menos intermediários e prazos de entrega mais curtos, o prazo para produtos e serviços pode ser mais breve.

O comércio eletrônico agora também está disponível para os fabricantes. Direto ao consumidor é o nome desse modelo (D2C) referindo-se a vendas diretas a clientes finais. É também um modelo de venda direta que não requer revendedores ou distribuidores intermediários. O conceito está sendo usado por grandes empresas como Tesla Motors, Nike, Citroen e Apple. Todos eles têm suas próprias lojas online e já estão envolvidos no comércio eletrônico.

No contexto atual, é importante ainda observar que a pandemia da Covid-19 terá um impacto significativo na economia do Brasil. Isso incluirá uma mudança no comportamento do consumidor brasileiro e, com isso, afetará o perfil do varejo nacional. O e-commerce está se consolidando e alcançando novos patamares. Já crescia e ganhou espaço no coração dos consumidores.

De acordo com a ecommerce Brasil (2021), o comércio online brasileiro atingiu uma visitação de 1,49 bilhão em fevereiro. Isso representa um aumento de 21% em relação ao mesmo período do ano passado, segundo a Conversion que compilou o Relatório de E-commerce para o Brasil, indicando que dez segmentos apresentaram um aumento no comparativo anual (ano a ano) de mais de 10%, incluindo Farmácia e Saúde (78,29%) e Alimentos e Bebidas (53,37%), Casa e Móveis (51,89%), Moda (36,6%) e Educação (31,32%) e eletrodomésticos e eletrônicos (25,77%).

Um estudo dos CTT (Correios de Portugal) entre julho de 2020 e setembro de 2020 mostra que o número médio de compras de produtos em Portugal foi de 19,5, aumento de 3,8 em relação ao ano anterior. Acresce que o custo médio de aquisição de cada produto foi de 56,6 euros, aumento de 5,5 em comparação ao ano anterior. O faturamento total atingiu 5 bilhões de euros, indicando que os portugueses passam mais tempo comprando online (BARROS 2020).

Nesse sentido, o estudo *We Are Social da Hootsuite* constatou que em Portugal 69,1% preferiram comprar online a partir de qualquer dispositivo, sendo que 36,1% dos portugueses compraram online através de um dispositivo móvel. Esses dados sugerem que o comércio eletrônico pode crescer neste país, que também é um país plantado à beira-mar. Teremos que esperar e ver o que diz o mesmo relatório em 2022 (SOUZA 2021).

Observa-se, portanto, que o comércio eletrônico tem crescido de forma constante em Portugal, e muitas pessoas já procuram online produtos nacionais. Muitos desses produtos incluem frutas e vegetais, mantimentos e take-away, bem como vinhos e outras bebidas. O comércio eletrônico, especialmente produtos endógenos, pode ser uma forma poderosa de vender produtos de produtores locais. No entanto, isso geralmente

é acompanhado por dificuldades de acesso a atacadistas ou cadeias de distribuição (GRANDE CONSUMO 2020).

Apesar disto, o Procon-SP (2021) no Brasil registrou um aumento de 285% nas reclamações de compras online de 2019 a 2020. Os consumidores apontaram que houve dois problemas principais: atraso na entrega ou não entrega do item, com 70.279 reclamações em 2020, e 19.124 em 2019, respectivamente. Em seguida, veio a cobrança indevida, que foi de 36.221 e 5.605, respectivamente.

Isso também confirmou o Reclame Aqui, que é bastante conhecido no Brasil. De acordo com o site, o problema de não cumprimento dos prazos foi constatado nos prontuários da Reclame AQUI já em abril. Isso coincide com o momento em que a população passou a se isolar em casa. Este tópico teve 68,6% mais reclamações do que o normal em abril de 2019, com 117.734 registradas em abril. No entanto, o maior número de reclamações ocorreu em abril, que também foi o pico das medidas de isolamento. Junho, no entanto, quebrou o recorde de problemas de entrega atrasada. O número de reclamações foi de 231.784, um aumento de 294% em relação a junho do ano anterior (RECLAME QUI, 2021).

Portugal vive uma situação semelhante. Entre 20 de abril e o início do ano, a maior rede social de consumo recebeu 5.688 reclamações sobre e-commerce. Este é um aumento de 144% nas contas em comparação com 2.335 reclamações de 2020. Os setores mais demandados são Tecnologia e Comércio de Moda / Vestuário. De acordo com o Portal da Queixa, os motivos de insatisfação mais frequentes são os atrasos na entrega das encomendas e o mau atendimento (PPLWARE 2021).

De acordo com a ClearSale, consultoria especializada em proteção digital contra fraudes, o número de pedidos realizados em e-commerces aumentou 73,84% em relação a 2019. O aumento da atividade fraudulenta também está associado ao aumento do número de consumidores. O número de tentativas de fraude no comércio online aumentou 53,61% durante o mesmo período (LIMA, 2021).

Também o último estudo global da Juniper Research sobre fraude não fornece dados encorajadores para o comércio eletrônico. O relatório estima que o setor pode perder até US $ 20 bilhões este ano com fraudes no comércio eletrônico. Este valor é superior aos US $ 17,5 bilhões em 2020 (ECOMMERCE BRASIL 2021).

Golpes online em Portugal foram reportados ao Portal da Queixa. Isso é uma média de 20 por dia. 500 milhões de euros é o montante dos danos sofridos pelas vítimas. O Portal da Queixa recebeu 2.745 reclamações sobre golpes online entre 1º de janeiro e 19 de maio. Isso é 24% a mais que as 2.182 reclamações do ano anterior. A não perder, o Portal da Queixa informa que o número de reclamações de scam online aumentou 69% em 2020 em relação aos anos anteriores (PORTAL DA QUEIXA 2021).

De acordo com o portal, 5 tipos de fraude são mais prevalentes no ambiente digital em Portugal: Forex, sistemas de pagamento eletrônico e SMS e e-mails fraudulentos. Além disso, compras online via Facebook e Instagram, e roubo de registros do WhatsApp, são alguns dos principais métodos de fraude.

Assim, o estelionato (no Brasil) ou burla (em Portugal) é uma modalidade de crime patrimonial que ganhou novo fôlego na era digital. É um crime em que o perpetrador engana outra pessoa, causando-lhe prejuízo por meio de vantagens ilícitas. No caso da burla/estelionato eletrônico o que os diferencia é basicamente a elementar do tipo que estipula que o estelionato eletrônico deve ser praticado através do meio informático.

Este estudo foi motivado pelo fato de que a mídia eletrônica trouxe consigo novas oportunidades para os criminosos, embora tenham democratizado o comércio, facilitando e globalizando tanto um como outro.

Devido à vulnerabilidade da vítima e ao fato de ela poder ser contatada pela Internet, é mais comum cometer esse crime. É por isso que as vítimas de crimes digitais têm crescido em número devido aos avanços tecnológicos, ao isolamento social e à falta de educação da população sobre o uso da internet.

Assim, o presente estudo abordou inicialmente do que se trata a comercialização realizada através da internet, num contexto histórico e geográfico, abordando o contexto no Brasil, Portugal e Europa, bem como suas vantagens e desvantagens tanto para a empresa como para o consumidor.

Na sequência, elucidou-se o crime de estelionato no tocante à sua qualificação no Brasil e em Portugal, no qual recebe o nome de Burla, descrevendo como este crime é tratado nos dois países.

Uma vez compreendido o crime do estelionato, adentrou-se na questão dos crimes informáticos propriamente ditos, objetivando esclarecer o seu conceito e suas modalidades, uma vez que este pode se caracterizar por fraude eletrônica, ameaça, incitação ao crime, cyberbullying, calúnia e difamação entre outros. Observou-se também de forma breve a questão da prova nos cibercrimes e os principais óbices na investigação dos delitos informáticos, possibilitando uma visão ampla e fundamentada desta importante questão social.

Por fim, foi abordado a questão do estelionato/burla eletrônica, contextualizando inicialmente a questão da fraude eletrônica e seu regramento legal feito tanto pelo Brasil como Portugal, onde a doutrina engloba como atividades criminosas quatro tipos associados ao ciber crime: em meios informáticos, proteção de dados ou privacidade, crimes informáticos em sentido estrito e os relacionados com o conteúdo, dentre os quais a burla informática foi contemplada como um tipo legal que procurou colmatar as lacunas existentes de punibilidade quando da manipulação informática lesiva.

2 METODOLOGIA

A metodologia adotada foi de natureza qualitativa, empregando no presente estudo a pesquisa bibliográfica. Foram pesquisados materiais em repositórios como o google acadêmico, scielo e Bibliotecas digitais de teses e dissertações que possibilitaram encontrar trabalhos científicos publicados que elucidaram o tema proposto. Além destes, também se pesquisou livros, leis, jurisprudências e sites institucionais tanto do Brasil como de Portugal.

Como termos chaves de pesquisa foram utilizados: burla eletrônica, crime de burla, burla digital, estelionato eletrônico, estelionato digital, ecommerce, internet, Brasil, Portugal, crimes informáticos, crimes digitais, espécies de crimes informáticos, prova nos ciber crimes e fraudes eletrônicas.

3 COMERCIALIZAÇÃO ATRAVÉS DA INTERNET (BRASIL E EUROPA)

Mesmo que a primeira maneira de pensar na obtenção de lucro esteja certamente vinculada com a venda direta, ou seja, em uma relação fornecedor e consumidor, o emprego da *Web* como um meio voltado para o comércio eletrônico possibilitou enxergar inúmeras maneiras de poder adicionar certo valor para um negócio (Dias, 2018).

Esse fato só pôde ser alcançado porque o aparecimento da *Internet* veio com as evoluções tecnológicas, e desta forma, marcou muitos benefícios para os seres humanos, com a mudança de parâmetros voltados para a globalização, possibilitando às pessoas para que as mesmas tivessem uma revolução em suas vidas, tais como, obtenção de consumo, informações, mudanças na maneira de comunicação, dentre outros aspectos (Hyochimoto, 2020).

De fato, nota-se que a popularização da *Internet* também ocorreu através de dispositivos móveis, que possibilitaram um acesso rápido às informações sobre preços, associada à melhoria na experiência de comprar e qualidade dos serviços, que propiciaram um crescimento da transferência para o comércio eletrônico das compras do consumidor (Dias, 2018).

Com base no estudo de Albertin (2010), tem-se que o comércio eletrônico caracteriza-se como um comércio tradicional, ou seja, que ocorre em um ambiente eletrônico que é abundante em tecnologia de informação e comunicação, com o intuito de buscar atender os objetivos de negócios, caracterizado como de baixo custo e de fácil acesso.

Neste instante, deve-se também ter o esclarecimento sobre os termos de Loja Virtual e *E-commerce*, visto que muitas pessoas acabam por confundir o significado desses dois termos. Tem-se que *E-commerce*, com a tradução para o português possui o significado de comércio eletrônico, e se insere no ambiente virtual com o comércio de mercadorias e serviços. Nota-se que a Loja Virtual pode ser vista como uma das maneiras que existem para que ocorra a venda *online*, com a possibilidade de usar as redes sociais, como *Instagram, Facebook*, dentre outras aplicações que possam assegurar um contato com o cliente final (Bernardi, 2021).

Todavia, o termo *E-commerce* é frequentemente confundido com *E-business*, sendo necessário realizar a distinção entre esses dois conceitos. De um lado, o *E-business* pode ser caracterizado como um método mais complexo de transação, visto que o mesmo insere análises de investimentos, mercados, bem como uma análise

macroeconômica minuciosa, e interação com *stakeholders*, ao passo que o *E-commerce* possibilita a venda e compra de serviços e produtos *online* (Vieira, 2019).

Desta forma, nota-se que o comércio eletrônico está associado à atividade econômica que acontece *online* e insere todos os formatos de atividades comerciais, assim como todo o processo *online* relacionado com venda, manutenção, *marketing*, desenvolvimento, entrega e pagamento de serviços e produtos (Godara, 2016). Paralelamente à venda e compra, tem-se que muitos consumidores utilizam como fonte de informações a *Internet* para que seja possível examinar as novidades ou os produtos mais recentes, ou também para comparar preços, antes de realizar a compra em uma loja tradicional ou compra *online* (Khan, 2016). De fato, nota-se que o *E-commerce* redefine, transforma e cria relacionamentos na formação de valor entre indivíduos e organizações e dentre organizações (Chanana & Goele, 2012).

Tem-se que o *Marketplace* consiste outro método que pode ser empregado nas vendas, ou seja, esse método representa plataformas que têm toda a estrutura adequada para que haja a venda de produtos, isto é, torna-se possível iniciar as vendas sem que exista a necessidade de desenvolver um aplicativo ou *site*; no entanto, com relação ao aspecto negativo, há disputas do produto publicado com a presença de inúmeras outras marcas que usam a mesma plataforma, tais como: Lojas Americanas; *Walmart*, e Mercado Livre (Bernardi, 2021).

Com base no estudo de Kotler (2017), nota-se que os clientes se sentem com autonomia na economia digital, visto que é mais fácil para eles fazer uma avaliação, bem como detalhar a promessa relacionada com o posicionamento da marca de toda organização. Diante deste panorama, nota-se que as empresas que pretendem investir ou investem no comércio eletrônico devem desenvolver um vínculo próximo com seus clientes, e sempre buscar um diferencial de competição que possam destacar essas empresas no mercado concorrente, fazendo com que seus lucros e vendas aumentem (Diniz, Souza, Conceição, & Faustini, 2011).

Então, torna-se um imenso desafio para as empresas que as mesmas tentem compreender esse novo perfil de consumidor, visto que essas empresas desejam estar integradas ao mercado digital, assegurando a qualidade dos serviços que são fundamentados em fatores essenciais, como confiabilidade, usabilidade do *site*, entrega, atendimento e pós-venda.

De acordo com o estudo de Chaffey (2013) neste sentido, o mesmo pôde explicar que é relevante que haja um entendimento por parte dos gerentes do *E-business* sobre os distintos fatores que podem afetar a maneira pela qual muitas pessoas fazem o uso ativo da *Internet*, o modo pelo qual as ações podem ser tomadas para que algumas dessas barreiras possam ser superadas. Assim, verifica-se que as empresas devem

agir rapidamente frente às oportunidades e ameaças associados com esse novo ambiente de negociações.

Logo, tem-se que o comércio eletrônico pode ser caracterizado como um crescente e relevante segmento de transações de mercadorias pela *Internet*, tornando-se o gerenciamento do serviço logístico como uma distinção relacionada à vantagem competitiva, fornecendo uma base para as atividades que são realizadas pelas organizações que possuem uma atuação nesse setor (Bornia, Donadel, & Lorandi, 2006).

3.1 CONTEXTO HISTÓRICO

De fato, tem-se que ao final da década de 1970, apareceu a ideia de comércio eletrônico. De forma distinta ao modelo vigente, a prática desta época possibilitava que as empresas somente mandassem ordens de compra, ou seja, sendo caraterizado apenas como um serviço de mensagens. Todavia, o inventor inglês Michael Aldrich, no ano de 1979, fez uma adaptação em uma televisão de 26 polegadas, e desta forma a personalizou para estar vinculada a um computador doméstico, realizando transações com uma linha telefônica. Então, com os serviços disponibilizados na década de 1980 para os usuários domésticos de *Internet*, nota-se que a *CompuServe* pôde disponibilizar o *Eletronic Mall*, ou seja, um *site* em que diversas mercadorias estavam disponíveis em um catálogo, e possibilitava o envio de *e-mails* para solicitar a compra de produtos no conforto do lar, seria como um *shopping* virtual (Nakamura, 2011).

Diante deste panorama, também pôde ser complementado por Bernardi (2021) que no início de 1980, o cartão de crédito foi aceito, visto que a empresa *CompuServe* (anteriormente citada) pôde disponibilizar o primeiro serviço de *shopping* virtual, em que o usuário poderia realizar a compra de produtos. Com a criação do navegador *World Wide Web*, verificou-se que houve um dinâmico e rápido acesso por parte dos usuários, apresentando uma interface simples, e essa foi a invenção do pesquisador Tim Berners-Lee.

Por outro lado, existem algumas teorias que informam que o comércio eletrônico apareceu no ano de 1888 pela Sears, uma empresa norte americana de relógios. O princípio fundamental sugerido pela empresa estava voltado para a venda de produtos a distância. Pelo telégrafo chegavam as encomendas, depois que os consumidores haviam feito as escolhas de seus produtos no catálogo da empresa (Silva, 2017).

De todo modo, tem-se que a disponibilidade de proliferação de redes locais, modens, computadores pessoais e padrões abertos relacionados com o domínio público, que foram presenciados durante a década de 1980, puderam representar o adequado cenário para que a *Internet* tivesse um crescimento astronômico ao longo da

década de 1990, atingindo milhões de indivíduos, principalmente depois da *World Wide Web*, que se tornou popular depois de 1994. De forma natural, houve um interesse por parte das empresas, e muitas pessoas se perguntavam: enfim, como será possível ter lucro com a *Internet*? (Pereira, 2018).

Diante deste contexto, as gigantes *Amazon* e *E-bay* começaram a desbravar o caminho do comércio eletrônico para o total êxito ao longo da segunda metade da década de 1990 (Nakamura, 2011).

De fato, nota-se que *E-bay* e *Amazon* foram justamente essas empresas que disponibilizaram em seus *sites* um campo de busca, o que não estava presente nas outras lojas, assegurando e facilitando que o cliente pudesse encontrar o que estava procurando. Tem-se que surgia uma lista de produtos depois de realizar a busca, e então o usuário poderia realizar a compra de qualquer produto que estivesse disponível. Nos dias atuais, há integrações voltadas para os serviços que usam a postagem de produtos, fazendo com que a satisfação do cliente aumente. Jane Snowball, no ano de 1984, foi no mundo, a primeira pessoa que realizou uma compra pela *Internet* (Bernardi, 2021).

Deve-se também ressaltar que no princípio, a concepção deste tipo de comércio estava voltada para operações de transações comerciais. Ao longo do desenvolvimento desses serviços, tornou-se plausível fazer uma análise de que existiam enormes vantagens em empregar meios eletrônicos para realizar a compra de serviços e produtos pela *Internet*, especialmente ampliando o emprego de plataformas para que fosse possível fazer o pagamento *online* (Bernardi, 2021).

3.2 BRASIL

Com o crescimento da popularização do uso da *Internet* e de cartões de crédito, apareceram as plataformas de compras *online*, e desta forma, nasceu o *E-commerce.* Tem-se que o *E-commerce* apareceu no Brasil depois que houve a popularização da utilização da *Internet* comercial. Lojas Americanas, Grupo Pão de Açúcar, Submarino foram os pioneiros em vendas neste formato *online* (Dutra, 2011).

Diante este panorama, tem-se que o comércio eletrônico pôde inicialmente se difundir nas transações financeiras, mas durante a década de 1990 foi conquistando o interesse do público, e verifica-se que há uma estimativa de que o *E-commerce*, com o formato que é visto nos dias atuais, apareceu por volta de 1995. Com base no *Internacional Data Corporation* (IDC), tem-se que, desde a década de 1990, o Brasil mantém a posição dentre os 20 maiores usuários de *Internet* no mundo (Diniz, 2019).

No ano de 2013, verifica-se que as empresas de varejo *online* no Brasil tiveram um faturamento de R$ 28 bilhões, superando em mais de 20% as receitas que haviam

sido constatadas em 2012. De fato, a questão que se destaca mais está vinculada com a evolução da última década, tendo em conta que este tipo de comércio no ano de 2003 apresentava um valor em torno de R$ 1,18 bilhão (Ecommerce, 2014). Dados relacionados com esse setor mostram que em 2014, as compras *online* puderam movimentar aproximadamente R$ 35 bilhões, mostrando assim um aumento de 24% quando comparado com 2013 (Ebitempresa, 2015). Por outro lado, tem-se que o faturamento deste setor em 2015 foi de R$ 48,2 bilhões, um valor um pouco abaixo referente às previsões que haviam sido feitas por alguns especialistas, que faziam uma projeção de que as compras relacionadas com essa modalidade poderiam superar os valores de R$ 49 bilhões (Associação Brasileira de Comércio Eletrônico, 2015).

Com base no Ebit (2017), nota-se que o *E-commerce* esteve na contramão da crise no Brasil em 2016, com um faturamento de R$ 44,4 bilhões, um aumento de 7,4%. Ademais, cerca de 48 milhões de consumidores brasileiros, isto é, 1/4 da população do Brasil, realizou compras pelo comércio eletrônico ao menos uma vez por ano, apresentando uma alta de 22% quando comparado com o ano de 2015.

Verificou-se que houve em 2017, 111,2 milhões de pedidos realizados no *E-commerce*, quando comparado com 106,3 milhões realizados em 2016, um aumento de 5%. Houve uma ampliação do ticket médio por consumidor, ou seja, passou de R$ 418 no ano de 2016, para R$ 429 em 2017, um crescimento de 3% [...]. De fato, houve um aumento de 12% relacionado ao comércio eletrônico em 2017 quando comparado com 2016. Destacou-se por outro estudo, o E-commerce Radar 2017, que foi realizado pela Atlas, empresa que possui apoio da Associação Brasileira de Comércio Eletrônico (ABCOMM) e atua com análise de dados. Pôde ser relatado pelo radar *Webshoppers* que o volume de consumidores ativos no Brasil ultrapassou em 2016 os valores de 47,93 milhões, para 2017, 55 milhões, um crescimento de 15%. Consideram-se como clientes ativos aqueles consumidores brasileiros que fizeram pelo menos uma compra digital por ano.

Deve-se destacar um relevante adendo realizado no estudo de Antoniazzi, Novak e Fernandes (2020), em que se identificou que 70% dos negócios não conseguem realizar uma venda de mais de 10 produtos ao mês, mesmo com esse faturamento e crescimento exponencial e expressivo. Este fato acarretou o fechamento de parte das empresas antes que as mesmas pudessem completar três meses de operação.

Mesmo assim, de acordo com o Ebit (2019), notou-se que o *E-commerce* possui apenas 25 anos de chegada no Brasil. Torna-se frequente o processo relacionado com o crescimento, bem como um prestígio mais elevado a cada ano para as empresas que apresentam a divulgação de suas marcas em *sites* de *E-commerce*. Devido a isso, são

visíveis os lucros obtidos ao utilizar esses sistemas, bem como cada vez mais essenciais o acompanhamento e renovação tecnológica.

Nota-se que o comércio eletrônico tem crescido a cada ano, mesmo sob efeitos do desempenho negativo da economia do Brasil. De acordo com dados da ABCOMM (2019 como citado em Carvalho & Silva, 2020), nota-se que o *E-commerce* apresentou um crescimento de 8% para o ano de 2019, com um expressivo aumento de 47,7 bilhões em 2017, e de 61,9 bilhões referentes ao total de vendas. O fato associado com o aumento do *E-commerce* no Brasil está vinculado ao crescimento do número de pedidos.

Logo, tem-se que o comércio eletrônico no Brasil, por ter o acompanhamento da tendência mundial, atrai muita a atenção dos investidores, atraindo-os cada vez mais. Justifica-se esse movimento visto que esse setor tem a possibilidade de disponibilizar ótimas oportunidades de negócios, de maneira independente da área em que se pretende atuar. Encontrar um nicho que seja caracterizado como um potencial de desenvolvimento faz parte do segredo, e evidentemente, ter organização para ter uma competitiva loja virtual (Guimarães, 2018).

3.3 EUROPA E PORTUGAL

Nota-se que na Europa, a evolução do *E-commerce* pôde mostrar que existe um domínio no mercado referente ao *E-commerce* nos países da Europa Ocidental, apresentando aproximadamente 68% do valor de negócios totais (Eurocommerce, 2018). Com base neste mesmo estudo, tem-se que o destaque para este mercado fica para o Reino Unido que gerou uma quantidade de negócios de aproximadamente 178 mil milhões de euros, e em segundo lugar ocupa a França (93,2 mil milhões de euros), e posteriormente a Alemanha (93 mil milhões de euros) (Vieira, 2019).

De acordo com uma entrevista realizada para um jornal virtual, ou seja, o Jornal Virtual Público, tem-se que a diretora Ana Isabel Trigo de Morais, diretora-geral da Associação Portuguesa das Empresas de Distribuição (APED), destacou que o "momento que vivenciamos é uma etapa de *going* digital", apresentando os números que foram reunidos pelo Eurocommerce. De fato, tem-se que o *E-commerce* apresentou um faturamento de mais de 350 milhões de euros ao longo de um ano, e percebe-se que um em cada dois consumidores na União Europeia (EU) faz compras *online*. E nota-se que também em Portugal existe esta tendência em acompanhar o meio digital, conveniência, preço, bem como a adaptação às necessidades relacionadas com o consumidor que está se tornando cada vez mais evidente, a mesma destacou (Silva, 2015).

Diante deste panorama, tem-se que a *Amazon* se mostra como a principal protagonista pelo aumento na Europa do *E-commerce*, com a presença de mais de 20 anos de experiência nesta área, e cada vez mais essa empresa procura pela diversificação de seus serviços, visto que ao adquirir a cadeia *Whole Foods* no ano de 2017, possibilitou a entrada da *Amazon* no mercado *online* de *groceries* (Vieira, 2019).

Referente ao comércio eletrônico, nota-se que Portugal tem tido um expressivo crescimento, acima da média na UE. Com base em um estudo relacionado com o *E-commerce* B2C que foi realizado pela *E-commerce Europe Association* e posteriormente divulgado pela Associação do Comércio Eletrônico e da Publicidade Interativa (2016), verifica-se que houve um crescimento de 15,7% em Portugal referente ao comércio eletrônico para o ano de 2015, e quando comparado com o ano anterior, a média na UE era somente de 13,3%. De fato, tem-se que esse relatório indicou que 70% dos portugueses utilizam a *Internet* (cerca de 6,1 milhões de indivíduos), ou seja, dentre os 8,7 milhões de portugueses que possuem uma idade superior a 15 anos. Neste cenário, nota-se que 3,5 milhões de pessoas podem ser classificadas efetivamente como compradores *online* (cerca de 35%). Dentre as categorias de produtos que foram mais comercializadas podem ser destacadas “Eletrônica e Telemóveis”, posteriormente “Brinquedos e Bebês”, “Decoração, Arte e Mobiliário” e por fim “Informática” (Ponceano, 2018).

Com base em um estudo que foi realizado pelo *E-commerce* na Europa, existe uma estimativa de que em Portugal, o *E-commerce* registrou um aumento anual de 8% para o ano de 2016, quando comparado com o ano de 2015 – e até o presente momento novos inquéritos não foram desenvolvidos – mas com a presença de um total de 3,5 mil milhões de euros, Todavia, a mesma maturidade não havia sido alcançada por Portugal quando se compara com outros países da UE (A. Freitas, 2017).

Com relação ao uso da *Internet* em Portugal, e também de acordo com um estudo feito pela Associação da Economia Digital (“ACEPI”) em 2017, nota-se que a percentagem de portugueses nesse ano que usava a *Internet* representava 73%, e estima-se que esse uso aumente para 91% da população em 2025, mostrando que o uso da *Internet* será caracterizado como mais transversal a cada momento, e para qualquer geração. Referente ao nível de compradores *online*, registra-se igualmente um aumento durante os últimos anos, com uma previsão de que 59% da população de Portugal efetuará compras *online* em 2025. Também com base neste mesmo estudo, nota-se que 85% dos portugueses que realizam compras *online*, também realizaram compras em *sites* internacionais (Vieira, 2019).

Para o ano de 2017, verificou-se que houve um aumento no número de pessoas que faziam compras *online*, um crescimento de 36%, ou seja, um em cada quatro

usuários de redes sociais faziam as compras por essas plataformas, e a plataforma eleita é o *Facebook*. De fato, tem-se que os consumidores preferem utilizar essa tecnologia para poder ter uma interação com as marcas ao longo de todas as etapas de compra, e também procuram mais frequentemente por experiências *online*, bem como usam aplicações vinculadas com estilos de vida, culinária, bem-estar, ecologia, saúde e nutrição. De acordo com o Instituto Nacional de Estatística, nota-se que 80% das famílias em 2017 estavam com acesso à *Internet* (Marian, 2018). Entretanto, esse número foi superior no mesmo período ao que havia sido encontrado pela ACEPI.

Além disso, tem-se que os resultados referentes à uma análise da comScore e Mediapost, realizada em junho de 2017, revelou que o país da Europa em que os usuários passam mais tempo *online* foi Portugal, apresentando uma média de 13h por mês. Nota-se também que o comércio eletrônico teve a quarta colocação referente aos conteúdos que foram mais procurados na *Internet*, isto é, um alcance de 63%. O grupo retalhista que possui mais popularidade dentre os portugueses é a *Amazon*, com o número de visitantes em 800 mil em março de 2017, em seguida tem o *site* Alibaba, com 500 mil, e em terceiro lugar está o grupo Fnac, com 400 mil visitantes. Classificados como outros têm: IKEA; Continente; *Worten; Lightinthebox; e-Bay* e *Followprice* (Carvalho, 2018).

Com relação aos produtos que tiveram uma venda maior *online* pelos consumidores de Portugal podem ser destacados: acessórios de moda e vestuário (49,6%); acessórios e equipamentos móveis (47,8%); equipamentos de informática (35,1%); livros (30,6%); cosmética e perfumaria (26,0%); eletrodomésticos (13,9%); brinquedos (12,2%); bens alimentícios (11,8%), e para finalizar *softwares* e filmes (8,5%). Neste mesmo estudo que teve a divulgação pela ACEPI, tem-se que os serviços mais procurados foram os seguintes: jogos *online* (18,4%); aplicativos para mobile (15,2%); *software* (13,5%); música *online* (11,6%); também os *ebooks* (9,8%); formação a distância (8,7%), revistas e jornais digitais (7,5%); e por fim plataformas de *streaming* e vídeos *online* (7,3%) (Vieira, 2019).

Verificou-se que Portugal, no ano de 2018, registrou que 34% da população residente apresentando uma idade na faixa de 16 a 74 anos estavam usando a *Internet* para realizar encomendas de serviços ou produtos (Carvalho, 2018). Desta forma, tem-se que o comércio eletrônico referente a Portugal (B2B + B2G + B2C) aumentou expressivamente ao longo de 2018, atingindo o valor de 87,5 mil milhões de euros. De fato, nota-se que esses valores relacionados ao mercado de Portugal estão apresentando 2,1 pontos percentuais ainda abaixo da média da UE, mesmo com o aumento no número de portugueses que esteja fazendo compras *online* (ACEPI, 2019).

Verifica-se que esse valor compreende mais do que o dobro quando comparado com o início da década, quando o mesmo era de 15% em 2010, Mesmo com esse expressivo crescimento, tem-se que a posição de Portugal ainda estava abaixo da média na UE referente às compras *online*. Constatou-se que 76% tiveram acesso à banda larga em 2017.

Por outro lado, para o ano de 2019, nota-se que a evolução em Portugal com relação às compras pela *Internet* não apresentou muitas mudanças, de acordo com o gráfico abaixo:

Gráfico 1 – Parcela da população que comprou online durante os últimos 12 meses de 2019

Fonte: Ntech (2020).

Verifica-se que na UE o comércio eletrônico está em crescimento; no entanto, em todas as geografias não existe uma tendência com o mesmo ritmo. Referente às compras pela *Internet*, tem-se que Portugal permanece em última posição na UE, com base nos números que foram disponibilizados pelo Eurostat (2019). De acordo com esses números, tem-se que Portugal, 39% da população realizam compras pela *Internet*, média muito inferior à 60% na Europa, bem como aos números alcançados

pelo Reino Unido (87%), Dinamarca (84%), ou mesmo para a Suécia (82%), que permanecem nas primeiras colocações (Ntech, 2020).

Também com base na pesquisa por idades, nota-se que os maiores fãs relacionados com as lojas *online* compreendem a faixa de 25 a 34 anos, faixa em que está presente 79% da população que compram pela *Internet*. O segundo grupo compreende os usuários na faixa de 16 a 24 anos, representando 73% dos compradores *online*, e o terceiro grupo, com apenas dois pontos percentuais abaixo compreende a faixa de idade de 35 a 44 anos (Ntech, 2020).

Houve melhora nos índices de Portugal em 2020, mesmo com valores abaixo da UE, tais como: Portugal (44,8%); seguido de Chipre (46,4%); e depois Romênia (59,4%). Em resumo, 43% dos portugueses usam o computador para fazer compras pela *Internet*, ao passo que somente 33% compram através de um dispositivo móvel.

Diante deste contexto, tem-se que o trabalho de Teixeira (2020) pôde explicar que existem em Portugal certos constrangimentos com relação à evolução e desenvolvimento do *E-commerce*, tais como:

- Infraestrutura associada aos espaços comerciais. Com base no CBRE, nota-se que a oferta comercial em Portugal compreende uma fase adulta, e verifica-se que a densidade de centros comerciais está com um valor acima da média da Europa (0,27m2 por habitante em Portugal vs. 0,19m2 na Europa), que associado aos horários ampliados ao longo de todos os dias da semana possibilita um sentimento de conforto para as pessoas poderem comprar em seus espaços físicos;
- Logística. Para muitos portugueses, nota-se que existe uma fraqueza no país relacionada com as horas de suas encomendas e entrega a tempo, mesmo sem grandes problemas. Existem problemas mais expressivos como desempenho do serviço postal no chamado “interior”, caracterizado como assimetrias regionais. Conforme conhecido por todos, a logística compreende um dos setores mais importantes relacionados com esse processo, sendo um vital ponto para que haja o desenvolvimento da economia digital de Portugal. Tem-se que os CTT puderam admitir que houve falhas em todos os 24 objetivos associados com a qualidade de serviço que foram demandados pela entidade reguladora em 2019. Também houve o reconhecimento de que apresentou responsabilidades no setor operacional que acabou por prejudicar a qualidade do serviço, proporcionando o não andamento dos objetivos. Como nos casos de férias de Natal e de Verão ou mesmo constrangimentos relevantes no transporte aéreo para as regiões autônomas de Madeira e Açores, e também entre

as ilhas, principalmente a falta de transportes alternativos e infraestruturas a partir da data do mês de abril de 2019 em Açores. Consequentemente, após a realização do estudo “B2C E-Commerce Index”, que foi elaborado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento, em inglês *United Nations Conference on Trade and Development* (UNCTAD), em que se pode verificar que Portugal possui uma posição desfavorável, ocupando o 43º lugar dentre 152 países, por causa do critério de avaliação associado ao “Índice de Confiabilidade Postal”;

- Capacidade de Inovação. Há uma limitação para a capacidade de ter investimento em inovação devido à necessidade de alocar recursos destinados para outras atividades e à falta de escala;
- Literacia Financeira e Digital. O consumidor de Portugal possui alta iliteracia financeira e digital, representando um obstáculo efetivo para o crescimento do uso da *Internet* e para o desenvolvimento do *E-commerce*;
- Consumo de dados. Um alto custo vinculado à uma atual política de fidelização (duração de 24 meses) e ao consumo de dados móveis presentes em comparação com outros mercados na Europa ou ainda com outras economias emergentes, como o Brasil;
- Pagamentos *online*. Realizar compras *online* não é seguro para muitos portugueses. Inclusive, nota-se que a desconfiança está relacionada com um dos entraves mais expressivos para o pagamento *online* em Portugal. De fato, são ainda pouco numerosos os *e-shoppers* que acreditam que seus dados não são compartilhados sem autorização e que as lojas *online* conseguem proteger esses dados. Ademais, nota-se que há um significativo atraso na adoção e disponibilização em Portugal de formas de pagamentos que sejam mais usadas em transações digitais em um nível internacional. Mesmo com a presença de alternativas digitais (como cartões *contactless*, MB Net, MB Way), verificou-se que somente em 2019 chegaram em Portugal os seguintes serviços: *Apple Pay; Samsung Pay; Google Pay* e *Amazon Pay;*
- Retenção e Captação de Talento. Muitas empresas de Portugal não conseguem encontrar talentos em qualidade e quantidade suficientes para desempenhar as funções de informática, tecnologia e engenharia. De acordo com dados da Comissão Europeia, houve uma defasagem entre as necessidades das empresas e talento disponível nos últimos cinco anos, com um aumento de 14%, equivalente à procura de 15.000 postos de trabalho que não possuem a oferta correspondente em Portugal;

- Para a maioria das empresas, permanece como uma realidade não ter a disponibilização de um *site* otimizado. De fato, nota-se que muitos *sites* não estão preparados para aceitar pagamentos que podem ser realizados pelo dispositivo móvel ou não estão otimizados para os *smartphones*. A questão sobre esses *sites* não serem *user-friendly* faz com que haja uma dificuldade para pesquisar pelo objeto pretendido, imagens, características ou mesmo falta de atualização de *stocks*, falta de contato (muitos centrados somente no formulário de contato), não adoção de ferramentas que possam ter uma interação ao vivo para auxiliar os consumidores, tais como *LiveChat*, dentre outros pontos;
- Nota-se que muitos portugueses fazem compras fora de Portugal, visto que não existe uma diversidade no país de oferta suficiente, paralelamente ao fato de ser menos custoso comprar no estrangeiro. Com relação ao volume de compras que são realizadas em *sites* estrangeiros, nota-se que Portugal tem a posição de segundo maior país da UE referente a esse volume. Para a oferta, existe um problema associado com a falta de *sites* suficientes. Com base em um trabalho realizado pela "Economia Digital 2018", tem-se que Estados Unidos da América (EUA), Reino Unido, Espanha e China abarcam as preferências associadas com os *e-shoppers* nacionais. De forma curiosa, nota-se que o *site* AliExpress compreende a loja *online* onde os portugueses mais compram atualmente, principalmente os produtos com menor custo.

Deve-se destacar o papel do comércio *online*, especialmente, com relação à vida do dia a dia dos portugueses, desta forma facilitando a estratégia de viver, recriar, trabalhar espaços, que concordam com o tempo condicionado, com a liberdade de estar e ser, com uma transformação constante, sem deixar de pontuar a concepção do risco que possuem (Rocha, 2019).

De acordo com o estudo associado com publicidade Interativa/ *Analyse the future* [ACEPI/IDC] e a Associação de Comércio Eletrônico, pode-se prever um crescimento robusto do *E-commerce* referente ao B2C e B2B em Portugal até o ano de 2025, isto é, com um significativo impacto no PIB de Portugal.

Deste modo, tem-se que o comércio eletrônico conseguiu transformar de maneira rápida a forma como é feita a interação dentre as empresas, assim como com outros agentes econômicos. Sobretudo, trouxe mudanças significativas para os consumidores, sendo responsável também pelo crescimento do emprego e economias (Kumar & Nagendra, 2018).

Para essa finalidade, tornou-se essencial o papel referente às tecnologias de informação. A frequente utilização de *tablets, smartphones,* e também da *Internet*, associada à uma confiança maior do consumidor, fez com que houvesse um crescimento do comércio eletrônico de maneira extraordinária (Waghmare, 2012; Khan, 2016). O crescimento e desenvolvimento rápido da *Internet* transformaram as economias dos dias atuais, e facilitaram os negócios (Ray, 2011; Godara, 2016). De outro ponto de vista, houve um aprimoramento da experiência de compra dos clientes, das vendas, bem como melhora nos processos relacionados aos negócios e ao comércio eletrônico (Pecenec & Zoroja, 2018).

Com base nos estudos de Vikram (2012), nota-se que os avanços associados às tecnologias de computação e telecomunicações nos últimos anos fizeram com que as redes de computadores se tornassem uma parte integrante e fundamental para a infraestrutura econômica. Assim, tem-se que o comércio eletrônico assumiu a posição inegável de uma importante parcela em nossa sociedade (Shahriari, Shahriari, & Gheiji, 2015), caracterizado como um dos fatores mais relevantes para a globalização dos negócios (Smith, 2011).

3.4 CARACTERÍSTICAS GERAIS

Com relação aos trabalhos de Shahriari et al. (2015) e Khosla e Kumar (2017), tem-se que as categorias ou tipos principais de comércio eletrônico são: Consumer-to-Consumer (C2C); Consumer-to-Business (C2B); e Business-to-Business (B2B). O C2B compreende um modelo de negócios em que as empresas consomem o valor desenvolvido pelos consumidores, e em que esses consumidores criam valores. Para o B2C, este modelo consiste em um tipo em que se realiza uma transação diretamente entre consumidores finais e empresas. E por fim, o B2B representa uma transação comercial dentre empresas (retalhistas ou comerciantes, produtores ou fabricantes, armazenistas ou grossistas) em que se fundamenta o preço na quantidade de pedidos, sendo usualmente negociável.

Nota-se que o modelo que é caracterizado como “leilão” possibilita aos compradores que os mesmos possam exigir ou nomear um preço, para um serviço ou bem específico, que normalmente estão associados. Então, o C2C, que compreende uma transação que é feita de cliente para cliente, engloba a facilidade do ambiente pelo negócio, em que os clientes têm a possibilidade de vender esses serviços e/ou bens uns com os outros (Ribeiro, Fernandes, & Lopes, 2019).

Diante deste contexto, pôde ser explicado pelo estudo de Ascenção (2016) que os negócios B2B possibilitam milhares ou centenas de transações, seja como fornecedores ou como clientes. Colocar em prática essas transações feitas

eletronicamente propicia enormes vantagens competitivas quando comparada com os métodos tradicionais. Quando são empregadas eficientemente, nota-se que o *E-commerce* é mais conveniente, barato e rápido ao comparar com os métodos tradicionais referentes às transações de serviços e bens.

Paralelamente à essas categorias, o estudo de Turchi (2018) mostrou que o comércio eletrônico ainda pode ser classificado como:

- B2C - *Business to Consumer*: que consiste em um modelo amplo de negócios por inserir um perfil variado voltado para as transações diretas pela *Internet* entre os consumidores finais e a companhia/organização. Assemelha-se esse segmento às lojas que realizam através de catálogos uma venda direta com o consumidor, e essas lojas tipicamente se apresentam na *Internet* como lojas virtuais, da mesma forma como em modelos de shoppings virtuais e leilões, que funcionam de maneira similar aos shoppings tradicionais, em que as lojas pagam taxa de condomínio, e em que diferentes lojas vendem seus produtos;
- B2G - *Business to Government*: pode-se definir como atividades comerciais *online* que são realizadas entre empresas governamentais e privadas;
- B2I - *Business to Institutions*: associa-se às atividades comerciais *online* entre instituições (associações, educacionais...) e empresas;
- B2E - *Business to Employee*: representa um modelo de comércio eletrônico em que os produtos ou serviços são vendidos pelas empresas para seus funcionários;
- *E-procurement*: compreende um tipo de comércio eletrônico empregado pelas empresas para que seja realizada a compra de suprimentos, tais como: materiais de limpeza, higiene, escritório, dentre outros.

Mesmo com o exponencial crescimento, conforme descrito anteriormente, nota-se que não é uma tarefa simples abrir um *E-commerce*, visto que para abri-lo demanda um pouco de dinheiro, planejamento e tempo. Com base no estudo de Chaussard (2015), há três dimensões essenciais relacionadas com uma atividade de sucesso no *E-commerce*: comunicação; tecnologia; e negócio. Quando o tema negócio é abordado, o mesmo se refere ao planejamento dos processos de embalagem, desenvolvimento do modelo de negócio, escolha do produto e de como a parte logística será trabalhada, dentre outras atividades.

Com relação à tecnologia, a mesma se refere à plataforma de *E-commerce*, isto é, à plataforma/ferramenta que poderá fornecer o suporte para os processos operacionais do dia a dia da loja *online* (Silva, 2017).

Sobre a comunicação, a mesma se relaciona com o emprego de *inboud marketing,* redes sociais, *links* patrocinados, dentre outros. Pode-se caracterizar como os meios/canais que farão com que o endereço do *E-commerce* seja conhecido pelo público. Logo, nota-se que o negócio compreende a base do empreendimento voltado para o *E-commerce*, quer seja originário ou novo de loja física. Por outro lado, a comunicação e tecnologia propiciam condições para que o negócio seja rentável, e que o mesmo seja viabilizado (Silva, 2017).

3.5 VANTAGENS

Verifica-se que o comércio eletrônico pode ser caracterizado como um agente em potencial para aperfeiçoar os processos Inter organizacionais, com a presença de positivos reflexos para que haja uma competitividade organizacional. Nota-se que tem existido uma rápida expansão do acesso à *Internet*, fornecendo ao comércio eletrônico uma positiva perspectiva para crescer em longo e médio prazo, à proporção que os consumidores possam mudar seus hábitos, e desta forma adquirir confiança para que os mesmos possam realizar compras pela *Internet*, e também ao passo que as empresas possam adquirir competência para poderem ter uma atuação neste canal (Bornia et al., 2006).

Verifica-se que as vantagens podem se refletir no aumento das compras *online*, tanto para vendedores quanto para compradores, visto que essa venda fornece para lojas tradicionais ou físicas, um alcance maior de mercado, mais flexibilidade, transações mais ligeiras, estruturas com menos custos, ampla linha de produtos, maior possibilidade e comodidade de personalização (Eckert, Dal Bó, Sperandio, & Eberle, 2017).

3.5.1 Empresa

Abordando o lado do empresário, tem-se que, sem dúvida, o primeiro fator de atração referente ao *E-commerce* está associado à sua implementação barata e simples, ao fazer uma comparação com o investimento necessário para abrir uma empresa física. Destacando-se como fator crucial, tem-se que o investidor precisará de menos funcionários nesse processo, tendo em conta que os próprios consumidores escolherão os produtos (autosserviço), sem que haja a necessidade para contratar vendedores, e assim, haverá uma redução de custo (Oliveira, 2014).

Outro ponto que merece destaque está associado ao menor prazo para que uma estrutura *online* de vendas seja criada, ao fazer uma comparação com o modelo tradicional. Há plataformas que possuem uma estrutura de venda e compra montadas, com a presença de ferramentas prontas para realizar as operações, e também com o

suporte garantido, beneficiando e muito o controle de administração, estoque e compras do negócio. O aumento referente à margem de lucro, bem como a vantagem da redução voltada para o custo operacional possibilitam uma liberdade maior para operar linhas de promoções e descontos (Oliveira, 2014).

No entanto, para uma empresa que outrora apresenta uma estrutura elaborada de logística para que o seu varejo tradicional tenha o atendimento, quando ocorre a mudança para o varejo virtual, essa empresa deve, em princípio, explorar o seu investimento e conhecimento que havia sido efetuado para ter a possibilidade de atender seus clientes do *E-commerce*. Nota-se que são evidentes os benefícios da integração, tais como: economias nos processos logísticos; vantagens relacionadas com os processos de suprimentos e compras; comercialização mercadológica cruzada; compartilhamento de informações; dentre outros (Bornia et al., 2006).

Além do mais, diante deste contexto, reduzem-se as despesas com o espaço físico que é menor do que nas lojas físicas, mas é essencial para o armazenamento de produtos que são ofertados nas lojas virtuais, tendo em conta que alguns produtos disponibilizados nem sempre estão em estoques físicos, sendo somente solicitados quando for realizada a compra pelo consumidor, ocorrendo de forma direta o despache do distribuidor para o consumidor. Esse fato aqueceu os custos e propiciou para os preços finais um repasse, que são normalmente menores quando comparados com as lojas convencionais, desta forma, funcionando como uma motivação para que o consumidor possa optar no Brasil pelo comércio eletrônico (Diniz, 2019).

Ademais, de acordo com o estudo de Goberto (2011), o mesmo assegurou que o desenvolvimento de uma loja virtual possui muitas vantagens para os consumidores e empreendedor. Não existe limite de horário para um *site* de *E-commerce*, estando *online* constantemente, e possibilitando atender consumidores do mundo e de diferentes partes do país.

Diante deste cenário, pôde ser resumido por Manzi (2020) que:

- O comércio eletrônico consegue reduzir em até 90% os custos de distribuição, criação, armazenamento, recuperação e processamento de informações referentes aos documentos com base em papel;
- O comércio eletrônico possibilita diminuir as despesas administrativas e estoques;
- O relacionamento e serviços com os clientes são facilitados devido à comunicação pessoa a pessoa, interativa e com baixo custo;
- O comércio eletrônico tem a capacidade de reduzir o tempo decorrido entre o recebimento dos serviços e produtos e o desembolso de capital;

- Há uma redução nos custos de telecomunicações pelo comércio eletrônico;
- Existem condições pela publicidade da mesma poder empregar a multimídia, ser atualizada com frequência, ser personalizada e alcançar grandes massas;
- O comércio eletrônico possui a capacidade de igualmente poder fornecer às pequenas empresas as condições para que as mesmas possam enfrentar as grandes empresas.

Assim, também existe uma contribuição para que haja um avanço no comércio virtual, destacando-se a *performance* das empresas ao fazerem uma relação com os dados de seus clientes e também traçarem um perfil desses clientes com base nas suas necessidades e gostos, de acordo com as compras que foram realizadas. Desta forma, pode-se desenvolver um canal de informação, ponderando sobre os produtos em promoção, bem como o envio de sugestões relacionadas às informações e compras dos produtos que despertem interesse. Tem-se que a fidelização por uma parcela dos clientes abarca o resultado (Diniz, 2019).

Deste modo, pequenos negócios ou empresas começam suas atividades pautadas em um comércio eletrônico, de acordo com a enorme quantidade de vantagens que pode ser usufruída com este ramo. No entanto, há muitas empresas que cometem erros no instante em que desenvolvem ou apresentam a plataforma online. Esse fato acontece especialmente por causa da pressa em querer abrir seu próprio negócio e em desenvolver algo, sem que existam as necessárias condições para esta finalidade (Bernardi, 2021).

Além disso, para que uma loja virtual tenha sucesso, as características de sua página virtual são consideradas como primordiais. Essa página precisa ter uma apresentação simples para o consumidor, bem como privacidade, segurança, velocidade, e ter a presença de informações distintas e importantes. Por parte dos consumidores, nota-se que todas essas características relacionadas ao *design* podem influenciar nas decisões de compra *online*, visto que possuem um direto impacto veiculado com a facilidade de uso (Ponceano, 2018).

Logo, diante deste contexto reside o fator conveniência, que está vinculado com o emprego de ambientes de compra que estejam fora da loja. Reconhece-se esse fato como um fator principal de motivação para as compras *online*. O fator conveniência pode influenciar a decisão de compra, isto é, pela facilidade e velocidade com a qual os consumidores consigam realizar uma compra na *Internet* (Panda & Swar, 2013).

3.5.2 Consumidor

Com base em estudos de muitos autores, nota-se que o comércio *online* é usado pelo consumidor por causa do argumento de sua visão sobre os benefícios de natureza utilitária ou funcional, bem como sobre os benefícios de natureza hedônica ou emocional (Yulihasri, Islam, & Daud, 2011; Sarkar, 2011).

Há um conforto para o consumidor referente à essa relação de consumo, tendo em conta que o consumidor digital pode ter a opção de realizar a prestação de serviço ou a compra de um produto sem sair de casa, apenas precisa estar conectado à *Internet* por algum aparelho tecnológico, como aparelhos celulares ou computadores (Hyochimoto, 2020).

Diante deste contexto, pôde ser resumido por Manzi (2020) que os benefícios do comércio eletrônico para o consumidor são que:

- O comércio eletrônico, de um modo geral, propicia serviços e produtos mais em conta;
- O comércio eletrônico fornece aos clientes mais escolhas;
- O comércio eletrônico possibilita aos consumidores que os mesmos possam fazer transações ou comprar 24 horas por dia, de qualquer lugar do mundo;
- Os clientes têm a possibilidade de receber informações relevantes e detalhadas, bem como outros serviços em poucos minutos;
- O comércio eletrônico possibilita aos consumidores que os mesmos possam obter serviços ou produtos personalizados com preços competitivos;
- O comércio eletrônico possibilita aos consumidores que os mesmos possam interagir com os vendedores e outros clientes em comunidades eletrônicas para compartilhar experiências e trocar ideias.

Além disso, com base em um estudo realizado por Feliz (2020), tem-se que em um espaço de 1688 estudantes que estavam fazendo o ensino superior em português, verificou-se que 1225 dos entrevistados fizeram compras *online*, e grande parte o fez em um período de um a três meses, ou menos de um mês; e esses estudantes ficaram muito satisfeitos ou satisfeitos, motivo pelo qual possuem a intenção de realizar a compra novamente. Tem-se que as maiores vantagens destacadas por esses estudantes se relacionaram com os preços acessíveis, entrega da mercadoria em casa, poder realizar a compra a qualquer instante, não precisar sair de casa, bem como a chance de poder comparar preços (Ribeiro et al., 2019).

3.6 DESVANTAGENS

No entanto, observa-se que as lojas virtuais são vistas como se apresentassem desvantagens competitivas referentes aos temas de manuseio e transporte de cargas e problemas com as políticas de devoluções, reembolso e trocas de mercadorias. Ademais, não existe normalmente a ajuda dos vendedores, sem a presença de serviços de pós-vendas, e frequentemente, aparece uma incerteza com relação à obtenção do item (produto) certo, isto é, que seja mais adequado às expectativas, desejos ou necessidades do consumidor (Kacen, Hess, & Chiang, 2013).

Então, um dos problemas que o vendedor enfrentará referente ao quesito compras reside em poder convencer o cliente de que os produtos possuem a esperada qualidade. Uma experiência que não existe em compras pela *Internet* está no fato de não poder testar e experimentar os produtos antes de comprá-los (Oliveira, 2014).

Desta forma, tem-se que compreendem como desvantagens para o consumidor, os eventuais defeitos ou vícios que podem ser apenas constatados quando ocorrem as entregas dos produtos comprados que acabam por decepcionar a expectativa do comprador, dentre outros problemas oriundos deste novo tipo de mercado (Diniz, 2019).

De fato, tem-se que problemas deste tipo foram investigados em um estudo realizado por Rocha (2019), com a obtenção dos resultados a seguir em que: 36 respondentes (42,2%) confessaram que receberam um produto diferente daquele presente na descrição; 35 (41,2%) destacaram o atraso na entrega como um dos riscos/problemas; 17 (20%) constataram que os produtos estavam com defeito; e 11 (12,9%) relataram falta de informação presente no *site* de compra. Verificou-se que a falha de segurança não representou um levado risco, tendo em conta que somente 5 (5,9%) desses consumidores destacaram essa questão.

De acordo com os estudos de Isaías, Sousa, Carvalho e Alturas (2017) e Saxena (2019), os mesmos abordaram a confiança-risco vinculados com a confiança na tecnologia e transação, isto é, um risco relacionado com o comércio *online*. De acordo com esses estudos, verificou-se que a falta de confiança relacionada com a segurança do pagamento (25%) foi o motivo principal para os consumidores não realizarem a compra *online*. Esses estudos também puderam comprovar que não consiste um empecilho o uso da *Internet*, tendo em conta que 95,9% dos entrevistados a utilizam diversas vezes ao longo do dia.

Diante deste panorama, tem-se que Besouchet (2015) destacou que outro estudo, realizado pela E-commerce Europe2 pôde fazer uma estimativa de que o comércio eletrônico (*E-commerce*) consegui alcançar 3,5 milhões de euros no ano de 2015, apresentando um crescimento de 8% ao ano em Portugal. Desta forma, com a presença

deste crescimento neste tipo de consumo, tem-se que muitos clientes e empresas fazem um questionamento sobre a falta de importância que a loja física poderá vir a ter. Neste sentido, mesmo que sejam inegáveis as vantagens associadas com as compras *online* (conveniência e conforto de entrega de mercadoria, bem como facilidade para comparar preços); nota-se que com base no estudo de Besouchet (2015), a experiência de compra que existe no “ponto de venda” físico não será superada. Esse “ponto de venda” físico fornece sentimentos e sensações veiculados com os cinco sentidos, visto que o consumo pela *Internet* não propicia isso, tal como: percepção olfativa; visualização da cor com exatidão; toque do tecido; dentre outras.

Logo, para que esses “pontos de venda” físicos possam se manter ativos comercialmente, os mesmos precisarão explorar novas atrações, que possam ter uma renovação constante e despertar a curiosidade do comprador, com atrações sustentadas no visual de *merchandising* e novas tecnologias, que fazem parte da persuasão e estímulo para o consumo; tendo em conta que essas experiências são possíveis somente nas lojas físicas, visto que as lojas virtuais não as possuem pela impossibilidade ao enquadramento cênico, som, cheiro, toque, dentre outros (A. Freitas, 2017).

3.6.1 Quanto à segurança

Tanto o crescimento quanto a popularização das compras pela *Internet* têm tido o acompanhamento relacionado com as preocupações com a segurança *online*. Com mais frequência, as pesquisas relacionadas com o setor de *marketing*, principalmente as pesquisas sobre o comportamento do consumidor, indicam que alguns motivos principais pelos quais grande parte dos consumidores não compra *online* residem na preocupação com a segurança. Diante deste contexto, destaca-se a falta de segurança para compras *online* como um dos fatores mais importantes que ainda impedem o crescimento e adoção do comércio eletrônico (Choi & Nazareth, 2014).

Com base em um estudo realizado por Eckert et al. (2017), tem-se que os resultados mostraram que a qualidade das informações (preditores), segurança e privacidade dos *sites* relacionados com compras pela *Internet* podem ter uma influência expressiva na confiança que se coloca no *site* de compras *online*. Ademais, notou-se que 68,4% da confiança podem fornecer uma explicação para esses preditores, mostrando um relevante poder de explicação para este quesito.

4 CRIME DE ESTELIONATO

De fato, caracteriza-se um estelionato como um crime em que a fraude é praticada, visto que o agente, com o emprego de artimanhas, tem a capacidade de enganar a vítima, e desta forma convencê-la a entregar algum bem para esse agente, e assim, se enriquece de maneira ilícita com esse bem (Lopes, 2017).

Existe alguma preocupação desde a antiguidade com o agente que praticava fraudes contra uma pessoa, e deste modo, existia uma tentativa de proibir essas ações, e medidas punitivas eram aplicadas para o agente que praticasse esse ato abominável (Consoni, 2011).

Pode-se destacar que no antigo Egito, quando ainda não existia um direito estruturado, havia punições contra as pessoas que praticassem algum tipo de fraude, com a aplicação de bastonadas. Essas punições também ocorreram nos povos sumérios, babilônios e caldeus, em históricos momentos relacionados com o pré-Código de Hammurabi, e posteriormente, a punição contra a fraude pôde ser estabelecida com a efetividade dessas leis. De fato, tem-se que a influência dessas leis alcançaram os hebreus, e também os gregos, que realizavam punições para aqueles que praticassem fraudes (Theodoro Júnior, 2001).

Com relação aos romanos, tem-se que a punição contra o fraudador era essencial, visto que essa prática era considerada como um tipo de estelionato, e totalmente deplorável. De acordo com os códigos de leis, essa prática se caracterizava como um tipo de conduta que poderia encobrir uma conduta classificada como legal, bem como uma conduta danosa com o outro (Souza, 2002).

Dentre as diferentes modalidades de estelionato, podem ser destacadas aquelas que se configuravam como fraude para os romanos, como as seguintes:

1°) aquele indivíduo, que sendo um devedor, faz a transferência de como sendo sua uma coisa que foi fornecida em garantia, mas sem a presença do consentimento do credor;

2°) aquele indivíduo que fornece em penhor coisas de outros ou penhora coisas alheias;

3°) aquele indivíduo que se passa por outra pessoa, para poder lesar o credor;

4°) aquele indivíduo que fornecia para um credor em penhor cobre por ouro;

5°) aquele indivíduo que conseguia vender o estado livre como escravo, encobrindo sua condição de liberto.

De fato, destaca-se que o Código Penal da França do ano de 1810 considerava crime a tentativa ou obtenção relacionada com a vantagem patrimonial, através de meios fraudulentos (art. 405). Em diversos países, nota-se que o estelionato recebeu

nomes distintos, mas em todos os países, a atitude fraudulenta apresentava uma característica comum. Tem-se que na Espanha, o estelionato recebeu a denominação de *estafa*, na Alemanha, *betrug* (engano), na Itália, *truffd* (Códigos Rocco e Zanardelli), bem como *frode* (Código toscano), e em Portugal, *burla* (Bitencourt, 2018).

Referente às Ordenações Filipinas, tem-se que o estelionato pode ser caracterizado como *inliço* ou *burla* (Livro V, Título 665), e quando o prejuízo fosse maior do que vinte mil-réis, a pena de morte era atribuída. Com relação ao Código Criminal do Império (Lei de 16 dezembro, 1830), empregou-se o *nomen juris* estelionato prevendo-se inúmeras figuras, não estando fechada somente na descrição genérica, tais como qualquer e toda manobra fraudulenta, que se obtém de outra pessoa parte de sua fortuna ou toda a fortuna, bem mesmo qualquer título. Posteriormente, o Código Penal republicano (1890) também seguiu esta linha de pensamento, com a tipificação de onze figuras de estelionato, bem como uma modalidade genérica, tais como empregar artifícios para iludir a vigilância de outra pessoa, surpreender a boa-fé, ou mesmo ganhar a confiança; fazendo com que essa pessoa (vítima) seja induzida ao engano ou erro, por essa e outras artimanhas, a ter para si o proveito ou lucro (Bitencourt, 2018).

Desta forma, nota-se que nos dias atuais, o estelionato se caracteriza como um crime que apresenta perfis repletos de atuação e persuasão para obter vantagens. Há uma análise técnica relacionada ao público-alvo, frequentemente, a formação de uma estrutura pré-montada para que a pessoa possa ser induzida ao erro. Com base no estudo do penalista Hungria (2012), nota- se que a criminalidade, ocasionalmente, se origina lentamente da violência, ou seja, seria como um bandidismo inteligente e silencioso, e esse fato foi exposto em seu trabalho como o exemplo de que:

> O ladrão que usa da violência, extremamente comum em outras épocas, atualmente compreende um fenômeno esporádico ou retardatário. [...] Tem-se que a violência emprega sinais evidentes ou indiscretos, fornecendo perigo de reação, que é alarmante e escandalosa (Hungria, 2012, p.148).

Para a finalidade de ataque aos bens de patrimônio pessoal, não existe atualmente o emprego da violência, visto que o estelionatário atua de maneira sorrateira, sobretudo, de uma forma resguardada para que não se tenha alarde, com a presença de indícios relacionados com o consentimento da vítima. De fato, o emprego de violência não é mais necessário para obter o patrimônio pessoal de uma pessoa, tendo em conta que a violência foi retirada, para entrar em campo uma maneira mais “malandra” (Sanda, 2019).

De alguma maneira, para que um crime de estelionato possa ser cometido, torna-se fundamental, paralelamente às imorais inclinações para o crime que acabam por lesar uma vítima, que haja a oportunidade, bem como apresentar uma teoria hipotética

de uma mente muito desenvolvida. Se essas atitudes não são inerentes ao próprio estelionatário, torna-se possível que haja a transmissão de estratégias referentes aos golpes bem-sucedidos, sem que seja necessário fazer a elaboração dos mesmos do zero. Então, de acordo com a disponibilidade contida na literatura sobre crimes de fraudes e contos-do-vigário, esses golpes acontecem repetidamente em todo o país, e por gerações, sendo continuados por estelionatários diferentes, e que muitas vezes nem se conhecem. Esse fato demonstra um panorama de que alguns golpes podem ser reproduzidos e absorvidos como um tipo de “artefatos prontos”, ou seja, sem a necessidade de teorias dos golpes pelos estelionatários. Desta forma, para que o crime possa ser consolidado, não existe a necessidade de prever como será a reação da vítima, seja por aprendizado intenso ou observação. Obviamente, quando certo golpe é praticado repetidamente, pode-se ilustrar que ocorreu uma rotina do golpe, visto que não se torna mais essencial realizar a exploração de uma série de hipóteses sobre o comportamento das vítimas diante do golpe (Oliveira, 2013).

Além do mais, deve-se ressaltar que existe uma discussão doutrinária referente à “torpeza ou fraude bilateral”. Essa atitude acontece quando a própria vítima do crime de estelionato também age com má-fé. Esses fatos são conhecidos como os casos do bilhete premiado, assim como outros tipos de golpes que apenas funcionam quando o alvo (pessoa-alvo do estelionatário) também atua de maneira infame (Cabette, 2018).

Com base no estudo de Rogério Greco (2017), tem-se que o mesmo convergiu com a doutrina tradicional de Nelson Hungria, com o entendimento de que não haveria, nesses casos, a punição do estelionatário pelo crime de estelionato. Assim, esse autor compreende que o entendimento dominante se relaciona com a presença do delito referente ao estelionato, sem a relevância da má-fé do ofendido, isto é, sua intenção também era indecorosa (imoral, ilegal...). De acordo com o trabalho de Andreucci (2010), o mesmo pôde afirmar de maneira categórica que não há descaracterização do estelionato pela torpeza bilateral.

Referente aos efeitos jurídicos, caracteriza-se um estelionato quando um indivíduo realiza uma ação através de práticas enganosas com o intuito de poder tirar alguma vantagem da vítima. Mesmo que esta definição pareça evidente, torna-se essencial fazer a distinção dos crimes de estelionato de outras práticas realizadas na sociedade, visto que com o aparecimento de práticas enganosas que estão contidas na própria linguagem (não existe uma diferença de natureza, mas sim de qualidade), espera-se que se equipare a condição do insincero social ou mesmo mentiroso convencional à condição moral caracterizada como estelionatário. No entanto, compreende-se que existem especificidades que precisam ser destacadas para que as inúmeras interações

dos agentes possam ser distinguidas, ou seja, desde a simples mentira até a mentira criminosa (Oliveira, 2013).

De fato, nota-se que comumente a dificuldade reside no caso de uma mulher que não possui posses conseguir ascender na sociedade pelo casamento, com investimentos pesados com técnicas de sedução para conquistar o candidato a marido, esse exemplo se caracteriza como o conhecido “golpe do baú”, e esse golpe se enquadra em uma forma de estelionato, independente se o casal ficará casado por um longo tempo, tendo em conta que o sentimento verdadeiro da mulher residia na condição econômica do candidato. Assim, tem-se que esse casamento seria classificado como uma maneira de tornar legítima essa artimanha sobre a vítima. Então, nota-se que está inserida no imaginário social do Brasil a expressão 171, ou seja, qualquer meio empregado para que uma vantagem seja obtida, visto que seria impossível obtê-la de outra forma, classificando-se como um tipo de golpe. Todavia, mesmo com as similaridades que aparecem com o entendimento do dia a dia, tem-se que a definição criminal deduz que a vítima deva procurar uma delegacia para poder prestar queixa sobre o que aconteceu; no entanto, a vítima tem que se sentir lesada, e desta forma, relações afetivas são excluídas, visto que com esse tipo de relacionamento entende-se que existe o compartilhamento de bens materiais, não sendo classificado como um típico golpe. Ademais, não há interferência do Estado nesse caso, porque se trata de uma livre escolha da pessoa (Oliveira, 2013).

4.1 CRIME DE ESTELIONATO NO BRASIL

Com base no estudo de Bitencourt (2011), tem-se que o estelionato se caracteriza como uma prática que surgiu aproximadamente no século II d.C., sendo classificado como um tipo penal subsidiário e genérico. Apenas no século seguinte, o estelionato foi tratado e considerado como um tema mais grave. Foi decretado no dia 16 de dezembro de 1830 pelo Código Criminal do Império presente em seu art. 264 que:

> Art. 264. Julgar-se-á crime de estelionato:
> 1° A alheação de bens alheios como próprios, ou a troca das cousas, que se deverem entregar por outras diversas.
> 2° A alheação, locação, aforamento, ou arretamento da cousa própria já alheada, locada, aforada, ou arretada á outrem; ou a alheação da cousa própria especialmente hipotecada á terceiro.
> 3° A hipoteca especial da mesma cousa á diversas pessoas, não chegando o seu valor para pagamento de todos os credores hipotecários.
> 4° Em geral todo, e qualquer artificio fraudulento, pelo qual se obtenha de outrem toda a sua fortuna, ou parte dela, ou quaisquer títulos.
> Penas - de prisão com trabalho por seis meses a seis anos e de multa de cinco a vinte por cento do valor das cousas, sobre que versar o estelionato. (Lei de 16 de dezembro,1830, art. 264).

Então, nota-se que está previsto hoje o estelionato pelo ordenamento jurídico do Brasil, sedo discriminado no Código Penal em vigência no art. 171 de 1940. Paralelamente a outros agravantes que acarretam um aumento da pena, estando previsto neste artigo, existe um rigoroso critério com relação ao crime de estelionato praticado contra pessoas, que estejam de certa forma perdendo sua capacidade plena, como as pessoas da terceira idade (Sanda, 2019).

Desta forma, torna-se concebível entender o crime de estelionato, visto que o mesmo está discriminado no caput do art. 171 presente no Código Penal Brasileiro, que possui como inspiração o interesse da sociedade em poder reprimir as fraudes que acarretam dano ao próximo, assim como no interesse social em poder fornecer uma proteção para a boa-fé referente ao negócio jurídico, constituído pela mútua confiança que precisa existir nos relacionamentos patrimoniais comerciais e individuais, conforme disposto abaixo (Farah, 2017):

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis (Decreto-Lei n. 2.848, 1940, art. 171).

Há outras modalidades relacionadas com esse crime, tais como estelionato praticado com cheque sem fundos, que se inserem nos parágrafos e incisos do artigo (Lopes, 2017).

Conforme descrito anteriormente sobre a definição no art. 171 do Código Penal, nota-se que esse crime se utiliza de artifício, ardil ou qualquer outro tipo de meio fraudulento. Está presente esse “artifício” quando existe a intenção de enganar a vítima, e desta forma, o agente utiliza algum artefato, algum objeto que seja capaz de ludibriar a vítima. Com relação à “ardil”, a mesma se caracteriza como uma conversa enganosa que é praticada pelo agente para montar a farsa com mentiras verbais. Finalmente, empregou-se “outro tipo de meio fraudulento” pelo legislador para que pudesse abranger outra forma de artimanha que fosse capaz de ludibriar a vítima, tais como o silêncio. Nota-se que a no item 61 contido na Exposição de Motivos da Parte Especial do Código Penal, explica-se que o próprio silêncio, quando de forma intencional ou maliciosa, sobre o erro da vítima preexistente, é caracterizado como um meio fraudulento típico de estelionato (Lopes, 2017).

Também pôde ser complementado por Prado que ardil compreende uma aplicação astuta de maneira enganosa, estando revestida por uma forma intelectual. Essa prática ardilosa age sobre o sentimento ou inteligência da vítima, distanciando a realidade dos fatos que está voltado para o objetivo do agente, aplicando meios de persuasão à vítima para que a mesma acredite que a falsa aparência sentimental ou

lógica criada pelo estelionatário seja verdadeira, fazendo com que a vítima mantenha ou incorra neste erro, por conseguinte com lesão patrimonial e vantagem ilícita (Dantas, 2013).

Por outro lado, tem-se que o artificio compreende uma dissimulação ou simulação idônea para que a pessoa seja conduzida ao erro, fazendo com esta acredite em um mundo que nunca existiu, uma imagem distorcida da realidade, isto é, a vítima passa a ter uma equivocada impressão da realidade que está ao redor. Nota-se que esta técnica pode ocorrer tanto na modalidade omissiva ou modalidade comissiva, implícita ou explícita, sendo formada por qualquer meio de comunicação empregado pelo homem, ou seja, por palavras, gestos, ou mesmo o próprio silêncio (Dantas, 2013).

Referente a “outro tipo de meio fraudulento”, tem-se que o art. 171 do Código Penal indica que, ao fazer a citação de artifício ou ardil, o mesmo somente fornece exemplos de maneiras fraudulentas para enganar a vítima, desta maneira, tratando-se de um estelionato de crime caracterizado como de forma livre, não estando vinculado a nenhum meio de específica ação. Assim, observa-se que a criatividade do ser humano ditará as formas de estelionato que serão praticadas, sofrendo variações à proporção que aquela forma evolui (Dantas, 2013).

Ao abordar o tema da vítima do delito, nota-se que a mesma pode apresentar o conceito de sujeito passivo do estelionato, ou seja, compreendendo a pessoa que sofre a lesão patrimonial; de um modo geral, essa pessoa é a mesma que é enganada. No entanto, pode-se enganar uma pessoa para que um terceiro sofra o prejuízo, não sendo uma regra que a vítima do erro seja a mesma do dano patrimonial, tendo em conta que a lei se dirige, de forma genérica, a prejuízo alheio (Mirabete & Fabbrini, 2008).

Logo, há um crime quando o agente utiliza um meio fraudulento, fazendo com que uma pessoa seja induzida em erro ou que seja mantida nessa situação, para que posteriormente o estelionatário possa obter alguma vantagem indevida para ele próprio ou para outra pessoa, sempre com a presença de lesão patrimonial alheia. Sem a evidência de fraude antecedente, que mantém ou acarreta um erro à vítima, fazendo com que a mesma entregue a vantagem, não se aborda essa atitude como crime de estelionato (Santos, 2019).

Além do mais, torna-se pertinente abordar o tema sobre a necessidade de a vítima referente ao crime de estelionato possuir capacidade, visto que, deve haver fraude para que o crime de estelionato ocorra, enganando a vítima ardilosamente ou fazendo com que a mesma permaneça no erro. Deste modo, a pessoa iludida precisa ter a capacidade de poder ser enganada. Assim, um menor ou uma pessoa sem discernimento que não tenha a capacidade voltada para as relações cívicas não pode ser caracterizada como o sujeito passivo do crime vinculado como estelionato. No caso

concreto, tem-se que cumpre ao juiz esse juízo de valor referente à capacidade, sendo que deve ser constatada essa capacidade para um correto enquadramento da conduta defeituosa, tendo em conta, de acordo com a maior parte da doutrina, se a ausência de capacidade referente ao sujeito passivo for comprovada, o crime será classificado como abuso de incapazes, ou mesmo furto, mas não um caso de estelionato (Dantas, 2013).

Com base neste sentido, o estudo de Bitencourt (2009) pôde explicar que a falta de capacidade de discernimento pode ser entendida como um crime presente no art. 173 do Código Penal (abuso de incapazes). Além disso, tem-se que caso a vítima não possua uma natural capacidade para ser iludida, como no caso da vítima se encontrar em estado de coma, esse crime será classificado como crime de furto.

Prosseguindo nesta linha de pensamento, tem-se que o estelionato é considerado como um crime plurissubsistente, ou seja, desdobra-se em mais de um ato a conduta que é realizada pelo agente. Caso seja possível realizar o fracionamento desta conduta fraudulenta, torna-se plausível trabalhar com a tentativa, desta forma, quando o estelionatário começa a realizar os atos fraudulentos, mas por motivos alheios à sua vontade, o mesmo não finaliza o crime, e assim, esse estelionatário precisa responder pelo crime na forma tentada (Nova & Santos, 2019). Abordando sobre o que precisa ser compreendido como o princípio dos atos executórios com relação ao estelionato com o intuito de aplicação da tentativa, há uma explicação de Cezar Roberto Bitencourt (2012) sobre o tema:

> No estelionato, crime que requer a cooperação da vítima, o início de sua execução se dá com o engano da vítima. Quando o agente não consegue enganar a vítima, o simples emprego de artifício ou ardil caracteriza apenas a prática de atos preparatórios, não se podendo cogitar da tentativa (p. 227).

Além disso, torna-se primordial abordar o assunto *conatus*, bem como o engano da vítima em si, quando o agente não adquire a vantagem indevida, mas devido às circunstâncias alheias vinculadas à sua vontade, não por vontade própria (Nova & Santos, 2019).

Com relação ao furto, nota-se que o art. 171 contido em seu parágrafo 1º pôde prever a aplicação ao estelionato do privilégio vinculado ao furto conforme previsto no art. 155, contido no parágrafo 2º, tem-se que ambos estão presentes no Código Penal, desde que o agente seja primário e o crime de pequeno valor. De fato, tem-se que o legislador teve o cuidado nesse caso de adequar a redação referente ao dispositivo em consideração ao objeto material relacionado ao estelionato, deste modo, o artigo indicou o prejuízo corretamente em vez de apenas mencionar esse crime como de pequeno valor (Nova & Santos, 2019).

Neste instante, deve-se esclarecer sobre o furto perante estelionato e fraude, mesmo que os dois crimes sejam cometidos contra o patrimônio bem como empreguem a fraude como uma maneira de executá-los, a distinção entre os dois reside basicamente no instante em que se emprega a fraude na ação criminosa (Coimbra, 2020).

À vista disso, o Código Penal Brasileiro define furto mediante fraude, *in verbis*:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel: [...] Furto qualificado § 4° - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido: [...] II - com abuso de confiança, ou mediante fraude, escalada ou destreza (Coimbra, 2020, art. 155).

Ademais, com relação ao furto diante de fraude, tem-se que a fraude é empregada como uma maneira para que algo possa ser subtraído, como uma maneira de enganar a vigilância da vítima sem que a mesma perceba que o seu patrimônio está reduzindo. No entanto, não se deve confundir com a fraude que é utilizada no estelionato, em que a vantagem ilícita é obtida anteriormente com o intuito de viciar a aprovação da vítima para que a mesma tenha a postura positiva de entregar os bens, com a plena consciência de entrega de seu patrimônio para o estelionatário (Coimbra, 2020).

Pode-se exemplificar o caso do agente que realiza a clonagem de um cartão de crédito, e com esse cartão, esse agente realiza saques na conta bancária da vítima, neste caso, o agente pratica somente furto diante da fraude, sendo inicialmente, absorvida a falsidade. Da mesma maneira, esse agente realiza o estelionato quando o mesmo faz compras em estabelecimentos comerciais (Kunrath, 2014).

Tem-se que no art. 298 houve a inserção do delito relacionado com a falsificação de cartões de crédito com o objetivo de proteger a fé pública, entretanto, se houver a duplicação da tarja magnética do cartão de débito ou crédito, com a presença de sua utilização, nota-se que a falsidade provavelmente será absorvida de acordo com o delito de estelionato, com relação ao princípio de consumação com base na Súmula n.° 17 do Supremo Tribunal de Justiça (STJ) (Kunrath, 2014).

Todavia, entende-se como estelionato o delito que acontece contra o patrimônio, que é praticado ardilosamente com o intuito de iludir a vítima. Deve-se ressaltar que para o crime de estelionato, o mesmo é absorvido pelo crime fim, isto é, poderá ser absorvido o crime de estelionato pelo resultado final referente ao crime de maior gravidade (Santos, 2019).

Para que um crime possa ser caracterizado como estelionato, precisam estar presentes todas as características, visto que as mesmas compreendem os constitutivos elementos relacionados com esse crime. Esse crime compreende um crime que possui duplicidade do nexo causal. De fato, tem-se que o erro oriundo da fraude não basta, tem

de existir o proveito, vantagem ilícita ou benefício que não tenha sido justificado pelo ordenamento legal, acarretando para a vítima um prejuízo patrimonial. Em um primeiro instante, engana-se a vítima diante de fraude, e a mesma, caracteriza-se como a causa do engano, sendo o seu efeito. Posteriormente, caracteriza-se a nova relação causal pelo acometimento do consequente erro do engano, como uma forma de obtenção e causa da vantagem ilícita, e como efeito, tem-se o correspondente dano patrimonial (Santos, 2019).

Além do mais, denota-se que com relação ao objeto do crime, o mesmo se caracteriza como a vantagem ilícita, isto é, qualquer utilidade que seja conquistada em benefício do sujeito ativo ou mesmo de terceiros: execução de um ato; gozo; crédito, propriedade... [...] Mesmo que não seja primordial ter o caráter econômico inerente da vantagem, ao abordar crime patrimonial, esse é essencial. Sem vantagem econômica conseguida pela fraude, não se pode caracterizar o crime como estelionato. [...] A vantagem ilícita deve estar presente, visto que, caso devida, a mesma terá de acontecer somente pelo delito de exercício deliberado pelas razões próprias (art. 345). Ainda, de forma indispensável, para que haja a concretização deste tipo de crime, deve-se destacar o efetivo prejuízo da vítima, isto é, uma perda, um dano que seja de utilidade econômica (Mirabete & Fabbrini, 2008).

Diante deste contexto, é notável mostrar que os autores doutrinários discordaram com relação aos fundamentais requisitos para que o estelionato seja configurado como crime, tais como para o estudo de Cunha (2014), em que três requisitos estão inseridos: prejuízo alheio; vantagem ilícita e fraude. Por outro lado, para Bitencourt (2014), os três requisitos compreendem: obtenção de ilícita vantagem patrimonial em prejuízo alheio; manutenção ou induzimento da vítima para cometer o erro; e emprego de artifício, artimanha (ardil) ou outro meio fraudulento.

Desta forma, tem-se que o estelionato se caracteriza como um delito material. Considera-se como um crime material aquele em que um tipo de comportamento é descrito, e o resultado é mencionado, com a exigência de sua produção. De fato, o legislador na espécie consegue fazer uma definição do comportamento do agente, empregando fraude na manutenção ou induzimento de uma pessoa ao erro, e o resultado dessa ação compreende uma ilícita vantagem em prejuízo alheio. Tem-se que o verbo “obter” abarca o núcleo do tipo. Assim, torna-se essencial que o agente consiga ter uma vantagem ilícita para que o delito possa existir, o Código Penal faz a exigência de que haja uma produção do resultado duplo (presença de vantagem ilícita acarretando prejuízo alheio). Desta forma, exige-se um tipo relacionado com a produção do resultado, sendo caracterizado esse crime como não formal, mas sim material (Jesus, 2014).

Ao passo que o dolo representa o subjetivo elemento referente ao estelionato, demonstrando a vontade que o estelionatário possui de enganar alguém, de maneira espontânea, diante um meio fraudulento, com o objetivo de obter uma ilícita vantagem patrimonial, acarretando o prejuízo de outra pessoa. Referente ao termo “induzir ao erro”, tem-se que o dolo precisa ocorrer antes que o meio fraudulento seja aplicado, e, tanto prejuízo quanto vantagem ilícita de outras pessoas sejam concretizados. Todavia, com relação ao termo “manter em erro”, nota-se que o dolo estará acompanhado do erro, isto é, ao ser constatado o erro, será mantido o dolo nele (Bitencourt, 2009).

Com base no art. 171, §2°, V do Código Penal, tem-se que o mesmo concorda sobre o tema de que o estelionato “destrói, parcialmente ou totalmente, ou mesmo lesa a saúde, o próprio corpo, ou oculta coisa própria, ou mesmo acentua as consequências da doença ou lesão, com o objetivo de ter valor de seguro ou indenização (NASCIMENTO, 2014).

Então, trata-se de um crime próprio como a fraude, visto que se exige pela fraude uma qualidade pessoal do autor, caracterizado como o segurado, visto que esse autor tem de ser o proprietário do imóvel destruído ou da coisa móvel. Além disso, tem-se que o segurado precisa ser o portador da doença ou lesão, que então é agravada nessa situação pela conduta de delito. Caso tenha um terceiro envolvido, a mando do segurado para agravar a saúde, ou destruir o objeto material, os dois apresentarem a consciência desses atos ilegais, ambos terão de responder pelo crime de estelionato (Jesus, 2014).

De acordo com o autor Jesus (2014), compreende-se uma conduta ilícita em três ações:

> 1° destruir ou ocultar coisa própria:
> [...] o sujeito destrói, total ou parcialmente, a coisa própria, ou a oculta. No fato da destruição, as coisas podem ser móveis ou imóveis; no da ocultação, como é evidente, o objeto material só pode ser móvel. Trata-se de conduta que recai sobre coisa própria. Se de terceiro, o fato constituirá outro delito. (Jesus, 2014, p. 490).
> 2° lesar o próprio corpo ou a saúde: [...] conduta típica é de o sujeito lesar o próprio corpo ou a saúde. O Código Penal não pune a autolesão por si mesma, a não ser quando acompanhada de finalidade delituosa, como ocorre na hipótese (Jesus, 2014, p. 490).

Nota-se que não há punição pelo Código Penal para a pessoa que lesiona a si própria, no entanto, quando a mesma realiza esse ato com o intuito de obter alguma coisa de forma ilícita, essa pessoa estará infringindo a lei (NASCIMENTO, 2014).

> 3° agravar as consequências de lesão ou doença. [...] o sujeito é portador de lesão ou doença, que tem agravadas suas consequências em face da conduta. A finalidade é conseguir maior indenização (Jesus, 2014, p. 490).

Mesmo assim, nota-se que a doutrina não possui uma única convergência sobre o tema da vantagem ilícita que é obtida pelo agente, ou seja, se deve ser ou não ser de cunho econômico (Dapper, 2012).

De acordo com o estudo de Greco (2011), observa-se que a vantagem ilícita é sustentada quando for de cunho econômico, com base em uma interpretação sistêmica, à proporção que a mesma é tratada como crime patrimonial, inserido no Código Penal que acaba protegendo o patrimônio.

Por outro lado, o estudo de Bitencourt (2011) fez o entendimento de que uma ilícita vantagem obtida que é realizada pelo agente pode apresentar qualquer natureza, destacando-se o argumento de que:

> [...] os crimes que são cometidos contra o patrimônio acabam por fornecer proteção à inviolabilidade patrimonial referente à vítima em particular e à sociedade em geral, assuntos que não devem ser confundidos com a ilícita vantagem que é conseguida pelo agente. Por este motivo, tem-se que não é a vantagem obtida que necessariamente precisa ser de cunho econômico; mas deve ter essa qualidade referente ao prejuízo que a vítima sofre (Bitencourt, 2011, pp. 274-276).

Deve-se destacar que, não se considera eficaz arrependimento, isto é, mesmo que o estelionatário, exceto na concepção de pagamento com cheque sem fundos (§ 2a, VI), consiga ressarcir o prejuízo causado antes da denúncia ser recebida, tem-se que esse estelionatário não terá direito à retirada da punição, incidirá somente a causa obrigatória de redução da pena de acordo com o art. 16 do Código Penal, em uma prolatada decisão do STJ/PE (STJ, HC 7.578/PE, Rei. Vicente Leal, j. la-6-1999) (Ribeiro, 2019).

Torna-se primordial também destacar a figura relacionada com o estelionato judiciário, que consiste em uma ação bem recente no ordenamento jurídico do país, com origem em um intelectual exercício que possui como objetivo impedir abusos eventuais vinculados com o direito de ação, ou seja, uma garantia que é prevista no artigo 5°, inciso XXXV da Constituição Federal (Chanes, 2015).

Todavia, desconhece-se a origem desse injusto, mas pode-se afirmar que sua origem está no exterior, de acordo com as palavras do Professor Luiz Regis Prado (2011):

> Admite-se pela doutrina estrangeira que existe a possibilidade de haver um estelionato processual, inclusive presente no processo civil, quando por uma parte, com a presença de uma conduta enganosa ou fraudulenta, faz-se com a intenção de lucro e para que um juiz seja induzido ao erro, e consequentemente, esse juiz acaba por proferir uma injusta sentença que acarreta um dano patrimonial a terceiro ou parte contrária (p. 554).

Diante deste contexto, nota-se que existe a presença de um denominado trinômio que consiste em erro, fraude e vantagem ilícita, fundamentais para exemplificar um crime de estelionato, isto é, utiliza-se a parte consciente de uma fraude que é capaz de ludibriar o juiz, ocasionando uma ilícita vantagem, por conseguinte um dano de terceiros, e os terceiros representam a parte contrária (Chanes, 2015).

Logo, delineando sobre o tema de crime de estelionato, tem-se que três elementos fundamentais podem ser extraídos para que este crime seja configurado, tais como: 1) prejuízo da vítima e vantagem ilícita como resultado do engano; 2) manter ou induzir o prejudicado em erro; e 3) utilizar de meios fraudulentos, podendo ser um artifício, ser o ardil, ou qualquer outro tipo (Dantas, 2013).

4.2 EM PORTUGAL

Perante inúmeras configurações, tem-se que a burla apresenta sempre como típico elemento o intuito de receber algum benefício.

Nota-se que a concepção de criminológico de crime reside, de forma inevitável, em uma alusão dupla, ou seja, uma referência sociológica e uma referência jurídica. Certamente, conforme explicado por Vold, tem-se que o crime engloba normalmente dois critérios, que são: definição ou julgamento do comportamento humano por parte de outras pessoas que o consideram como permitido e próprio, ou proibido e impróprio; e o comportamento humano em si (Dias & Andrade, 2013).

Diante deste cenário, referente aos termos jurídicos penais, encontra-se a noção de crime no Código de Processo Penal (CPP), isto é, reunião de pressupostos de que descende uma aplicação ao agente de uma medida relacionado com segurança criminal ou de uma pena. Tem-se que a concepção de crime engloba um sentido material em que se pode definir a atuação típica, culposa, voluntária e ilícita de alguém, e no âmbito processual representa uma reunião de pressupostos e condições, para que, na ordem jurídica, a definição material de crime possa ter uma real expressão (Lôbo, 2017).

Tem-se que o crime de burla insere os crimes que compreendem a “ordem de criminalidade econômica”, em que esse tipo de crime se encontra no Código Penal e na legislação avulsa, presente na seção dos crimes que estão relacionados com o patrimônio, e na subseção, como crimes associados contra o patrimônio de um modo geral, em que “o patrimônio compreende o bem jurídico protegido” (Ferreira, 2011).

Então, reflete-se a relevância deste tipo de crime quando o mesmo se aplica em faixas etárias que são caracterizadas como mais vulneráveis, como a terceira idade. Aproximadamente 5% dos crimes foram cometidos contra idosos, compreendendo 4.338 casos de 2013 até 2019 (Guarda Nacional Republicana, 2020). De fato, tem-se que este fenômeno criminal é analisado de forma particular, por ser empregado

vulgarmente como preocupante em abordagens sobre o problema da criminalidade contra a terceira idade, e que precisa originar um certo cuidado referente à sensibilização aos idosos. Observa-se que o crime de burla é caracterizado como um crime, mesmo não sendo o mais comum, em que foram registrados números acima de 500 ocorrências por ano no período de 2013 a 2018, tendo em conta que para o ano de 2019 foram registrados 973 casos (Guarda Nacional Republicana, 2020). Mesmo que não seja um crime classificado como preocupante, deve-se fornecer um alerta para que haja a necessidade de um contínuo trabalho sobre esse assunto.

Dentre os tipos de burla contra idosos que puderam ser registrados pela Guarda Nacional Republicana (GNR) no período de 2013 a 2019, tem-se:

- Burla com fraude bancária;
- Burla informática e nas comunicações;
- Burla para obtenção de alimentos, bebidas ou serviços;
- Burla relativa a trabalho ou emprego;
- Burla tributária (Guarda Nacional Republicana, 2020).

Com base no art.° 217 do Código Penal sobre burla, tem-se que a pessoa que comete o crime de burla é aquela que têm a intenção de ter enriquecimento ilícito, para si mesma ou para terceiros, através de engano ou erro sobre ações que provocou de forma astuta, determinar para outra pessoa a prática de atitudes que possam causar prejuízo para terceiros ou para a mesma pessoa (Ferreira, 2011). Por outro lado, o art. 220º destaca a questão da burla para obter bebidas, alimentos ou serviços, para a pessoa que não possui a intenção de pagar. Nota-se que essa distinção parece evidente, visto compreenderem duas fases ou partes de um mesmo tipo de comportamento (Reis, 2019).

Também podem ser identificados nos artigos 218.° a 226.°, que estão presentes na mesma norma, que existem inúmeros tipos de burla. Nos artigos 256.° a 261.°, presentes na seção II, referenciam-se diversos tipos de falsificação, principalmente a falsificação de documentos.

De fato, a distinção entre fraude e burla reside no fato de que a fraude tem origem na atividade econômica existente, com a obtenção dos mesmos benefícios; ao passo que a burla compreende um ato fictício com o intuito de obter indevidas vantagens patrimoniais (Machado, 2014).

Com base em notícias que têm anunciado esse crime em distintos meios de comunicação, nota-se que o ilícito ato da fraude no medicamento pôde ser caracterizado como associação criminosa, burla grave, branqueamento de capitais e corrupção (Machado, 2014).

Segundo os artigos 217.° e 218.° do Código Penal, tem-se que a burla é classificada como qualificada caso aconteça um dano patrimonial que tenha um elevado valor, e o agente poderá ir para a cadeia (Machado, 2014).

Desta forma, representa-se a burla como um crime de prejuízo com relação ao nível de lesão do bem jurídico que é protegido, e por fim, com relação à maneira de consumação, sendo caracterizada como a vítima neste ato ilícito, a pessoa que ficou com o patrimônio empobrecido, podendo ou não ser a mesma pessoa que foi enganada (Albuquerque, 2015). Nota-se que o elemento que consiste no objetivo do crime de burla representa a determinação de um agente através de engano ou erro sobre fatos que esse agente acarretou de forma astuta, em uma prática de ações que ocasionam dano patrimonial para terceiros ou para si, pondo-se deste modo, a pauta sobre a imputação objetiva referente ao resultado da ação, e tem-se que essa é a compreensão que assegura a observância plena relacionada com o princípio da legalidade, visto que o significado de “astúcia” é como foi visto, de “ardil” ou “manha” (Domingues, 2020).

De fato, nota-se que a sociedade está diante de um crime que possui a participação da própria vítima, visto que a vítima representa o próprio sujeito passivo que realiza os atos que acarretam o empobrecimento de seu patrimônio; entretanto, o engano que o agente ativo produz é o que faz com que a vítima permaneça no erro. Mesmo que uma culpa eventual da vítima possa ser verificada, devido à sua ingenuidade, para o agente, essa culpa não representa uma desculpa, porque o crime de burla é imputado, porque há um nexo entre o perfil astúcia/mentira inerente ao agente ativo e a ação da vítima (agente passivo) naquele momento, e pode-se considerar o padrão associado ao “homem médio”, sendo que essa ação não seria tratada como burla (Domingues, 2020).

Desta forma, tem-se que a burla se constitui um crime de cunho semipúblico, com base no art. 217.º do Código Penal, em que se encaixa uma pena de multa ou uma pena de prisão no período de até três anos, bem como a tentativa também de possuir caráter de punição. Além disso, caso certos pressupostos sejam preenchidos, a pena também pode ser agravada, bem como ser classificada como burla qualificada, ou seja, um crime punido e previsto no art. 218.º do Código Penal (Domingues, 2020).

Logo, nota-se que a burla representa um crime de dano, mas essa burla apenas será consumada caso exista um efetivo prejuízo no patrimônio de terceiro ou da vítima (sujeito passivo) da infração (Reis, 2019).

4.2.1 Burla qualificada

De fato, tem-se está consagrado no art. 218.º o crime de burla qualificada, que está presente no capítulo III do Código Penal referente aos crimes de patrimônio de um

modo geral. Em um momento, verifica-se que o bem jurídico que possui a intenção de ser protegido pela incriminação, de um modo geral, representa o patrimônio de outra pessoa. Então, todo empobrecimento relacionado com o patrimônio ofendido é considerado como prejuízo patrimonial, sem considerar o benefício que a vítima tenha obtido devido à ilícita conduta do agente. Desta forma, tem-se que:

> Artigo 218.° Burla qualificada
> 1 - Quem praticar o facto previsto no n.° 1 do artigo anterior é punido, se o prejuízo patrimonial for de valor elevado, com pena de prisão até cinco anos ou com pena de multa até 600 dias.
> 2 - A pena é a de prisão de dois a oito anos se:
> a) O prejuízo patrimonial for de valor consideravelmente 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 econômica.
> 3 - É correspondentemente aplicável o disposto nos n.os 2 e 3 do artigo 206.°
> 4 - O n.° 1 do artigo 206.° aplica-se nos casos do n.° 1 e das alíneas a) e c) do n.° 2.

Deste modo, caracteriza-se a burla como crime de lesão ou dano, de resultado ou material, sendo considerado um crime muito comum, ou seja, um crime de omissão imprópria ou mesmo de conduta associada que é dependente de queixa no âmbito vinculado aos crimes semipúblicos, como um crime doloso. O dolo eventual também é admissível (Pereira & Lafayette, 2014).

Diante deste contexto, tem-se que o crime de burla qualificada ainda é caracterizado como um crime de resultado (referente à maneira de consumação da investida ao objeto da ação) e como um crime de dano (com relação ao nível de dano do bem jurídico protegido) (Marques, 2019).

De acordo com o estudo de Faria (2019), nota-se que o tipo de burla qualificada, conforme previsto no art. 218º do Código Penal, seguiu a mesma linha do tráfico de estupefacientes, isto é, um ato ilícito penal que é dominante na pendência relacionado ao juízo criminal central da cidade de Lisboa.

Também de acordo com Faria (2019), tem-se que ao considerar sobre as regras de competência referente ao tribunal coletivo, essa seara compreende um exclusivo domínio da burla qualificada, visto que a burla simples possui punição com a presença de um limite máximo que seja menor do que cinco anos. Pelo o que foi constatado, tem-se que essa qualificação sempre esteve vinculada com o prejuízo patrimonial que possui alto valor, mas na maior parte dos casos, ascendendo a centenas de milhares de euros. Entretanto, tornou-se plausível fazer uma análise de outras circunstâncias e que outros

motivos fundamentavam a qualificação da burla, tais como o fato de o agente fazer da vítima o seu modo de vida ou a própria vulnerabilidade da vítima.

Logo, de acordo com a associação entre os tipos penais referente à burla qualificada e burla simples, insere-se o entendimento de uma relação de especialidade que possui concurso aparente, tendo em conta que essa situação representa um tipo especial e fundamental, por conseguinte, as duas normas são convocadas nessa situação, não podendo acarretar apenas um concurso aparente, à proporção que a burla qualificada (tipo especial) insere essenciais elementos da burla simples (tipo fundamental), bem como insere elementos especiais (Santos, 2017).

4.2.2 Burla relativa ao trabalho

De maneira efetiva, trata-se de um tipo legal de crime que não tem sido muito estudado, seja sobre a jurisprudência, seja pela doutrina, visto que as únicas referências que lhes foram atribuídas direcionam-se para os comentários contidos no Código Penal, e são escassas as decisões realizadas nos Tribunais que puderam fazer a convocação da aplicação desse Código aos casos concretos que puderam ser submetidos à sua apreciação (Fidalgo, 2017).

De fato, tem-se que o crime de burla referente ao trabalho possui como base o art. 217º (Emigração) associado ao Projeto de Revisão do Código Penal do ano de 1966; entretanto, somente no ano de 1998, com a Lei n° 65/98, de 2 de setembro, e o mesmo introduziu efetivamente a disposição no ordenamento português. Esse fato ocorreu por causa do art. 217º, que não havia sido acolhido no Código Penal do ano de 1992, tendo em vista que somente a emigração legal estava inserida. Todavia, este tipo legal foi posteriormente reportado tanto com relação à emigração clandestina quanto à emigração legal, enfatizando para que não apenas o agente atue com o objetivo de ter um ilegítimo enriquecimento (alheio ou próprio), bem como a ocorrência de um prejuízo efetivo do patrimônio alheio, estando assim de acordo com o tipo legal contido no art. 222º (Pereira, 2018).

Segundo a reforma do ano de 1998, nota-se que houve modificações expressivas para o tipo legal, devido às condições caracterizadas como infra-humanas, ou seja, as vítimas se iludem com a promessa de poderem trabalhar no exterior. Assim, com base nos termos do art. 222º e até os dias atuais, tem-se que o tipo legal começou a criminalizar a promessa ou aliciamento de emprego ou trabalho no exterior para a pessoa residente em Portugal, ou mesmo de emprego ou trabalho em Portugal para a pessoa que reside no exterior. Desta maneira, tem-se que o agente age com o intuito de enriquecer de maneira ilícita, e esse enriquecimento é devido ao engano ou erro que

especificamente recai sobre uma promessa de emprego ou trabalho no exterior (Pereira, 2018).

Desta forma, tem-se que o agente consegue convencer a vítima para que a mesma possa trabalhar na Espanha com a presença de uma promessa de remuneração, para explorar a vítima em seguida, fazendo com que a mesma esteja sujeita a condições infra-humanas, e o agente recebe a remuneração para si, e esse crime se caracteriza como crime de burla com relação ao emprego ou trabalho com base no Acórdão do Tribunal da Relação do Porto de 27-11-2013 (Pereira, 2018).

De forma curiosa, nota-se que em um dos escassos acórdãos que foram encontrados referentes a esse tipo legal de crime, há o acórdão do Tribunal da Relação do Porto, 27 de novembro de 2013, que foi relatado pelo Juiz Desembargador Augusto Lourenço, Proc. 322/04.1TAMLG.P1, estando disponível em www.dgsi.pt. Nesse acórdão, assegura-se a compreensão de que com a sua criação, houve a intenção de fornecer repostas pelo legislador para as políticas criminais e anseios sociais, visto que essas políticas nutrem sobreposições normativas e representam apenas uma demagogia pura, motivo pelo qual a burla relacionado com o não emprego ou trabalho não deveria existir (Fidalgo, 2017).

Com relação ao confronto entre o tipo legal de crime de burla vinculado a emprego ou trabalho e o tipo legal de crime de burla (art. 217º do Código Penal), nota-se que é verificada a similaridade entre esses tipos legais de crime, e mesmo o intérprete mais distraído consegue perceber isso (Fidalgo, 2017).

Por fim, não se verifica essa similaridade somente com o tipo legal de crime, ou seja, o crime “matriarcal” de burla, mas é possível encontrar uma comparação entre os crimes de burla do tipo legal relacionado com emprego ou trabalho e os crimes que estão previstos no Título I da Parte Especial do Código Penal “Dos crimes contra as pessoas”, e de forma mais concreta no Capítulo IV “Dos crimes contra a liberdade pessoal”, em que está contido o crime relacionado com o tráfico de pessoas (art. 160.º do Código Penal) (Fidalgo, 2017).

4.2.3 Burla tributária

De fato, tem-se que o crime relacionado com burla tributária (art.° 87 Regime Geral das Infrações Tributárias (RGIT)) acontece quando uma pessoa através de falsificação, viciação de documento que seja relevante fiscalmente, falsas declarações, ou de outros meios de fraude consegue determinar a administração da segurança social ou administração tributária para que a mesma possa realizar atribuições patrimoniais que acarretarão enriquecimento de terceiro ou do próprio agente (Barros, 2020).

Esta forma, tem-se que a burla tributária aborda um tipo de burla mais evoluída, sendo considerada até mesmo sofisticada em poder captar o bem do outro, em que o agente se beneficia do engano ou erro, por meios astuciosos, de burlar em seu benefício a Administração Tributária, caracterizando-se como um tipo novo de fraude fiscal qualificada, voltadas para os casos mais graves (Gasalho, 2013).

Então, nota-se que o tipo legal relacionado com a burla tributária foi trazido pelo Regime Geral das Infrações Tributárias (RGTI), sendo uma inovação, encaixando-se no setor da nova categoria de classificação voltada para os crimes comuns tributários, porém, apenas desde a validade deste diploma foi que esse tipo de burla se caracterizou como um crime autônomo no âmbito do direito penal fiscal, principalmente por motivos pragmáticos (Gasalho, 2013).

Diante deste panorama, conforme explicado por Ferreira (2018), verificou-se que é evidente que, referente ao ordenamento jurídico de Portugal, que um dos desafios mais expressivos precisamente deve passar pela diferenciação entre a fraude fiscal e a burla tributária, demonstrando que é um assunto não muito abordado, e desta forma suscitando a vontade e curiosidade de englobar a responsabilidade vinculada com uma análise mais detalhadas dos crimes em pauta, facilitando o correto, em situações futuras, ou no mínimo tornando menos complicado o enquadramento jurídico.

De acordo com o estudo de Jesuíno Alcântara Martins (2013), tem-se que há uma notória diferença entre a burla tributária e a fraude fiscal, visto que na burla não há uma diminuição relacionado com as receitas tributárias, existindo somente a extorsão de valores presentes no tesouro público; ao passo que na fraude fiscal, o agente intenciona diminuir os impostos a liquidar ou as receitas tributárias com sua conduta ilícita.

Desta forma, verifica-se a formação deste novo delito relacionado intrinsicamente à abundante e frequentemente cacofônica discussão que se instalou na década de 1990 no meio da sociedade sobre o crime de fraude fiscal, que estava na época previsto no art. 23º do Regime Jurídico das Infrações Fiscais Não Aduaneiras (RJIFNA). De acordo com as palavras de Germano Marques da Silva (2009), autor do anteprojeto relacionado com o RGIT, o mesmo destacou que o crime de burla pôde ser inserido no RGIT como um tipo de crime tributário por motivos conjunturais. Foi somente para pôr termo o assunto polêmico que o RGIT tornou independente o crime de burla.

Perante este panorama, tem-se que uma das inquietações que motivou o legislador no ano de 2001, na passagem de outros diplomas fiscais penais voltados para o RGTI e do RJIFNA, foi sanar e ultrapassar as dúvidas que permeavam a aplicação e interpretação do crime relacionado com a fraude fiscal diante a previsão de um novo perfil de incriminador, ou seja, a burla tributária, que pudesse atribuir um equivocado relevo específico penal voltado para atos de fraude que acarretassem uma lesão do

patrimônio fiscal. Pela Exposição de Motivos da Proposta de Lei n° 53/VIII, foi abertamente aberto esse propósito com base no RGIT, em que no âmbito fiscal, um tipo autônomo relacionado com a burla fiscal é introduzido, com a possibilidade de pôr termo à duvidosa doutrina que tem permeado a repressão penal de algumas defraudatórias práticas associadas com a administração tributária (Dias & Brandão, 2015).

Desta forma, tem-se que o crime de burla tributária visa ter uma fonte de inspiração no crime de burla comum, conforme previsto no art. 217º do Código Penal, fazendo uma reprodução sobre o que é fundamental, mesmo que apresente importantes peculiaridades. De acordo com o que foi afirmado pelo STJ contido no Acórdão de 07-05-2003, Proc. n° 99P735, nota-se que a tipicidade possui específicas características referentes ao crime fiscal sobre a maneira fraudulento; no entanto, busca inspiração na burla comum sobre o enriquecimento de terceiro ou do próprio agente (Gasalho, 2013).

Deste modo, nota-se que o legislador de Portugal, em vez de empregar distintos ordenamentos jurídicos que priorizassem uma cláusula geral referente à fraude fiscal que englobasse uma abrangência dos comportamentos criminais no setor relacionado à delinquência fiscal (como exemplo o ordenamento jurídico da Espanha), fez a opção de formular um tipo legal de aspecto tributário que pudesse fazer a previsão do constitutivo comportamento vinculado com a burla comum, com a presença de suas peculiaridades. Todavia, muitas críticas têm sido abordadas sobre a autonomia deste tipo novo de crime, no âmbito de não ter a justificativa inserida em um contexto metodológico e técnico-legislativo para sua consagração. Entretanto, o fato é que a tese que prosperou foi àquela relacionada com a autonomização, conforme descrito na Exposição de Motivos da Proposta de Lei n° 53/VIII: foi introduzido no campo fiscal um tipo autônomo referente à burla fiscal, com a capacidade de pôr termo à doutrinária incerteza que tem permeado a repressão penal associada com algumas práticas de fraude da administração tributária (Gasalho, 2013).

Com relação à pena, deve-se destacar que a redação inicial que foi fornecida pela Lei n.° 15/2001 ao n.° 2 relacionada com o crime de burla tributária que está previsto no artigo 87.° do RGIT, compreendia a concepção de que se fosse de alto valor a atribuição patrimonial, deveria ser aplicada uma multa de até 600 dias ou pena de até cinco anos de prisão. Nos dias de hoje, tem-se que a redação relacionado com esse mesmo n.° 2 do artigo fornecido pela Lei n.° 64-B/2011, reside na ideia de que se for elevada a atribuição patrimonial, deve-se aplicar uma multa de 240 a 1200 dias para pessoas coletivas, e uma pena de prisão de um a cinco anos para pessoas singulares (Costa, 2019).

Então, além da diferenciação da pena que precisa ser aplicada para pessoas coletivas e singulares, verificou-se que houve um crescimento do limite mínimo

relacionado com a pena de prisão que estava prevista inicialmente, bem como um crescimento dos limites máximo e mínimo da pena vinculada à multa, visto que nos termos contidos no art. 12º do RGIT há presença dos limites de penas de multa e de prisão, e quando nada é especificado sobre os tipos, compreende-se o período de 10 a 600 dias e até oito anos de prisão para pessoas singulares, e de 20 a 1920 dias voltados para as pessoas coletivas (Costa, 2019).

Diante deste contexto, tem-se que Costa (2019) abordou o tema para que fosse possível aplicar esse regime ao crime tributário continuado ou crime continuado, e nota-se que pode acontecer que o arguido não tem a possibilidade de ter um benefício da aplicação retroativa referente à lei penal que seja mais adequada, quando existem alterações nos limites de pena, com base na percepção que se esperaria. Este fato acontece porque, através da alteração da sanção, nota-se que a pena aplicável pode ser mais favorável no âmbito da lei nova, entretanto, diante situações em que diversos tipos penais compreendem a unidade jurídica, considerações precisam ser feitas.

4.3 BREVES CONSIDERAÇÕES FINAIS

Mesmo com a presença de um elo comum entre a herança do direito de Portugal oriunda desde os tempos coloniais e o sistema romano-germânico, nota-se que a legislação do Brasil pôde evoluir ao longo dos anos sob influência de distintas vertentes.

Desta forma, as distinções partem desde as nomenclaturas sobre as formalidades e acabam passando pelos ritos processuais e organização judiciária.

Nota-se que o estelionato se converte em burla, Tribunal de Justiça converte-se em Tribunal de Relação; um defensor dativo pode se converter em um oficioso; Visitas, alimentos e guarda convertem-se somente em responsabilidades parentais; Fórum converte-se em Tribunal; Medida socioeducativa converte-se em medida tutelar educativa; Extinção sem a presença de resolução de mérito converte-se em absolvição de instância. Perante diversas diferenças, pode ser frequente a dúvida sobre a correspondência dos conceitos (Rodrigues, 2017).

Aliás, acontece tanto em Portugal quanto no Brasil um processo relacionado com a adaptação de um “Novo Código de Processo Civil (CPC)”, denominado desta forma pelos dois países. O CPC de Portugal de 2013, e do Brasil de 2015.

De fato, as distinções entre os Códigos que foram pesquisados são notórias sobre o crime de estelionato, em especial ao abordar a nomenclatura (crime de burla). Todavia, a diferença não reside apenas nisso. Observou-se que com relação aos crimes de roubo e furto presente no Código Penal de Portugal, o mesmo se caracteriza como o mais moderno sobre a pena de prisão ser designada como *ultima ratio*, tendo em conta que esse Código consegue fazer uma previsão das penas menores para um

determinado crime que possui uma definição idêntica presente em todos os códigos penais que foram analisados, e dessa forma, também se caracteriza com menor pena referente a outros crimes abordados, visto que esses foram apaziguados anteriormente com o advento da modernidade (Hobaica, 2016).

Por fim, tem-se que o Código Penal Brasileiro se diferencia dos outros Códigos referentes à vertente da valoração dos meios utilizados para o estelionato, distinguindo as penas de um crime que têm um perfil mais simples para um perfil mais complexo. Com relação ao valor do bem material, independentemente do valor, mas que o mesmo não seja ínfimo, o mesmo ocorre na maioria das penas aplicadas.

5 CRIMES INFORMÁTICOS (GOLPES APLICADOS NA INTERNET / DELITOS INFORMÁTICOS / CIBER CRIMES / CRIMES VIRTUAIS / CRIMES DIGITAIS / CIBERCRIMES / DADOS PESSOAIS)

José Lagatheaux, em um evento para a imprensa em 1994, apresentou a internet em Portugal. Passados os anos, atualmente, a internet e as redes sociais são parte do cotidiano de milhares de portugueses, representando um meio de transformação na comunicação. Trata-se de uma “revolução digital” que impactou diversas áreas, entre elas, o plano criminal, que passou a utilizar os sistemas informáticos e a web rede como instrumentos para a prática de ilícitos penais. Como consequência, viu-se o surgimento do conceito de crime informático, também denominado cibercrime (Ferraz, 2020).

Vale ressaltar que, para se referir ao uso do computador como base, instrumento ou meio de ação ilícita, existem vários termos, tais como crime digital, crime eletrônico, cibercrime, crime virtual, crime informático, entre outros (Silva, 2017).

Um dos motivos quem tem levado ao crescimento da criminalidade no meio virtual é a visão deste espaço como passível de impunidade aos delitos. Importa dizer que a criminalidade informática abarca quaisquer infrações exercida por meio informático, não focando apenas aquelas que tratem do elemento digital como parte formadora do seu tipo legal ou matéria de proteção (Santos, 2020).

Algumas características inerentes ao ciberespaço o tornam um ambiente propício à prática de crimes, tais como a possibilidade de anonimato, o acesso global e a escalabilidade. São propriedades desse meio que demandam dos responsáveis vistoria e manutenção constante da segurança e o empenho no combate ao e-crime. Em Portugal, por exemplo, a estimativa é que, até 2026, essa prática ilegal represente 10% das ocorrências de delitos no país (Correia & Jesus, 2016).

De acordo com o relatório de cibersegurança em Portugal (2020), as tecnologias emergentes, dentre as quais estão a internet das coisas, as plataformas em nuvem, o 5G e a inteligência artificial, são tendências mundiais crescentes e, com elas, se elevam também os vetores de ataque, a imprevisibilidade dos métodos de segurança nesses meios a nível global e os impactos de práticas ilícitas como as ciberameaças. O relatório indica também que o contexto da pandemia de COVID-19 também proporciona algumas mudanças, como o desaceleramento de determinadas tecnologias, o risco de exposição de dados pessoais, o crescimento de ataques na web rede, ameaça a serviços e infraestruturas necessárias, mas críticas, e a possibilidade do uso político das

decorrências da crise sanitária por meio da desinformação e/ou da desestabilização política e social (Portugal, 2020).

Segundo explicação de Costa Andrade e Figueiredo Dias (1997), dois critérios são necessários para enquadrar como crime determinado comportamento: primeiro, que a ação seja danosa socialmente e, segundo, que existam previsões legais das sanções possíveis. Em Portugal, de acordo com Amador (2012), a recente Lei do Cibercrime foi a responsável por estabelecer aplicabilidades a esse tipo de delito nos campos do direito processual e do direito penal material.

Também cabe discorrer que o fato típico é composto dos elementos tipicidade, conduta, nexo causal e resultado. A relação de contrariedade entre a norma legal e o fato configura a antijuridicidade. No contexto brasileiro, o direito penal abarca algumas hipóteses nas quais a antijuridicidade é excluída, quais sejam, estado de necessidade, legítima defesa, exercício regular do direito e o cumprimento estrito do dever legal (Lima, 2018).

À reprovabilidade decorrente de um ato ou omissão típica e ilícita chama-se culpabilidade. Conforme a normal penal brasileira, a decisão pela aplicação de uma pena depende da imputabilidade do agente, ou seja, deve-se verificar a consciência da ilicitude da ação executada bem como da existência de possibilidade de evitar esta ação na circunstância em que ela foi cometida. Desse modo, diz-se que o direito penal centra sua visão no comportamento do indivíduo. De acordo com a teoria tripartida, depois de tipificar a conduta que, por meio ou contra um dispositivo informático, prejudica ou ameaça o bem jurídico, deve-se constatar a existência desses três elementos qualificativos (Lima, 2018).

5.1 CONCEITO DE CRIMES INFORMÁTICOS

O conceito mais claro e objetivo de delito informático o define como uma ação ilícita e típica qualificada como contravenção ou crime, culposo ou doloso, omissivo ou comissivo, de autoria de pessoa jurídica ou física, por meio da informática, ofendendo, seja na rede ou não, diretamente ou não, a segurança de dados e informações, ferindo a integridade, a confidencialidade e a disponibilidade destes. De maneira resumida, tratam-se de comportamentos transgressores da ética e da moralidade pelo dinamismo da tecnologia, sendo que os agentes ativos e passivos são os usuários das plataformas virtuais (Mesquita Filho, 2020).

Visto que é apenas virtualmente que se pode ocorrer a invasão de dispositivos informáticos e a violação de mecanismos de segurança, então, diz-se que o meio eletrônico é o elemento do tipo objetivo. Desse modo, há uma unanimidade no entendimento de crimes digitais próprios a elaboração e disseminação de vírus e demais

códigos danosos, a invasão bem como a destruição de bancos de dados, sejam eles privados ou públicos (Escóssia, 2020).

No Brasil, o ano de 2011 foi mercado por diversos ataques de negação de serviço a sites governamentais. Além disso, ficou conhecido o caso da atriz Carolina Dieckmann, que teve fotos particulares roubadas de seus arquivos pessoais e disponibilizadas na internet. Esses fatos contribuíram com o debate acerca do tema e levou à aprovação de leis específicas em caráter de urgência em busca de preencher os vazios legais até então existentes no ordenamento brasileiro quanto aos crimes digitais (Ramos, 2017).

Em novembro de 2012 foram promulgadas as leis n.º 12.735 e n.º 12.737, que tratam, respectivamente, do estabelecimento de órgãos investigativos especializados e da inclusão do tipo penal invasão de dispositivo informático e das regras da ação penal para esses delitos no Código Penal, representados pelos arts. 154-A e 154-B, nessa ordem. Ademais, a Lei n.º 12.737/2012 modificou a redação de dois crimes já previstos nos arts. 266 e 298 desse mesmo documento, que discorrem sobre a perturbação ou interrupção de serviços informáticos, telefônicos, telegráficos, telemáticos ou de dados de utilidade pública (o primeiro) e sobre a falsificação de documento pessoal, incluindo, após a alteração, os cartões de crédito e débito (o segundo) (Ramos, 2017).

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (Lei n. 12.737, 2012).

São duas as finalidades não cumulativas do crime relatado: uma é o ato da invasão do dispositivo informático a partir de uma violação do aparato de segurança tendo em vista deter, alterar ou destruir informações e dados; a outra refere-se à invasão cujo objetivo é instalar vulnerabilidades no sistema a fim de conseguir benefícios ilícitos (Meloto, Soares, & Chaia, 2020).

No que diz respeito à aplicação do delito de dano à destruição, deterioração ou inutilização de sistemas ou arquivos digitais, verifica-se que existem divergências na doutrina (Santos, 2011). Souza Neto (2009) cita Ivanete Senise Ferreira, que defende o estabelecimento do dano informático, ou seja, um novo tipo penal.

O cerne do tipo consiste na invasão de dispositivos informáticos de terceiros sem consentimento – ou seja, não se pode falar em fato típico caso esse acesso se dê com autorização do responsável para, por exemplo, realizar algum tipo de conserto do equipamento. É um crime formal já consumado unicamente pelo acesso não concedido a um dispositivo informático alheio, não havendo a necessidade de que os dados nele

encontrados sejam roubados ou danificados nem que algum tipo de vírus seja instalado. Caso isso ocorra, constata-se a incidência do disposto no §3° da Lei n.º 12.737/2012 (Maues, Duarte, & Cardoso, 2018):

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave (Lei n. 12.737, 2012).

Vê-se que o crime tem sido considerado pela doutrina finalista moderna do direito penal como um comportamento típico, antijurídico e culpável. No que se refere ao e-crime, entende-o, desse modo, como um ato típico, antijurídico e culpável cometido pelo ou contra o uso de processamento automático de informações e dados ou sua disseminação. Ou seja, referem-se às ações que utilizam ou prejudicam de modo ilegal dados guardados ou tramitados em dispositivos informáticos (Thomas, 2010).

A doutrina entende que núcleo e objeto protegido de condutas já tipificadas não são alterados pelo surgimento de um novo meio de agir nessa ilegalidade. Sendo o sistema informático um novo meio para a execução do crime, o que ele poderá promover é a qualificação da conduta e outros estabelecimentos de pena, no entanto não se vê mudanças no tipo penal (Santos, 2011).

Então, é fundamental compreender que a lei penal em vigor no ordenamento jurídico do Brasil ampara pessoas físicas e jurídicas estabelecendo punição ao agente responsável por ações danosas aos dados armazenados em bancos públicos ou privados e à proteção de programas de dispositivos informáticos. Além disso, também é possível mencionar delitos que, embora não dispostos na mencionada Lei n.º 12.737 de 2012, são contemplados pela Lei n.º 9.983/2000, que trata de crimes eletrônicos, sobretudo abordando os dispositivos informáticos. Os arts. 313-A e 313-B dessa lei, por exemplo, narra sobre os peculatos eletrônicos (Machado, 2017).

Os delitos dispostos nos mencionados artigos são considerados crimes próprios cometidos contra a administração pública, nos quais só poderão ser responsabilizados funcionários públicos, permitindo a participação de um particular apenas como coautor. O primeiro, o art. 313-A, ampara os dados arquivados em sistemas informatizados usados por órgãos públicos; já o 313-B protege os programas instalados nos equipamentos da administração pública (Machado, 2017).

Importa ressaltar que o alvo da tutela é a liberdade individual dos indivíduos, tendo em vista a inviolabilidade de segredos. Além disso, vale dizer também que, para que exista, esse crime precisa ser praticado dolosamente. A tentativa é possível e se dá pelo fato de o crime ter caráter plurissubsistente e, portanto, permitir o fracionamento do

intercrimini. Por exemplo, quando são realizadas manobras para invadir o dispositivo informático alheio objetivando destruir dados, mas estas não funcionam por conta de métodos de proteção ao equipamento implantados pela vítima (Maues et al., 2018).

No cenário internacional, frente ao crescimento da criminalidade informática, foi adotada a Recomendação n.º R (89) 9 pelo Comitê de Ministros dos Estados-Membros do Conselho da Europa, estabelecida no segundo semestre de 1989. Tal recomendação trazia duas listas de incriminações: uma mínima, que apresentava as condutas de punição obrigatória pelos direitos específicos dos Estados-Membros; e outra cujas tipificações eram optativas. A primeira dessas listas é aquela que mais se aproxima do que veio ser a construção típica desse crime em Portugal (Pedra, 2019).

São as leis nacionais de transposição que determinam a criminalização da violação de dados não autorizados. No contexto português, a transgressão de regras de controle previstas, de natureza técnica ou não, são classificadas como crime no art. 2 da lei específica, seguindo a Convenção de Budapeste, que diz que os Estados-Membros deverão implementar as medidas legislativas e quais mais se mostrarem necessárias para tipificar o acesso ilícito a um dispositivo informático ou aos seus sistemas. É permitido que, para confirmar o crime, as partes exijam que a conduta seja atuada pela violação dos procedimentos de segurança objetivando acessar dados informáticos ou alcançar outros intentos, ou que ela seja relacionada a sistemas informáticos em rede, sendo que o art. 6º da Lei do Cibercrime determina como crime o acesso não autorizado a um sistema informático (Pereira, 2020).

Verificam-se partes processuais e substanciais de regulamentação na Convenção de Budapeste, que instrui seus alinhados a adotar medidas que criminalizem os delitos que ajam contra a disponibilidade, integridade e confidencialidade dos dados arquivados em dispositivos e sistemas informáticos, incluindo nessas infrações o acesso não autorizado, a interferência nos sistemas, a interceptação de transmissão não público e a utilização indevida de equipamentos informáticos (Liu, Travers, & Chang, 2017).

Brevemente, quanto à criminalização de ações danosas em meios digitais e informáticos, a legislação portuguesa, pela Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de agosto), trouxe acréscimos a já existente Lei da Proteção de Dados Pessoais face à Informática, de n.º 10/91 (Costa, 2017).

A Lei da Criminalidade Informática dispôs redações acerca da cooperação entre países em matéria penal, tratando do e-crime e da coleta de indícios de violações em suportes digitais e, também, determinando as penas materiais e processuais para esses casos. As mudanças advindas com a promulgação dessa lei trouxeram as definições das disposições materiais, quais sejam o dano referente a programas e/ou outros dados

informáticos, a falsidade informática, o acesso e a interceção não autorizados, a sabotagem informática e a reprodução ilícita de programa protegido (Caiado, 2020).

De modo semelhante, no dia 24 de agosto de 2017 foi estabelecida a Resolução do Conselho de Ministros (RCM) n.º 115 – fundamentada em uma resolução de 2015, a RCM n.º 36 –, que, objetivando aprimorar a segurança das redes e dos dados e assegurar a proteção as infraestruturas críticas (IC) e aos serviços essenciais de informação, aprovou a Estratégia Nacional de Segurança do Ciberespaço (ENSC). Compreende-se, portanto, que a RCM n.º 115/2017 buscou promover uma estratégia para proteger as tecnologias da informação e comunicação (TIC), entendendo que tanto Estado como a sociedade estão atrelados a essas tecnologias, que promovem tantos benefícios e, ao mesmo tempo, oferecem riscos (Caiado, 2020).

Entretanto, esse regime internacional não se mostrou suficiente e, portanto, os Estados incluíram medidas de amplitude extraterritorial em suas legislações de investigação criminal. No caso de Portugal, o art. 19 da Lei do Cibercrime permitiu ampliar o registro de um equipamento informático aos demais sistemas possíveis de serem acessados pelo primeiro, rompendo as limitações territoriais, já que tais sistemas podem se encontrar em territórios estrangeiros (Martinez, 2019).

É incontestável a tendência crescente do crime informático, sendo este, hoje, um dos delitos de grande representação dentre os crimes investigados em Portugal. A proliferação e os meios e formas de execução dessas infrações estão em ascensão. Constata-se que a criminalidade em meios informáticos não se resume àqueles mencionados na Lei do Cibercrime, existindo também outros, como o crime de burla informática e nas comunicações e o crime de devassa por meios informáticos, tais como descritos, respectivamente, nos arts. 221 e 193 do Código Penal (CP). Outros exemplos são aqueles que não necessitam obrigatoriamente do meio informático para serem cometidos, mas que, no entanto, vê-se crescente utilização dessas plataformas em suas ações, como os crimes de ameaça, injúria e difamação, também pontuados pelo CP (J. Freitas, 2017).

Neste interim, ao tratar de crimes cibernéticos, são fundamentais a definição e a qualificação das condutas. Os e-crimes podem ser separados em crimes próprios e impróprios. Os primeiros são aqueles cujas ações são realizadas, independente das motivações, contra um sistema informático; já os segundos são os que agem por meios informáticos para prejudicar outros bens jurídicos (Santos, 2020).

5.2 TIPIFICAÇÃO DOS DELITOS INFORMÁTICOS

Como explicado anteriormente, os crimes de informática são divididos entre aqueles direcionados contra um sistema de informática – ou seja, ações contra o próprio

material: dados arquivados em computadores ou os suportes lógicos – e os que agem danosamente em outros bens jurídicos ou valores sociais a partir de sistemas informáticos (Alves Neto, 2019).

De modo diferente, Rita Coelho dos Santos (2005) apresenta três divisões para essa criminalidade: 1) crimes tipicamente informáticos, os quais têm como instrumento ou objeto de ação o dispositivo informático, sendo este um requisito fundamental; entre eles, a autora destaca o crime de sabotagem informática; 2) crimes essencialmente informáticos, configurados como aqueles que ofendem uma realidade informática, como um telemóvel ou um programa computacional; destes, ela menciona a reprodução ilegal de programa protegido, como um software, por exemplo; e 3) crimes acidentalmente informáticos, que utilizam os instrumentos da informática como novo modo de cometer delitos já previstos; como os já mencionados crimes de difamação e injúria.

5.2.1 Comuns

Os crimes virtuais comuns são aqueles que, a partir de ferramentas comuns, violam o meio informático em si. É o que ocorre quando o agente utiliza um martelo para destruir um equipamento, por exemplo, danificando as informações nele contidas. O alvo, portanto, é físico, mas o resultado é a violação de dados (Costa, 2019).

Em definição distinta, Humelnicu (2016) define os crimes virtuais comuns como aqueles que recorrem à internet como meio para a execução de um crime já estabelecido por lei. Desse modo, o meio informático se mostra como apenas mais um instrumento para a ação ilícita.

5.2.2 Próprios e Impróprios

Há uma grande variação de classificações dos e-crimes, mas a mais usual é aquela que os divide em crimes efetivados contra um sistema informático – os próprios – e os que agem prejudicialmente a outros bens jurídicos – os impróprios). Tais divisões, portanto, levam em conta o bem jurídico atingido pelo ato ilícito (Crespo, 2011; Ferreira, 2011). Fiorillo e Conte (2016) também contribuem explicando que os crimes virtuais próprios são aqueles cujo alvo são programas informáticos (software) ou partes físicas do dispositivo informático (hardware).

Importa ressaltar que essa divisão dos crimes cibernéticos em próprios e impróprios não equivale à classificação vigente no direito penal, que usa os mesmos termos para definir os crimes segundo o sujeito ativo, que entende o crime próprio como aquele que demanda uma condição especial do agente que cometeu o delito – como exemplo, pode-se mencionar o crime de peculato, cujo responsável pelo delito só poderá ser um funcionário público (Ferreira, 2011).

Os crimes virtuais próprios, então, atingem o meio informático em si e utilizam para tal necessariamente o meio informático. É o que acontece, por exemplo, quando se inclui ilegalmente um código em um computador de terceiro para impedir que o usuário acesse determinados arquivos (Costa, 2019).

Nesse tipo de crime, portanto, os alvos são bens jurídicos entendidos como sistemas de telecomunicações ou dados ou sistemas informatizados. São ações danosas ao dispositivo informático e ao seu hardware bem como contra os dados e programas armazenados nesse dispositivo (Silva, 2017).

Os crimes virtuais impróprios, por sua vez, se caracterizam como aqueles que recorrem ao equipamento informático como ferramenta para sua efetivação. São, desse modo, ilícitos já tipificados pela lei e que ganharam o meio informático como novo modus operandi. Portanto, nesse tipo de crime, o responsável pelo delito utiliza o computador – ou outro dispositivo informático – para ofender o mundo físico, ou seja, ameaçando ou danificando bens que não da informática (Souza, 2020).

5.2.3 Mistos

Entende-se como crime virtual misto aquele que recorre ao meio informático como ferramenta para lesar um bem não informático. Por exemplo, o envio de um e-mail com conteúdo falso que pretenda convencer o destinatário a depositar dinheiro ao remetente (Costa, 2019).

O dispositivo informático, portanto, é requisito para a prática do delito, como se ocorre em crimes que buscam a transferência ilícita de valores, como mencionado no parágrafo anterior, ou aqueles que intentam retirar pequenas quantias de dinheiro em contas variadas (Damiani, 2019). Nestes últimos casos, o valor retirado da conta é ínfimo para o correntista, o que faz com que, em muitos dos casos, ele sequer perceba que foi lesionado, mas, somadas todas as contas subtraídas, o montante acumulado pelo cibercriminoso é alto. Nesse exemplo, o agente do crime utiliza a internet para executar um delito já estabelecido legalmente, configurando o tipo penal de crime virtual comum (Alves Neto, 2019).

5.3 ESPÉCIES DE CRIMES INFORMÁTICOS

Muito embora Portugal não registre grandes quantidades desse delito, a prática de crimes cometidos utilizando o serviço de e-mail é uma realidade, e já existem diversas decisões de tribunais superiores que a revelam. Por exemplo, o Tribunal da

Relação de Coimbra, em 2016, no Acórdão n.º 902/13.4TBCNT.C1[1] debateu o risco advindo da prática de phishing, ilícito cometido a partir do envio de mensagens por e-mail, os spams, objetivando coletar senhas, PINS e outras informações pessoais dos receptores. Em 2014, o Tribunal da Relação do Porto[2] constatou a possibilidade de invadir uma conta de e-mail para disponibilizar ilegalmente dados e informações particulares dos proprietários das contas lesionadas.

A partir do entendimento da possibilidade de um indivíduo recorrer a aplicativos ou ferramentas para se passar por outra pessoa física ou jurídica para conseguir informações como senhas, números de cartão de crédito etc. surgiu o conceito de fraude eletrônica. Geralmente, esse crime é cometido por meio de envio de e-mail visando obter dados pessoais do destinatário (Aguiar, 2017).

No caso de Portugal, por exemplo, há uma diferença significativa entre os pontos de vista penal e civilístico sobre a fraude no homebanking. Nos termos penais, somente o responsável pela ação poderá ser punido pelo crime, já no que se refere aos termos civilísticos, há presunção de culpa sobre a instituição bancária, a não ser que o próprio cliente (dono da conta violada) tenha permitido as movimentações em sua conta, seja por negligência, seja por dolo (Alves, 2019).

Desse modo, se o banco não conseguir provar que, no decorrer do delito, o cliente foi informado sobre a fraude, ou caso o proprietário da conta não for provido de conhecimentos eletrônicos, ou se este tiver avisado a instituição bancária assim que soube das movimentações ilícitas, nesses casos, entende-se negligência leve da prestadora de serviço, conforme o previsto no RSP, art. 115, n.º 1 (Alves, 2019).

Para os crimes de furto de identidade, também recorrentes nos meios informáticos, Portugal define como crime. Aliás, esse furto, bem como a utilização de identidade de terceiros, correspondem a mais de um tipo de delito. A punição nos casos

[1] Acórdão do Tribunal da Relação de Coimbra de 02-02-2016, com o seguinte sumário: “Não se tendo provado que o cliente forneceu a terceiros (ao aceder a página ilícita) as chaves de acesso ao serviço de home banking nem que, ao navegar na inter-net, permitiu que outrem tenha capturado as credenciais de acesso e validação, recai sobre o banco a responsabilidade pela movimentação fraudulenta da sua conta bancária, através da internet (Serviços Homebanking)” (Acórdão do Tribunal de Coimbra, 2016).

[2] Acórdão do Tribunal da Relação do Porto de 08-01-2014, já previamente mencionado, com o seguinte sumário: ”A alínea d) do n.º 2 do art.º 120º do CPP abrange a omissão de atos ou diligências processuais na fase de julgamento e de recurso, que se reputem essenciais à descoberta da verdade. O juízo sobre a essencialidade ou indispensabilidade da diligência de prova cabe ao tribunal e deve basear-se em critérios objetivos, independentes das convicções pessoais dos intervenientes processuais. A sentença é nula quando a fundamentação da convicção for insuficiente para efetuar uma reconstituição do iter que conduziu a considerar cada facto provado ou não provado. O crime de acesso ilegítimo, previsto no art.º 6º da Lei n.º 109/2009, de 15/9, (Lei do Cibercrime), estruturalmente acolhe o crime anterior, previsto no art.º 7º da Lei 109/91, de 17/8, com alterações decorrentes dos compromissos internacionais que Portugal assumiu e, em particular, da Convenção sobre Cibercrime do Conselho da Europa. A factualidade incriminada é exatamente a mesma que era antes, não se exigindo, agora, qualquer intenção específica, por exemplo, a de causar prejuízo ou a de obter qualquer benefício ilegítimo pois que apenas se exige o dolo genérico. O bem jurídico protegido é a segurança do sistema informático. O crime de acesso ilegítimo é praticado por quem actue de forma não autorizada, concretizando-se por qualquer modo normalmente idóneo de aceder a um sistema ou rede informáticos. O crime de devassa por meio de informática, previsto no art.º 193º do C. Penal, decorre do art.º 35º, n.º 3, da CRP, e visa proteger a reserva da vida privada contra possíveis atos de discriminação, que a utilização de meios informáticos torna exponencialmente perigosos”.

de roubo e usurpação de identidade ocorrerá quando estas intentarem conseguir outros materiais por meio da extorsão, falsificação, roubo, burla ou phishing. De acordo com o Centro Internet Segura[3], a prática do furto de identidade ocorre em duas partes: 1. As informações pessoais de um sujeito são roubadas, sem a necessidade de contato direto com o infrator; 2. Os dados obtidos são utilizados por um terceiro para cometer ilícitos. Por isso, é fundamental que os usuários da internet tenham consciência dos benefícios desse meio, mas também dos riscos aos quais estão expostos na web rede (Sá, 2017).

De modo mais específico, o roubo de identidade digital configura a obtenção, a posse e o compartilhamento não autorizados dos dados privados da vítima a fim de usá-los em atos fraudulentos. Cabe mencionar que, tendo sido obtidos pela internet ou por meio diferente, chamam-se de furtos de identidade on-line quando esses dados são transferidos pela internet ou utilizados em práticas criminosas. Contudo, nos casos em que apenas uma dessas condutas é constatada (a obtenção, ou a posse ou a utilização), o furto de identidade digital é caracterizado quando a ação é realizada pela internet. Com o objetivo de apoiar as vítimas desse tipo de delito, a Associação Portuguesa de Apoio à Vítima (APAV) criou, em 2015, o Projeto Proteus, que busca meios, também, para informar e prevenir os indivíduos acerca da criminalidade informática (Sá, 2017).

O atual contexto da sociedade da informação facilita as práticas que intentam interromper os fluxos informacionais e obter dados de forma não autorizada. Chama-se esse fenômeno de apropriação indevida de identidade, que se amplia na mesma medida em que avançam as tecnologias que o possibilitam. Nesse cenário, alguns países, como os Estados Unidos, o México e a Espanha, criaram regulamentações específicas para a criminalização dessas práticas. A Alemanha, por sua vez, optou por criminalizar unicamente o phishing, que, hoje, caracteriza a forma mais usual de obtenção ilegal de dados. Portugal ainda não estabeleceu um crime autônomo, no entanto já descreveu alguns tipos legais, como a falsidade informática, prevista na LC art. 3º, o prejuízo a programas e dados informáticos, o acesso ilegal e a interceção não autorizada, mencionados no mesmo documento, nos arts. 4º, 6º e 7º, respectivamente. O país já prevê também ações que podem ser configuradas como apropriação indevida de identidade, tais como a falsificação de documentos, a utilização de documentos de terceiros e a falsificação informática. Entretanto, ainda restam práticas digitais desamparadas pela lei, como o phishing e o catfighing (Reis, 2019).

No caso do uso dos meios informáticos para o envio de mensagens injuriosas, o tipo penal executado é o comum, de injúria. O cibercrime deve ter como elemento típico o meio ou bem informático, o que significa dizer que esse meio deve ser penalmente relevante (Simas, 2014).

[3] https://www.internetsegura.pt.

No que se refere à sabotagem, o ataque de DDoS[4] pode ser mencionado como um exemplo, cuja intenção é prejudicar o sistema informático por meio de interrupção ou danificação deste. É um delito que se configura como crime de sabotagem informática, para o qual há previsão na Lei do Cibercrime, em seu art. 5º. A sansão ao responsável poderá variar entre um e dez anos de prisão, caso os sistemas violados sejam de apoio a funções essenciais (Caiado, 2020).

5.4 PROVA NOS CIBER CRIMES

A legislação portuguesa, hoje em dia, regulamenta a prova digital e a sua obtenção em três documentos distintos: o Código de Processo Penal, a Lei n.º 32, de 17 de julho de 2008, que discorre sobre a conservação de dados criados ou tratados em serviços de comunicações eletrônicas, e a Lei n.º 109, de 15 de setembro de 2009, a já mencionada Lei do Cibercrime, que estabelece normas acerca de e-crimes e quaisquer outros delitos cujas provas precisem der recolhidas em meios eletrônicos (Martinez, 2019).

Mann (2018) complementa que esse foi o primeiro diploma a apresentar um regime próprio de obtenção de prova digital, preenchendo os vazios deixados pela Lei n.º 109, de 17 de agosto de 1991, que discorria sobre criminalidade informática e estabelecia um modelo processual aplicável a denúncia de delitos cometidos por meio de um sistema informático ou cujo recolhimento da prova precise ser feira em dispositivos ou sistemas digitais.

A Lei do Cibercrime é mais ampla, apresentando ferramentas que podem ser empregadas em investigações de todos os tipos penais que demandam a obtenção de prova digital. Os arts. 12º a 17º do referido diploma são disposições gerais, o que significa dizer que podem ser aplicados em delitos descritos na própria lei, contudo a aplicabilidade dos arts. 18º e 19º é restringida pelo art. 11º, o que acontece devido ao caráter intrusivo desses dois textos (Mann, 2018).

Os dispositivos informáticos, na atualidade, são amplamente utilizados pela sociedade e, hoje, mostram-se como fonte significativa de evidências em diversas recorrências (Lopes, 2020). Recorrentemente, utilizam-se softwares de anonimização que impedem que o investigador identifique facilmente o responsável pela conduta ilícita, portanto são instrumentos que se mostram como obstáculos às investigações (Ramalho, 2017). É nesse cenário que a Computação Forense se mostra fundamental, empregada nas esferas penal, civil e administrativa de forma a auxiliar o perito na busca por evidências (Lopes, 2020).

[4] Segundo a CERT, estes ataques são “caraterizados por solicitações em massa direcionados para um site ou servidor, fazendo com que ele não suporte as solicitações e fique indisponível, ou seja, impedir que utilizadores legítimos tenham acesso a determinado serviço” (Peres, 2010, p. 33).

No que diz respeito à infiltração digital, assim como o Brasil, Portugal apresenta diversas normas e leis que a abordam. No contexto brasileiro, a infiltração para a investigação de delitos contra o público infantil é abordada pela Lei n.º 13.441, de 2016. Contudo, esse diploma não trata da infiltração digital para os processos envolvendo e-crimes. No caso de Portugal, a Lei de Cibercrimes denomina o agente infiltrado para a obtenção de crimes, denominando-o de "regime de ações encobertas", trazendo-o como meio de repelir os crimes dispostos nesta lei (Valente, 2017). Vê-se que, no Brasil, essa definição não foi considerada, talvez pelo fato de a questão já ser popularizada por juristas e leigos; da mesma forma, não o fez a regulamentação portuguesa, que apenas tratou do assunto a partir da menção ao regime das ações encobertas (Mann, 2018).

Importa ressaltar que, depois de uma série de modificações em torno da criação da Unidade de Combate à Criminalidade Informática, uma estrutura orgânica mais adequada da Polícia Judiciária (PJ) foi publicada em 2016, no Diário da República. Ela seguiu os moldes implementados pela Europol e surgiu não apenas para combater os crimes de abuso sexual infantil na internet, mas também os delitos de burlas informáticas, acesso ilegítimo, fraudes eletrônicas etc. (J. Freitas, 2017).

No caso da União Europeia, há apoio aos países membros em situações de incidentes ou ataques informáticos, sendo que as ocorrências devem ser informadas a Europol ou ao EC3[5] para que as investigações, em conjunto aos policiais dos Estados afetados, sejam iniciadas em busca de encontrar e preservar provas, identificar os responsáveis e, se necessário, garantir o prosseguimento do processo judicial[6] (Caiado, 2020).

Depois da etapa de identificação do responsável pelo ato ilícito e/ou do sistema ou dispositivo informático utilizados para o delito – estes últimos que podem conter informações importantes para a investigação e evidências relevantes a partir de exame e análise, então os dados informáticos são convertidos em provas digitais para compor a tese judicial em teste. No entanto, não é raro que os praticantes desses atos tenham conhecimentos tecnológicos que os permitam eliminar, por vezes até de maneira irreversível, as evidências contidas nos sistemas ou equipamentos investigados, o que fazem por meio de ferramentas de proteção da informação ou pela instalação de

[5] EC3 significa European Cybercrime Centre. "A EUROPOL criou em 2013 o EC3 para reforçar a resposta da aplicação da lei ao cibercrime na UE e, assim, ajudar a proteger os cidadãos europeus, as empresas e os governos, contra a cibercriminalidade, que custa aos EM da UE, 265 mil milhões de euros todos os anos, sendo o prejuízo para a economia global, de cerca de 900 mil milhões de euros, contabilizando-se unicamente os custos financeiros" (Copeto, 2018).

[6] "Se o incidente estiver aparentemente relacionado com espionagem informática ou houver suspeitas de se tratar de um ataque comanditado por um Estado, ou tiver implicações na segurança nacional, as autoridades nacionais de segurança e de defesa alertarão as suas congéneres, para que estas saibam que estão a ser atacadas e se possam defender. Os mecanismos de alerta precoce serão então ativados e, se necessário, também os procedimentos de gestão de crises ou outros. Um incidente ou ataque informático particularmente grave pode constituir razão suficiente para um EM invocar a cláusula de solidariedade da UE (art.º 222.º do Tratado sobre o Funcionamento da UE (TFUE)" (Comissão Europeia, 2013, p. 21-22).

programas que adulteram e dissimulam dados, danificando as provas recolhidas (Ramalho, 2017).

6 ESTELIONATO ELETRONICO / DIGITAL (BURLA INFORMÁTICA / PHISHING)

De fato, tem-se que a sociedade passa por um desenvolvimento constante ao longo da história. O assunto associado com fraude e estelionato na era digital pode ser somente verificado em uma parcela presente diante de toda criminalidade que acontece na rede mundial de computadores (Sonda, 2019).

Geralmente, nota-se que a atividade criminosa, passível de acontecer nos meios comuns, usa os aparatos tecnológicos de informática para que possam praticar os crimes que estão contidos na norma incriminadora penal, como fraudes e estelionato (art. 171 do Código Penal Brasileiro). Ao passo que os crimes de informática puros ou próprios compreendem típicas figuras que apenas podem ser praticados por meio de um computador, englobando tecnologias novas de informação e dados (Kunrath, 2014).

Tem-se que fenômenos como burla informática, *phishing*, *Haching*, espionagem comercial ou empresarial (roubo de segredos de negócio ou patentes), invasão da vida privada e mesmo o terrível *Ransonware* têm evidenciado a vulnerabilidade das falhas de segurança dos sistemas e redes, acarretando graves problemas relacionados com os fundamentais direitos das pessoas. Pode-se exemplificar essa vulnerabilidade com o que houve no *iCloud* da *Apple* em 2013, quando a *Apple* sofreu um ataque, e assim milhões de usuários de *iPad* e *iPhone* seriam colocados em perigo, com relação ao acesso de seus dados pessoais, como números de cartões de crédito, agendas e contatos (Aguiar, 2017).

Além disso, atualmente, tem-se que o crime de estelionato possui um sério agravante perante a margem digital à proporção que o estelionatário ou fraudador conseguem definir o quanto deseja tirar de uma pessoa, bem como quantas pessoas sofrerão o ataque em extremo anonimato e com apenas um *click*. Seja empregando um *wi-fi* de outro usuário ou rede aberta, ou disfarçando o IP da máquina, assim como utilizando computadores de outros (Sonda, 2019).

Com base no estudo de Sydow (2015), nota-se que essa fraude foi cometida no meio digital com o intuito de ter uma vantagem ilícita, classificada como *scamming*. Esse autor pôde explicar que o *scammer* é caracterizado como um estelionatário virtual, que emprega golpes e armadilhas que são elaborados com o intuito de conseguir informações originadas desses dados, que consequentemente, são transformados em *bits*, ou seja, são unidades matemáticas virtuais.

Verificou-se por Melo (2013) que as condutas que são realizadas pelo *pharming, phishing* e *scam* podem ser classificadas como crimes de furto diante estelionato ou fraude antes da formulação da Lei n. 12.737/2012. Com o aparecimento desta Lei, as

primeiras mudanças começaram a ter certo entendimento. Tendo em conta essa situação, torna-se possível desenvolver uma conscientização do brasileiro sobre o tema de medidas preventivas, pois, deste modo, haverá um decréscimo da incidência relacionada com a fraude eletrônica presente no *Internet Banking*.

Diante deste panorama, tem-se que o tipo legal relacionado ao crime de burla tem ficado mais robusto pelo emprego de meios digitais, configurando-se como um crime dissimulado e complexo presente em muitas práticas de informática. De acordo com o trabalho de Verdelho (2009), observou-se que os crimes que são praticados no meio digital têm acarretado problemas devido ao perfil de imaterialidade (...), tendo em vista que não é evidente a localização física dos agentes.

Com relação ao Brasil, nota-se que o legislador, quando o mesmo não se restringe às maneiras para as quais se comete o crime de estelionato, mas também engloba o cometido com o emprego do computador através da *Internet*, nota-se que existe em sua essência a presença de toda a descrição relacionada com o tipo penal, modernizando-se somente o modo de execução conforme descrito por Pierangeli. De acordo com alguns autores, tem-se que a pessoa que foi enganada precisa também ser considerada como o objeto material, com base no estudo de Nucci (2003) que ao conseguir um lucro ou benefício ilícito em virtude de engano acarretado contra a vítima, tem-se que a vítima acaba por colaborar com o agente sem ter a noção de que está se desfazendo de seus bens.

Então, notou-se que o próprio legislador, na presença de propostas de anteprojetos de reforma do ano de 2011 para o Código Penal Brasileiro, teve a ideia de sugerir uma modalidade específica referente ao estelionato digital; no entanto, suprimiu-se essa redação, com um entendimento transparente de que não teria necessidade de ter um novo tipo penal que fosse específico para esse caso, visto que o mesmo se inseria no caput genérico do art. 171 referente ao diploma legal. Assim, nota-se que o projeto de lei relacionado com a reforma do Código Penal não apresentou inovações sobre este assunto (Almeida, 2013).

Além do mais, tem-se que o Projeto de Lei 89/2003 conseguiu realizar uma adaptação de outras condutas para os tipos penais que existem, realizando a previsão de estelionato eletrônico, que compreende o roubo de senhas com mensagens que possuem *phishing scam*, deterioração, destruição e inutilização de dispositivos e dados de informática como crimes de dano com a presença de inserção, difusão de vírus ou códigos maliciosos, ou seja, a inserção de um código malicioso para em seguida ocorrer o dano, realização de falsificações de dados relacionados com documentos eletrônicos particulares ou públicos, assim como a paralisação de serviços telefônicos, telemáticos,

telegráficos, informáticos de aparelhos de comunicação com o emprego de sistemas informatizados (Matos, 2016).

Desta forma, nota-se que com o emprego da análise jurídica sobre o que existe de concreto em Direito Penal nos dias de hoje, há chances de inseri-lo à nova modalidade relacionada com o estelionato digital que abrange as fraudes realizadas em lojas virtuais fantasmas, e esses agentes terão a possibilidade de receber punição com a presença de elementos virtuais probatórios (Almeida, 2013).

Também pôde ser complementado por Prado (2013) que, com relação ao crime de invasão realizado em dispositivo informático, tem-se que de maneira diferente ao estelionato, o bem jurídico tutelado não compreende o patrimônio da vítima, e sim a liberdade individual, de forma específica, a privacidade sobre informações e dados de perfil profissional ou pessoal que estão presentes no dispositivo informático, e que a segurança desse dispositivo foi de algum modo quebrada sem que houvesse a autorização do titular.

Deve-se ressaltar que caso a conduta seja da forma mais grave quando comparada com a simples invasão que possui o intuito de destruição, adulteração ou obtenção de informações ou dados, ou mesmo, por exemplo, interceptação referente à comunicação telemática, instalação de vulnerabilidades, como extorsão ou estelionato, fraudes em *netbanking* (denominado como furto qualificado), nota-se que o crime de invasão associado com dispositivo informático não poderá ser considerado, visto que o mesmo compreenderá apenas uma maneira para que aquelas condutas pudessem ser realizadas. Então, para que esse criminoso possa ser processado pelo Ministério Público (MP) ou investigado pela Polícia, tem-se que a vítima precisa autorizar, fornecendo a representação. Nota-se que o MP poderá processar o criminoso diretamente apenas quando esse tipo de crime for realizado contra a administração pública indireta ou direta em qualquer esfera dos Poderes do Distrito Federal, União, Estados ou Municípios, ou mesmo praticado contra empresas concessionárias referentes aos serviços públicos (Vellozo, 2015).

Para um panorama internacional diante da evidência da formação da criminalidade informática-digital, nota-se que o Comité de Ministros dos Estados-Membros do Conselho da Europa pôde adotar a Recomendação n.° R (89) no dia 13 de setembro de 1989 com relação aos crimes de informática, em que duas listas sobre incriminações estavam inseridas, tais como: 1) uma lista opcional, que apresentava as condutas em que se apresentavam como facultativas as criminalizações; e 2) uma lista mínima, que compreendia um grupo de condutas que deveriam ter obrigatoriamente uma punição pelo direito interno relacionado com os Estados-Membros. Dentre as previstas condutas contidas nessa lista mínima pode-se destacar a "*computer fraud*",

que possui proximidade com o que se caracterizaria no futuro como burla digital em Portugal (Pedra, 2019).

Então, nota-se que a doutrina de Portugal insere quatro tipos relacionados com as atividades criminosas vinculadas com o *Cibercrime*, tais como: 1) crimes de informática em um estrito sentido, sendo caracterizado como o meio informático ou bem que se configura como o elemento do próprio tipo de crime, em que se englobam os crimes associados com o conteúdo, inserindo-se neste caso os crimes que difundem pornografia infantil (art. 172º, nº3, alínea d) e os crimes que são previstos na lei do *Cibercrime* ; 2) crimes associados com proteção da privacidade ou de dados pessoais (Lei n° 69/98, de 28 de outubro e Lei n° 67/98, de 26 de outubro); e 3) crimes que se aproveitam de meios digitais, como o crime de burla digital nas telecomunicações e burla informática (art. 221ª) (Santos, 2018).

Diante do contexto da referida adequação, tem-se que à similaridade do caminho trilhado por outros países situados na Europa Ocidental, o legislador de Portugal pôde proceder a formação de uma figura jurídico-penal, que teve uma inspiração no tipo legal de burla, visto que o mesmo intencionou identificar as lacunas referentes à punição oriunda da inadequação das figuras criminais relacionadas com conteúdo de patrimônio tradicional para que as condutas de certas condutas fraudulentas pudessem ser punidas, mesmo que, do engano ou erro de qualquer indivíduo, pudessem ser concretizadas as maneiras de manipulação digital que lesam o patrimônio (Pedra, 2019).

Diante deste panorama, tem-se que na seara da experiência alemã não havia menção ao crime de burla informática, sem previsão contida na versão original do Código Penal (1982), visto que esse tipo de crime foi inserido no sistema jurídico-penal de Portugal somente no ano de 1995, ao ser realizada uma revisão pelo Decreto-Lei n.° 48/95, de 15 de março (Pedra, 2019).

Diante deste contexto, tem-se que Garcia e Rio puderam verificar a presença de duas figuras relacionadas ao delito, tais como: burla nas telecomunicações e burla informática (Garcia & Rio, 2015). Perante este movimento, nota-se que o tipo relacionado com a burla informática surgiu ao ser realizada a revisão do Código Penal do ano de 1995, bem como por apresentar uma influência do direito alemão com o entendimento de “burla de computadores”, e posteriormente, ao realizar a Reforma de 1998, juntamente com o n.º 2 do artigo 221.° do Código Penal, em que pôde ser classificada como um tipo de “burla nas telecomunicações”, surgindo o conceito jurídico-penal que está vigente atualmente (Dias, 1999).

Desta forma, pela revisão do ano de 1995, esse crime pôde ser inserido como crime de “burla Informática”, e pode-se interpretá-lo como a produção de consciente

engano formado através da manipulação de um sistema de informática, mas não por atingir diretamente uma pessoa, como o denominado crime de burla presente no Código de Processo Civil (CPC), mesmo que seja possível fazer uma previsão de finais idênticos e objetivos materiais (Acórdão do Tribunal da Relação de Évora, 2012).

Nos dias atuais, nota-se que o art. 221º. Do Código Penal consegue prever dois tipos de crimes, burla nas comunicações e burla informática, que se opõem ao que foi inserido no Código Penal de 1988. Pelo motivo simples de que o bem jurídico que está protegido não se restringe somente ao patrimônio, mas também à integridade patrimonial, nos quais os programas informáticos estão inseridos, os dados na sua segurança e fiabilidade e o respectivo processamento. Com relação à burla informática, nota-se que a mesma engloba os casos em que os seguintes pressupostos estão presentes no agente: utilização de dados sem intervenção ou autorização por outro modo que não seja autorizado no processamento; utilização incompleta ou incorreta de dados; causar prejuízo patrimonial para outra pessoa; fazer uma interferência mediante incorreta estruturação de programa informático ou no resultado relacionado com o tratamento de dados; e intenção de ter para terceiros ou para si o enriquecimento ilícito. Segundo o tipo legal de burla relacionado com as comunicações, nota-se que essa burla engloba os casos em que os seguintes pressupostos estão presentes no agente, tais como: causar prejuízo patrimonial para outra pessoa; ter a intenção de obter para terceiros ou para si um benefício ilegítimo; e utilizar dispositivos eletrônicos, programas ou outros meios que, em conjunto ou separadamente, que se destinam a alterar, diminuir ou impedir, parcialmente ou totalmente, a exploração ou funcionamento normal de serviços de telecomunicações (Filipe, 2018).

Deve-se ressaltar que a burla informática, que está prevista no n.° 1 do art. 221.° do Código Penal, representa um crime do tipo semipúblico. Consequentemente, tem-se que o procedimento criminal é dependente da queixa por outra pessoa para quem esse direito seja conferido ou por parte da vítima, presentes nos artigos conjugados 113.° e 116.° do Código Penal, bem como o art. 49.º do CPP. Com relação ao n.° 3 do art. 221.° do Código Penal, pode-se consagrar a punição do crime de burla informática na maneira tentada, ao passo que o n.º5 deste mesmo preceito consegue realizar a previsão de burla informática qualificada, que possui uma natureza pública, ou seja, para esse tipo de burla, o MP consegue promover um procedimento criminal, de acordo com o que está disposto no art. 48.° do CPP (Alves, 2019).

Segundo os termos conjugados relacionados com o art. 13.° e do art. 221.° do Código Penal, tem-se que a burla informática pode ser caracterizada como um crime doloso, sem que seja possível admitir a título de negligência este tipo de punição.

Ademais, esse tipo de crime é intencional, visto que há uma específica intenção de obter enriquecimento ilegítimo (Alves, 2019).

Convergindo com esse referido, pôde ser evidenciado pelo Tribunal da Relação do Porto, em acórdão, do dia 03 de fevereiro de 2016, com o processo n.º 482/10.2SJPRT.P1, que se encontra disponibilizado no *site* www.dgsi.pt, que a burla informática consiste em um consciente erro que é realizado pela manipulação de tratamento informático ou sistema de dados. Não há uma exigência para qualquer artifício ou engano pelo agente, mas certamente a utilização e introdução abusiva de dados voltados para o sistema informático (Alves, 2019).

É evidente que, com relação ao tipo legal de burla nas comunicações e burla informática, é possível ter a vinculação com outros crimes ilícitos, por exemplo, com crimes de interceção ilegítima, falsidade informática, sabotagem informática, danos relacionados aos programas ou dados informáticos, ilegítimo acesso, e também ilegítima reprodução de programa protegido, deste modo acarretando um real concurso de infrações. Torna-se evidente e compreensível que o crime de burla nas comunicações e burla informática podem ser entendidos em seu âmago como um crime de “não perigo e de lesão”, porque o mesmo possui um caráter público, semipúblico ou particular (Garcia & Rio, 2015).

Desta forma, pode-se dizer com base no estudo de Manuel Lopes Rocha (1996) que a introdução legal relacionada com o crime de burla informática presente no ordenamento jurídico de Portugal residiu na confirmação das realidades abaixo:

a) Ações frequentes em que utilizações abusivas relacionadas com caixas automáticas foram verificadas;
b) Presença de condutas, que, normalmente, englobam consideráveis riscos para o sistema ou tráfico de provas ou para o comércio jurídico;
c) Detecção difícil desse tipo de conduta, que deveria ter uma repulsa cada vez mais forte da sociedade;
d) Insuficiência vinculada com os tipos tradicionais penais (enriquecimento de patrimônio) para que haja a proteção do bem jurídico.

6.1 EMAIL

Por causa da complexidade relacionada com os processos de fraude de captura de dados, tem-se que qualquer tipo de *phishing* pode ser caracterizado com um tipo de crime de burla (art. 217º do Código Penal), quando ocorre prejuízo patrimonial com esse crime, visto que a chamada de voz, SMS, ou mesmo e-mail de uma pessoa pode fazer com que essa pessoa forneça os seus dados, compreendendo assim um tipo de engano ou erro (Reis, 2019).

Com relação ao estelionato praticado em um meio digital, nota-se que para o criminoso manter ou induzir a vítima em erro, o mesmo precisa conquistar a confiança dessa vítima, ou seja, torna-se corriqueiro que o criminoso envia e-mails para as possíveis vítimas, para persuadi-las a fazer depósitos em dinheiro, agregando-se a promessa de que as mesmas receberão depois de um tempo vantagens financeiras, normalmente valores altos em dinheiro (Vianna & Machado, 2013). Pode-se citar um exemplo neste caso como a participação em correntes da sorte, com a falsa ilusão de que a pessoa receberá muito dinheiro (Maia, 2017).

Diante deste contexto e referente ao papel de enunciatário, tem-se que o leitor do e-mail precisa fazer a seleção de abrir ou não estes tipos de mensagens. Caso opte por abri-las, deve escolher se baixa algum anexo que acompanha o e-mail ou clica em algum *link*. Nesse instante, corre-se o risco de ter o seu e-mail contaminado por e-mails fraudulentos. Em muitos casos, o internauta é envolvido pela sensibilização presente em seu *pathos*, e acaba clicando em arquivos e *links* falsos de maneira compulsiva, acarretando dano ao usuário e ao computador, visto que o usuário pode terminar sendo uma vítima de estelionato virtual (Silva, 2014).

Pode-se destacar também como exemplo, o tipo de crime de estelionato que é praticado com a ajuda de páginas falsas na *Internet* que se camuflam como um *site* real de uma instituição bancária, fazendo com que as vítimas acessem esse *site* falso por engano, e assim forneçam aos criminosos suas credenciais de acesso, e desta forma, os criminosos conseguem ter esse acesso para ter alguma vantagem ilícita, ocasionando um prejuízo econômico para a vítima (Maia, 2017).

No caso de Portugal, nota-se que a criação de páginas (como exemplo *homebanking*), pode ser caracterizada como um crime de falsidade informática (art. 3º da Lei Complementar (LC)), bem como um crime de burla (se for consumado). De fato, tem-se que esse tipo de crime possui uma conduta objetiva e típica de conseguir apagar, introduzir, suprimir ou modificar os dados informáticos, ou de qualquer forma, interferir no tratamento informático referente aos dados, acarretando produção de documentos ou dados não genuínos. Essa ação possui ainda a intenção de ocasionar engano vinculado às relações jurídicas, tendo em conta que esses documentos ou dados falsos foram utilizados ou considerados para finalidades juridicamente importantes como se fossem verdadeiros, caracterizando-se como um subjetivo elemento do dolo. Mesmo que os SMS, e-mails ou chamadas telefônicas não puderem mais ser caracterizados como um crime de falsidade (Reis, 2019).

Perante esse contexto, nota-se com detalhes que o estudo de Correia e Jesus (2016) pôde destacar a conveniência em se concretizar o crime de burla informática, destacando a ineficácia do crime de burla, conforme descrito no art. 217.º do Código

Penal, voltado para as manipulações dos dados e sistemas informáticos, tais como: Com destaque para o caso em que os criminosos enviam um e-mail para solicitar informações bancárias do titular da conta, para posteriormente terem acesso à essa conta pela *Internet*, e assim poderem transferir uma quantia em dinheiro sem a autorização do titular, nota-se que esse típico elemento que está presente na prática, pela vítima, relacionada às atitudes que acarretam prejuízo patrimonial ainda não está preenchido. Realmente, pode-se caracterizar esse e-mail que é enviado como se fosse um banco oficial como um fato provocado maliciosamente. Ademais, por esse e-mail, tem-se que o titular da conta é levado ao erro. Todavia, tem-se que a transferência bancária realizada pelo criminoso é que acarreta prejuízo patrimonial, não a transferência do código de acesso pelo titular. Assim, não pode ser caracterizado como completo, o crime de burla. Pode-se também afirmar que os computadores não estão vulneráveis ao engano ou erro, visto que essa característica compreende uma atitude humana.

Mesmo assim, de acordo com o estudo de Velozzo (2015), tem-se que parece (ao menos inicialmente) que não existe uma exigência sobre a intervenção da vítima para se concretizar o crime, sendo que o agente através do uso de meios que possam afetar a exploração referente aos serviços de comunicação (burla nas comunicações) ou o funcionamento normal, poderá intervir e/ou agir de forma direta sobre o patrimônio da vítima (informações, programas e dados) com a presença de um *animus delicte* com o intuito de ocasionar um prejuízo patrimonial.

Perante essa situação, pode-se citar a notícia recente sobre fraude por meio de mensagens de SMS que foram enviadas para algumas pessoas do Hospital Pedro Hispano e todos os Centros de Saúde de Matosinhos com o intuito de cobrar taxas moderadoras (Observador, 2016).

Assim, nota-se que as novas tecnologias de comunicação que estão sendo disponibilizadas atualmente pela *Internet*, como exemplo as redes sociais, facilitam e agravam muito a ação dos criminosos, e infelizmente atrapalham a ação da polícia (Ribeiro, 2019).

Por fim, pela *Internet*, para que um crime possa ser caracterizado como crime de estelionato, deverá ser considerada a conduta, em que o agente procura como ponto principal manter ou induzir a vítima em erro, e ao empregar esse comportamento, adquirir ilícita vantagem para outros ou para si mesmo (Ribeiro, 2018).

6.2 CARTÃO DE CRÉDITO

Com relação às ações que farão parte do delito, tem-se que a integração relacionada com o universo cibernético terá máxima importância na criminalidade

patrimonial, no qual está inserido o furto por carteirista. Com base no entrevistado, nota-se que o delito continuará apresentando ocorrência no plano físico, visto que as pontes que conectam esse tipo de crime ao universo digital serão fortalecidas. Referente ao furto de carteirista, torna-se corriqueira a associação entre o crime de burla de cartão de crédito e o furto por carteiristas, tendo em conta que na burla de cartão, os criminosos se apoderam das quantias presentes na conta; ao passo que o furto de carteirista, os criminosos se apoderam dos conteúdos que foram furtados, e os utilizam (Bicho, 2020).

Paralelamente à elevada organização e mobilidade, surge uma insatisfação sobre a relação do furto por carteirista com outros tipos de crimes, tais como a falsificação de documentos e a burla. Com a proeminência do mundo da *Internet* e a intensificação dos dispositivos digitais, nota-se que tem ocorrido uma escassez do dinheiro físico pela maioria das pessoas, que passaram a usar dispositivos eletrônicos e cartões que possibilitam, igualmente, a realização dos pagamentos e transações (Bicho, 2020).

De acordo com o Tribunal da Relação do Porto, relacionado ao processo n.° 347/10.8PJPRT.P1, de 21 de fevereiro de 2018, tem-se que esse processo aborda a questão de uma rede organizada de carteiristas que tem cometido crimes em Portugal, inclusive em muitas cidades, bem como pela Europa. Todavia, os criminosos acabaram sofrendo uma condenação pelos crimes de roubo, burla, associação criminosa, furto qualificado, burla informática qualificada e burla informática. De fato, efetuavam-se as burlas com os cartões multibanco que estavam presentes nas carteiras que haviam sido roubadas (Acórdão do Tribunal da Relação do Porto, 2018).

6.3 DISTINÇÃO ENTRE ESTELIONATO ELETRÔNICO E FURTO ELETRÔNICO

Nota-se que os dois delitos, ou seja, estelionato realizado por meio eletrônico ou furto diante fraude possuem algumas similaridades, fazendo com que existissem dúvidas referentes ao típico enquadramento desses atos, então, torna-se primordial que uma análise detalhada fosse realizada pelos tribunais sobre a conduta realizada pelo criminoso (Matos, 2016).

Perante um contexto primário relacionado com a insegurança jurídica para que fosse aplicada uma legislação correta nos casos de fraude no comércio eletrônico, *phishing*, bem como fraude em *Internet banking*, tem-se que foram divididas a jurisprudência e a doutrina em duas vertentes, tais como: a jurisprudência defendia a aplicação por fraude do furto qualificado (artigo 155, §4°, inciso II, do Código Penal); e a doutrina defendia ter a aplicação do estelionato (artigo 171 do Código Penal) (Coimbra, 2020).

Tanto no estelionato quanto no fruto diante fraude, tem-se que o criminoso consegue obter de maneira fraudulenta uma ilícita vantagem patrimonial. E por este motivo, ocorre muita polêmica sobre o assunto da classificação jurídica relacionada com os golpes patrimoniais que são realizados com cartões de banco clonados. Normalmente, os golpistas conseguem realizar a clonagem dos cartões de débito ou crédito através dos “chupa-cabras”, assim como diante ligações telefônicas maliciosas (clonagem telemática ou virtual) ou pela *Internet*. Ao ser realizada a clonagem do cartão, tem-se que esses cartões serão empregados para transferências de valores entre contas, compras, pagamentos de contas e compras em geral (Farah, 2017).

De fato, observa-se que os golpistas conseguem burlar tanto as lojas ou empresas quanto as instituições bancárias realizando compras ilícitas, e acarretando prejuízos que podem ser refletidos no próprio dono do cartão ou em seus patrimônios. Pode-se exemplificar a situação de quando o golpista utiliza o cartão de crédito clonado para retirar dinheiro da poupança ou conta corrente de algum cliente, verifica-se que a máquina eletrônica ou funcionário do banco realiza a entrega do dinheiro para o golpista, observando-se que a própria instituição está sendo induzida ao erro. Deste modo, nota-se que a transferência do dinheiro acaba ocorrendo livremente para o golpista, visto que não se observa o amortecimento da vigilância bancária referente ao dinheiro. O operador do direito ou intérprete deve raciocinar de acordo com a existente realidade, em que há uma substituição por máquinas pela pessoa física. De fato, tem-se que o fruto da modernidade consiste na automatização, que direciona o jurista moderno a realizar uma revisão associada aos entendimentos, com a presença de interpretações fundamentadas no mundo real, mas não são com base em um mundo ideal (Farah, 2017).

Diante deste panorama, conforme destacado pelo estudo de Farah (2017), o mesmo destacou que a fraude é considerada como uma característica corriqueira das duas tipificadas condutas. De fato, como uma característica que afronta a moral, interesse social, visto que a mesma é alvo do legislador penalista, anteriormente à existência de caixas eletrônicos e cartões de crédito eletrônicos e magnéticos. A jurisprudência e a doutrina da época demonstraram não ter problemas em ter um claro discernimento entre as duas condutas criminais perante os fatídicos casos existentes até o momento. Todavia, são feitas hoje duas perguntas: com o aparecimento de caixas eletrônicos e cartões eletrônicos e magnéticos pelos bancos, será que esses tipos de condutas, escritas e tipificadas em um Código Penal da década de 1940, conseguiriam se adequar perfeitamente perante reprováveis condutas (criminosas) com o emprego de tecnologias modernas (caixas eletrônicos e cartões)? Será que a tipificação

adequada relacionada com essas condutas perante as modernas situações seriam classificadas como tão incontroversas?

Para as duas condutas contidas no Código Penal (Furto mediante fraude: multa e pena de reclusão de dois a oito anos; Estelionato: multa e pena de reclusão de um a cinco anos), verificou-se que existe uma diversidade relacionada com as penas, e por essa diferença, justifica-se a relevância do debate. Entretanto, não se deve esquecer que a interpretação com base no assunto repressivo-penal precisa ser sempre com restrições, e apenas diante deste sentido negativo pode-se admitir o judicial arbítrio, sem que a taxatividade vinculada com o princípio da reserva legal seja violada (Farah, 2017).

Mesmo assim, nota-se que a solução voltada para os crimes virtuais (furto diante fraude e estelionato) não possui maior punição pelo Estado no setor do direito penal. Tem-se que existe uma previsão pelo direito civil de que a responsabilidade será de acordo com o tamanho do dano; no entanto, poderá ser analisado pelo julgador maior dano referente à conduta do criminoso na seara cível e da vulnerabilidade da vítima (Barros, 2015).

Ademais, dirigem-se as condutas de fraude contra aparelhos e máquinas que não são caracterizados como estelionato, visto que, deve-se enfatizar que a vítima precisa ser uma pessoa. Diante deste contexto, não existe estelionato, mas sim furto por causa da clonagem do cartão para que um indevido saque seja efetuado diante um terminal eletrônico presente em uma instituição financeira (Farah, 2017).

Portanto, tem-se que esse tipo de crime não se caracteriza como estelionato, tendo em conta que nenhuma pessoa foi induzida ao erro, e esse ato consiste em uma prerrogativa do tipo penal que está contido no art. 171 do Código Penal, tais como: obter uma ilícita vantagem, para outro ou para si mesmo, mantendo ou induzindo uma pessoa em erro, diante ardil, artifício ou outro meio fraudulento (Barbosa & Rocha, 2016).

Diante deste panorama, existe também uma compreensão sobre o tema no Tribunal Regional Federal (TRF) da 4º Região:

> PROCESSO PENAL. COMPETÊNCIA. TRANSFERÊNCIA FRAUDULENTA PRATICADA PELA INTERNET. SUBTRAÇÃO DE VALORES DEPOSITADOS EM BANCO. FURTO MEDIANTE FRAUDE. COMPETÊNCIA. LOCAL DA SUBTRAÇÃO. 1. Em que pese a existência de recentes julgados desta Corte entendendo tratar-se de estelionato (com a divergência deste Relator) firmou-se a jurisprudência do Superior Tribunal de Justiça no sentido de que a hipótese de subtração, por meio eletrônico, de valores depositados em instituição bancária configura o crime de furto mediante fraude. 2. Modificada a orientação da 4ª Seção para, com base nos precedentes citados, declarar competente a Subseção Judiciária onde está situada a agência que mantém a conta corrente da qual os valores foram subtraídos (Recurso em Sentido Estrito 608/RS, 2007).

Ainda presente em uma jurisprudência mais recente, tem-se que foi afirmado por Maia (2017) que o STJ pelo agravo regimental contido no Código Civil (CC) 74.255-SP compreende que a realização de um saque fraudulento feito em uma conta corrente, por exemplo, da Caixa Econômica Federal não se caracteriza como um estelionato, mas sim furto diante fraude. Para o estelionato, tem-se que o criminoso intenciona deixar a vítima em erro para que a mesma possa entregar seus bens espontaneamente; ao passo que na fraude de furto, existiria uma redução relacionada com a vigilância da vítima para que a mesma não perceba que o seu patrimônio está sendo subtraído.

Desta forma, conforme destacado no estudo de Costa (1995), nota-se que o estelionato na informática é classificado como meio fraudulento, um ardil, um artifício que é empregado pelo criminoso para que o mesmo possa ter o patrimônio de outra pessoa.

Assim, para que o crime mencionado anteriormente possa ser caracterizado, retirou-se a decisão do TRF da 3ª Região:

> PENAL. RECURSO EM SENTIDO ESTRITO. **ESTELIONATO. SAQUES INDEVIDOS DE CONTA CORRENTE VIA INTERNET BANKING. PREJUÍZO PATRIMONIAL À CAIXA ECONÔMICA FEDERAL**. ART. 171, § 3º, DO CP. COMPETÊNCIA DA JUSTIÇA FEDERAL. ART. 109, IV, DA CF. PROVIMENTO.
> 1. **Os fatos apurados consistem na retirada indevida de valores de correntista da Caixa Econômica Federal, por meio de movimentação financeira fraudulenta através do sistema de internet banking**.
> [...]
> 3. Cabe recordar que, **na hipótese de estelionato**, é pacífica a doutrina ao enunciar que **figuram no pólo passivo do delito tanto aquele que foi ludibriado quanto aquele que sofreu o prejuízo econômico, podendo ser pessoas distintas**.
> 4. **No caso sob análise, desde o desfecho da execução do crime, o artifício fraudulento ludibriou os mecanismos de vigilância e guarda de responsabilidade da CEF, provocando-lhe posterior lesão patrimonial, além de dano subjacente à credibilidade da instituição bancária**. [...] (Recurso em Sentido Estrito 7720/SP, 2011, grifos nosso).

Além disso, de acordo com o trabalho de Damasceno (2007), o mesmo destacou: “compreende-se que o estelionato se caracteriza como um tipo penal (art. 171 do Código Penal) e que a infração se concretiza quando existe a obtenção de uma indevida vantagem pelo criminoso [...]”. Também pôde ser acrescentado que o local do crime se caracterizaria como o local onde os agentes puderam receber a indevida vantagem, com a possibilidade de divisão entre local mediato e local imediato.

Desta forma, compreende-se que há um ideal entendimento jurisprudencial e doutrinário que seja anterior à Lei 12.737/2012, e nota-se que existe a aplicação da fraude vinculada ao *Internet Banking*, ou seja, presença de um furto qualificado diante estelionato e fraude, tornando-se essencial um atual conhecimento sobre esse tema (Melo, 2013).

De acordo com a caracterização do crime referente ao estelionato eletrônico, tem-se que o mesmo ocorre pela produção de provas, visto que ao ser considerado um crime que é praticado em ambiente virtual, bem como empregarem-se ferramentas que estão disponíveis, verifica-se que fica mais fácil para o criminoso conseguir se desfazer das provas, isto é, o criminoso pode se desfazer das mensagens, correios eletrônicos, *sites*, dentre outras formas, fazendo com que a ocultação do crime seja beneficiada, assim como favorecendo a falta de comprovação de que realmente aconteceu o crime (Ribeiro, 2018).

Perante este contexto, torna-se claro que a dificuldade em poder impedir ações de estelionato eletrônico reside na carência de equipes que sejam treinadas frequentemente e capacitadas para investigação, mas não na "falta de específica legislação", isto é, torna-se primordial que exista uma capacitação profissional, que seja indispensável para haver uma formação da justa causa voltada para a ação penal (Cerqueira & Rocha, 2013).

Diante deste entendimento, tem-se que, em Portugal, no setor de investigação associado com subsumíveis condutas voltadas para a prática de crime de burla nas comunicações e burla informática, essa investigação assume um relevo particular para conseguir obter a prova digital (Pedra, 2019).

Conforme destacado por Santos (2005), verificou-se que as técnicas de produção e recolhimento de provas digitais não se concretizam do mesmo modo em que são obtidas as provas empregando-se as técnicas dos métodos tradicionais. A quantidade significativa de informação digital, que tem a possibilidade de ser eliminada, modificada ou criada, em instantes, bem como em qualquer lugar do mundo, faz com que exista uma imposição da investigação, para que a mesma se especialize e se equipe com específicas ferramentas que assegurem a integridade relacionada com a prova digital. De fato, nota-se que a faceta mais frágil da justiça é revelada, evidenciando-se claramente as vulnerabilidades da investigação, e sendo constatada com base nos números que são apresentados em Portugal sobre a segurança interna pelo relatório anula mais recente, mostrando que apenas 801 processos de inquérito para o ano de 2016 foram levantados com relação aos crimes informáticos, em que somente 402 deles foram caracterizados como arguidos, visto que a maior parte dos crimes recaiu sobre crimes nas comunicações e crimes de burla informática (Aguiar, 2017).

Além disso, deve-se destacar que há crimes que se encaixam no âmbito de reservada competência referente à investigação criminal da Polícia Judiciária (PJ), em que se confere tipo legal associado aos crimes de burla nas comunicações e burla informática, bem como ao tipo legal relacionado com a burla qualificada; todavia, pode

ser delegada a investigação pelo MP em outro Órgão de Polícia Criminal (OPC) (Filipe, 2018).

Inclusive, cita-se o seguinte julgado:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE **FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO**. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE. (...) 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. (...) No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal. 5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão - SJ/PR (Conflito de Competência 67343/GO, 2007, grifos nosso).

Referente a outro concreto caso, pode-se destacar o julgado que foi analisado por Coimbra (2020) sobre a fraude em *Internet Banking*, em que o criminoso conseguiu realizar a subtração no sistema da Caixa Econômica Federal da conta corrente da vítima de R$2.525,15 (dois mil quinhentos e vinte e cinco reais e quinze centavos), visto que a vítima tinha uma conta corrente na agência de Campo Mourão, no estado do Paraná. Sobre este assunto, tem-se que:

> [...a] a Turma firmou o entendimento que tal crime informático se **trata de furto mediante fraude, não de estelionato, sob o fundamento de não ter a vítima consentido, tampouco ter participado de alguma sorte na empreitada criminosa**. Destaca, para esse fim, a relatora que não houve qualquer vício de consentimento pela parte da vítima, tendo a fraude se resumido na quebra da vigilância eletrônica do sistema de informação de dados do banco, não havendo que se falar em estelionato (Coimbra, 2020, p. 29, grifos nosso).

Pode-se citar um interessante caso que aconteceu em Portugal em que houve a condenação por falsidade informática e burla tributária, como maneiras diferenciadas do crime praticado. Relaciona-se o fato com o Acórdão do Tribunal da Relação de Évora em que o mesmo foi proferido no processo n.º 370/06.7TACBR.C1 de 26-01-2011, e explicado da seguinte forma:

> Estamos, neste caso, perante uma condenação pela prática, em autoria material e na forma consumada, de um crime continuado de burla tributária (o qual consome o crime de falsidade informática, na forma continuada). Veio o MP interpor recurso solicitando, também, a condenação pelo crime de falsidade informática, em concurso efectivo e real sendo emitido parecer por parte do Exmo. Procurador-Geral Adjunto defendendo que deverá ser considerado o concurso real e não aparente entre os crimes de burla tributária e de falsidade informática, com as respectivas condenações e efectivação do competente cúmulo jurídico, julgando procedente o recurso e revogando o Acórdão recorrido (Acórdão do Tribunal da Relação de Coimbra, 2011).

Neste caso, verificou-se que a funcionária conseguiu alterar dados contidos no programa informático para que a mesma pudesse obter uma prestação patrimonial. De fato, pôde-se entender com essa ação que a inserção de dados falsos, bem como a modificação realizada no programa informático nacional referente ao rendimento social que havia sido inserido pela funcionária, foi classificado como um ato fraudulento utilizado por ela para fazer com que a administração da segurança social pudesse realizar indevidas atribuições patrimoniais, proporcionando com o pagamento e processamento dessas atribuições para que houvesse o enriquecimento dos beneficiários. Exemplificando-se de outra forma, com a falsificação de dados informáticos, bem como alteração e introdução de dados falsos direcionados para o programa informático, pode-se concretizar então, contra a funcionária o crime de burla tributária (Ferreira, 2018).

Ao realizar a defesa da decisão, tem-se que a falsificação foi a maneira idônea de conseguir realizar a burla, tendo somente um aparente concurso de normas, e por este motivo não foi possível ter a condenação por dois crimes por causa do impedimento em ter dupla valoração, tendo em conta que o Tribunal da Relação informa que apesar disso, atribuindo peso para as duas gravidades em questão (molduras penais), verificou-se que o crime-meio é um pouco superior, isto é, de maneira alguma o mesmo não pode ser considerado como desprezível, desta forma reclamando a sua autonomização e por conseguinte condenar a funcionária pelos dois crimes realizados, ao ser efetuado o cúmulo jurídico respectivo (Ferreira, 2018).

De um modo geral, tem-se que a punição relacionada ao crime de falsidade compreende uma pena de prisão de um a cinco anos; porém, a mesma pode se apresentar com mais severidades quando comparada com a pena aplicável ao crime associado à burla tributária, que compreende uma multa de até 600 dias ou prisão de cinco anos, de acordo com o n.º 4 do artigo 87.º do RGIT sobre viciação ou falsificação de documento relevante fiscalmente, falsas declarações ou o emprego de outros meios fraudulentos conforme previsto no nº1 que não são autonomamente previstos, exceto caso a pena mais grave possa ser aplicada, verifica-se que o Acórdão do TER que fez a opção pela resolução mais apropriada da situação (Ferreira, 2018).

Mesmo assim, conforme destacado pelo estudo de Geraldes (2013), há um aparente concurso entre outros crimes e burla informática com a sabotagem de informática e ilegítimo acesso, visto que todos possuem uma finalidade ter um ilegítimo enriquecimento, tendo como base que esses últimos servem somente de simples atos de execução, bem como com relação ao princípio *ne bis in idem*, com o qual nenhuma pessoa pode ser punida duplamente pelo mesmo ato ilícito (art. 29.°, n.º 5 da Constituição da República Portuguesa).

6.4 FRAUDES PRATICADAS NO ECOMMERCE

De fato, nota-se que há outras formas de estelionato virtual que residem em falsas páginas de comércio eletrônico, em que o pagamento vinculado aos produtos oferecidos é realizado pela vítima, e a mesma não recebe o bem que havia comprado. Diante desta situação, tem-se que as vítimas acabam sendo atraídas para páginas falsas devido ao valor de baixo custo dos produtos que são vendidos em comparação às lojas mais conhecidas (Wendt, 2010).

Deve-se destacar também comuns aspectos referentes ao delito de estelionato virtual presente em *sites* do comércio eletrônico que fornecem preço baixo para as mercadorias, assim como a maneira estabelecida para realizar o pagamento vinculado aos produtos comprados, visto que normalmente realiza-se o pagamento à vista por depósitos ou boleto bancário (Matos, 2016).

Desta forma, com base no estudo Nogueira (2009), pode-se destacar como se aplica o crime de estelionato eletrônico no *E-commerce*, tais como, uma pessoa ativa faz a criação de um *site* relacionado com o comércio eletrônico para que ocorra a venda de produtos informáticos, disponibilizando produtos que possuem um preço com menor valor, e com a promessa de uma entrega em 15 dias úteis, mas apenas com a realização do pagamento em depósito que precisa ser feito em uma conta corrente. Ao longo desse período, pode ser feita a contabilização do lucro, sem que alguma coisa seja entregue, de maneira que, mesmo depois de um tempo, esse criminoso faz a remoção do *site* do ar, fazendo muitas vítimas em prejuízo. De fato, tem-se que existe outra hipótese em pode ser caracterizado o crime de estelionato está relacionado com a venda de bens associados com *sites* hospedeiros, assim como por exemplo, um par de tênis, em que um produto é oferecido por um suposto vendedor, e o mesmo pode ser adquirido através de um lance, e quando a vítima é declarada vencedora, exige-se um pagamento em conta corrente pelo agente para que a entrega do bem possa ser realizada (Ribeiro, 2018).

De fato, pode haver uma precaução para que mais fraudes sejam evitadas e desta forma informar o consumidor sobre esses *sites*, com o intuito de que o consumidor se torne mais uma vítima de estelionato, tem-se que o legislador do Brasil pôde estabelecer o art. 6° do Decreto n. 7.962 (2013): “tem-se que as contratações relacionadas com o comércio eletrônico terão de seguir o cumprimento associado com as condições de oferta, apresentando a entrega dos serviços e produtos contratados, observando-se quantidade, prazos, adequação e qualidade”.

Torna-se evidente que ao pesar uma crítica, no instante da promulgação desse decreto, referente aos veículos de comunicação sobre a abordagem excessiva sobre o

comércio eletrônico, pode-se destacar uma extrema relevância tanto para a legislação brasileira quanto para o consumidor, visto que, assim, tornou-se positiva pela intenção de confrontar uma prática relacionada com o comércio virtual com a presença de deveres e direitos que precisa ter um comércio físico, conforme houve o entendimento de confrontar o crime de estelionato relacionado com as fraudes que também ocorrem no mundo do comércio virtual (Almeida, 2013).

Como exemplo real, pode-se destacar a Operação Ostentação que tinha sido feita no dia 10 de outubro de 2018 pela Polícia Civil de São Paulo (Departamento Estadual de Investigações Criminais (DEIC)) com o auxílio do Núcleo de Investigações de Crimes Cibernéticos (Cyber Gaeco), com a presença da força tarefa do MP conseguiu realizar uma prisão de um estelionatário com apenas 24 anos que estava sendo investigado por volta de 18 meses, com uma fortuna no valor aproximado de 400 milhões de reais. Então, tem-se que os promotores do caso vinham investigando esse caso para que os suspeitos associados com organização criminosa no ambiente virtual pudessem ser identificados. Esse suspeito conseguia desviar uma quantidade da conta dos clientes de bancos diferentes através de *phishing*, e o mesmo empregava avançadas técnicas que dificultava o rastreamento (Costa, 2018).

Deve-se ressaltar que ainda há um rastro que distancia as peculiaridades entre um ilícito contratual e um delito, tornando-se provável desenvolver impasses relevantes no emprego de norma jurídica, especialmente no que se refere às demandas sobre a aplicação do direito penal relacionado ao delito que é praticado sobre o consumo na *Internet*. Desta forma, contextos que podem ser classificados como delito de estelionato são classificados como descumprimento simples contratual, devido ao fato de não existir uma especificação para estelionato e fraude cometidos no comércio *online* (Sonda, 2019).

De fato, tem-se que essa prática representa apenas uma parcela desta perspectiva, e a mesma merece uma atenção especial, visto que o *E-commerce* está se caracterizando como uma ferramenta mais empregada pelos usuários nos dias atuais, e essa ferramenta está sendo inserida cada vez mais nas negociações (Sonda, 2019). Perante o que foi descrito, tem-se que o estudo de Rosa (2007) mostrou que estelionato é sempre caracterizado como estelionato, que é praticado com a presença de um computador ou mesmo sem ele.

Logo, nota-se que o crime de estelionato está sendo cada vez mais complicado para elucidar, especialmente com as práticas que têm sido praticadas no ambiente virtual, e assim, torna-se difícil para a vítima conseguir identificar quem praticou o delito sem que exista uma investigação criminal mais detalhada, pela polícia civil, com o emprego de técnicas mais apuradas para a indicação e desvelamento do autor, que

frequentemente fica encoberto com maneiras sutis relacionadas com fraudes que conseguem iludir até os indivíduos mais cuidadosos que caem em golpes acarretando danos patrimoniais para os mesmos (Pereira, 2020).

7 CONCLUSÃO

Esta tese esclareceu e apresentou objetivamente o problema do estelionato no Brasil e Burla em Portugal. Também permitiu um melhor entendimento da contravenção à luz dos modernos instrumentos tecnológicos, que possuem maior alcance e potencial de dano à propriedade.

O engano e a malandragem, a mentira e o engano são todos aspectos da humanidade que, dependendo de sua cultura e tradições, vêm aumentando a capacidade de trapaças das pessoas e, portanto, dando vantagem à vítima. Quanto mais um homem se comunica, quanto mais ele domina a arte de usar tramas astutas em seu proveito, melhor ele consegue algo em seu próprio benefício.

Nesse contexto, tanto no Brasil como em Portugal, a modalidade de crime patrimonial ganhou novo fôlego com a era digital, e foi possível através do presente estudo descrever como este crime é observado nos dois países, sendo crimes similares e com designações distintas, pois no Brasil sua origem advém do latim *stellionatu* ou *stellio natus*, sendo *stellio* o camaleão que muda de cores para ludibriar a sua presa. Em Portugal a influência foi castelhana, pois o termo burla é uma evolução do latim *burrula* ou *burrae*.

Embora exista um fio condutor entre o direito romano-germânico e o legado português, o direito brasileiro evoluiu ao longo do tempo sob diferentes correntes. Essas diferenças podem ser descritas como uma gama de nomenclaturas, formalidades, por meio da organização judicial e rituais processuais.

Inclusive, em Portugal este tipo de crime patrimonial ganhou uma sintética e normativa linguagem, alusivo típico do alemão. Fica para trás a descritiva linguagem que tornava facultativo discussões se os descritos meios faziam complemento a um taxativo elemento da forma de cometimento do tipo legal do crime de burla. O atual texto do artigo, é resultante da operada revisão ocorrida pelo advento do Decreto lei n.º 48/95, o qual tem correspondência ao artigo 313.º da originária versão do CP, inclusive porque houve introdução deste ordenamento jurídico com a reforma ocorrida em 1995 (Decreto-lei n.º 48/95) bem como através das alterações advindas da Lei n.º 59/2007.

As variações linguísticas são, portanto, as mais problemáticas. Pelas semelhanças entre os institutos jurídicos, é fácil comparar a legislação luso-brasileira por meio da leitura de códigos e leis.

É claro que, nesta área, o principal tipo de burla/estelionato é aquele que permite a você ou outra pessoa obter uma vantagem ilícita. Isso pode ser feito por meio de artifício, ardil ou qualquer outro meio fraudulento. Perceber que a fraude é o objeto principal do tipo em estudo, que é o dano patrimonial perpetrado por meio de engano e

meio malicioso, é crime que tem punição prevista. No entanto, é necessário que exista uma queixa para que o mesmo se verifique.

A ordem penal material e formal limita-se à promoção e combate ao fenômeno social do "crime econômico e financeiro". Existem muitos diplomas legais que podem causar diferentes tipos de infrações penais. Estes incluem crimes fiscais (segurança social, fiscais, alfandegários fiscais), fraude e violação da fé contra o Estado, setor bancário, fraude e corrupção internacional, tráfico de influência e peculato e participação econômica em negócios, administração prejudicial, crimes do mercado de valores mobiliários, lavagem de dinheiro e outros. Os menores crimes econômicos e financeiros, como no caso das fraudes judiciais, não são tão explorados.

Uma vez que foi possível compreender o crime ora em estudo, aprofundou-se na sua compreensão mais contemporânea, onde ele passa a fazer parte de uma esfera dos crimes cibernéticos abertos, que são os que podem ser feitos utilizando-se ou não de ambientes virtuais, significando esta uma classificação de que este crime independe de recursos tecnológicos para ser executado, ainda que estes facilitem muito a sua prática.

Neste sentido, o presente estudo também possibilitou o conhecimento de que há um rol bastante grande nas modalidades dos crimes informáticos, podendo estar entre eles a fraude de identidades, quando informações pessoais são roubadas e usadas; fraude por e-mail e pela Internet; roubo e venda de dados corporativos; roubo de dados financeiros ou relacionados a pagamento de cartões; ataques de ransomware, um tipo de extorsão cibernética; extorsão cibernética, que exige dinheiro para impedir o ataque ameaçado; espionagem cibernética, quando hackers acessam dados do governo ou de uma empresa; cryptojacking, quando hackers exploram criptomoedas usando recursos que não possuem entre outros.

Ao olhar para a Internet como um bem jurídico independente, existem dois pontos de vista possíveis: ações ou crimes que merecem incriminação praticados utilizando-se a internet e ações ou crimes que merecem incriminação contra a Internet praticados, enquanto autônomo bem jurídico. O primeiro pode incluir crimes que resultem em conduta livre, crimes conexos, crimes de conduta simples ou formais (embora não seja necessário distingui-los) e crimes com finalidade específica. No entanto, a inclusão de elementos normativos pode ser possível. Nos crimes de resultado de conduta livre, à lei apenas importa o evento modificador da natureza, como, por exemplo, o crime de fraude. O crime, no caso, é provocar o resultado do dano patrimonial, qualquer que tenha sido o meio ou a ação que o causou.

Foi possível ainda observar que esses crimes podem caracterizar-se como crimes de informática próprios, impróprios, mistos e ainda mediatos. No caso do primeiro,

ocorre quando os dados informáticos foram violados. Já o impróprio ocorre quando o computador, normalmente empregando-se a internet, serve apenas como meio para que o crime fim seja realizado. Os mistos protegidos pela norma como dois diferentes bens jurídicos, estando obrigatoriamente entre eles a inviolabilidade dos dados informáticos e a lesão. E o crime informático mediato, o qual é utilizado como meio para que depois se realize o crime fim. Uma vez da existência do princípio da consunção, a punição ocorre apenas para o crime fim.

Em casos criminais envolvendo crimes contra a propriedade, alguns países adotaram a disponibilidade da técnica de propriedade no direito penal. A título de exemplo, na legislação penal portuguesa, título II, crimes contra a propriedade, um grande número de crimes que não envolvem violência ou ameaça grave à vítima têm como ação penal, a privada. Uma reclamação pode ser apresentada por simples roubo, abuso de confiança e usurpação ou alteração de marcos, fraude e usura.

O Código Penal de Portugal, que trata do furto e do roubo é também o mais avançado em termos de penas de prisão, é o *ultima ratio*. Prevê a pena mais baixa para um crime que tenha sido definido de forma idêntica em todos os códigos penais examinados, bem como aquele com a pena mínima para outros crimes, que foram alcançados pela modernidade.

O Código Penal brasileiro difere do português na forma como valoriza os meios de estelionato, diferencia as penas dos crimes mais simples dos mais complicados e no valor que tem o bem material, o que pode ter impacto no montante das penas aplicadas.

Além disso, é sabido que a consumação do crime só ocorre após a obtenção de vantagem indevida. Isso corresponde a danos materiais. É um crime material porque exige a produção do resultado. A tentativa de criar o resultado será considerada malsucedida se não for produzida.

Observou-se ainda que o sujeito ativo de estelionato pode ser qualquer pessoa, podendo ainda ser mais de uma. É uma pratica comum no estelionato que duas pessoas apliquem o golpe, sendo ainda possível que um agente engane a vítima para garantir a um terceiro a vantagem, podendo este responder pelo delito se estiver de má-fé. Seguindo essa esteira, caso descubra o beneficiário antes que a vantagem ilícita seja obtida, cometerá o crime de receptação dolosa, posterior ao acontecido por apropriação de coisa havida por erro.

Em relação à competência, pode-se observar que, segundo a teoria da atividade, o local do crime é considerado o da omissão/ação. De acordo com a teoria do resultado, a cena do crime é onde está o resultado ou se deveria ter ocorrido. Finalmente, de acordo com a teoria da Ubiquidade, a cena do crime seria o cruzamento de duas teorias. Este seria o local da ação / omissão, bem como o local onde ela produziu o resultado.

Assim, o crime de burla qualificada não difere muito do tipo básico descrito no artigo 217.º do CP. Nesse sentido, é evidente que o Estado não é mais diligente no exercício do *jus puniendi*. Isso se deve à prática reiterada e difundida do ilícito, bem como à crescente gravidade e precariedade nos prejuízos financeiros e econômicos aos sujeitos. Esse preceito legal foi criado com a reforma de 1995, que substituiu o artigo 314.º no CP de 1982. Daí resulta que a diferença maior encontrada versa na ocorrência de dois níveis distintos de "qualificação", até porque contempla o prejuízo de valor "elevado" ou "consideravelmente elevado" no texto da disposição legal.

A possibilidade de extradição por burla / estelionato merece destaque. A situação do Brasil é que a extradição não é impedida pelo fato de o extraditado ser casado com uma brasileira e ter um filho brasileiro. A prescrição do pedido punitivo pelo delito de fraude qualificada no Código Penal português produz efeitos em 10 anos, enquanto a prescrição por peculato é tida em conta pelo Código Penal brasileiro em 12 anos.

Assim, entendemos que a lei penal deve ser pensada de forma séria, sob pena de ser utilizada meramente de forma simbólica, que "atende" de forma precipitada os anseios sociais. Ela deve partir de uma política criminal adequada, e não apenas para "tapar o sol com a peneira". Pensamos assim porque nos parece que o legislador, a respeito do crime hora em questão, pensou em aumentar a pena apenas porque esta modalidade de delito aumentou em decorrência dos instrumentos tecnológicos que lhe conferiram maior dinamismo.

A verdade é que se aumenta a pena e não se lhe aplica, porque não há quem se punir. Logo, opção desnecessária e sem eficácia, trabalho do legislador em vão, já que para o estelionato já há punição prevista. O que se deve fazer é haver investimentos na inteligência da polícia bem como na polícia científica, pois a dificuldade agora está em capturar e provar a culpa dos criminosos.

REFERÊNCIAS

Acórdão do Tribunal da Relação de Coimbra. (2011, 26 janeiro). *Burla Tributária*: Elementos Constitutivos. Relator: Eduardo Martins. Recuperado em 21 abril, 2021, de http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/73f64d621743e9a280257842003ce75b?OpenDocument.

Acórdão do Tribunal da Relação de Coimbra. (2016, 02 fevereiro). *Processo 902/13.4TBCNT.C1*. Relator: Arlindo Oliveira. Recuperado em 08 junho, 2021, de http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/aba8f7cea02531c180257f4f003e6e54?OpenDocument.

Acórdão do Tribunal da Relação de Évora. (2012, 26 junho). *Burla informática*: tentativa meio idóneo. Relator: João Martinho de Sousa Cardoso. Recuperado em 21 abril, 2021, de http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/9e4d23e33c93144580257de10056f883?OpenDocument.

Acórdão do Tribunal da Relação do Porto. (2018, 21 fevereiro). *Burla informática*: crime de apropriação ilegítima de coisa achada. Relator: Neto Moura. Recuperado em 21 abril, 2021, de http://www.dgsi.pt/jtrp.nsf/-/09A6786FB4EE2B6D802582AC00561189.

Aguiar, T. L. S. (2017). *O correio eletrônico*: a apreensão e a interceção no processo penal português. Dissertação de mestrado, Universidade de Coimbra, Coimbra, Portugal.

Albertin, A. L. (2010). *Comércio eletrônico*: modelo, aspectos e contribuições de sua aplicação. (6a ed.) São Paulo: Atlas.

Albuquerque, P. S. P. de. (2015). *Comentário do Código Penal à luz da constituição portuguesa e da convenção dos direitos do homem*. (3a ed.) Lisboa: Universidade Católica.

Almeida, T. C. (2013). *O estelionato digital no e-commerce*: a fraude da loja virtual fantasma. Monografia de bacharelado, Universidade do Sul de Santa Catarina, Araranguá, SC, Brasil.

Alves Neto, V. (2019). *Considerações acerca do estupro virtual*. Monografia de Graduação, Universidade Federal de Tocantins, Palmas, TO, Brasil.

Alves, I. C. (2019). *Operações abusivas na banca eletrônica*: a imputação de responsabilidades pelas perdas resultantes da movimentação não autorizada de fundos. Dissertação de mestrado, Universidade Nova de Lisboa, Lisboa, Portugal.

Amador, N. J. R. (2012). *Cibercrime em Portugal*: Trajetórias e perspectivas de Futuro. Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, Portugal.

Andrade, M. C., & Dias, J. F. (1997). *Criminologia*: o homem delinquente e a sociedade criminógena. Coimbra: Coimbra.

Andreucci, R. A. (2010). *Código Penal anotado*. (4a ed.) São Paulo: Saraiva.

Ascenção, C. P. (2016). *O que é o E-commerce?* Recuperado em 02 maraço, 2021, de http://www.pwm.pt/eCommerce/Artigose-commerce/Oque%C3%A9eCommerce/tabid/3854/Default.aspx.

Associação Brasileira de Comércio Eletrônico. (2015, 02 fevereiro). *E-commerce brasileiro deve faturar R$ 49,8 bilhões em 2015.* ABCOMM. Recuperado em 01 março, 2021, de https://abcomm.org/noticias/e-commerce-brasileiro-deve-faturar-r-498-bilhoes-em-2015/.

Barbosa, C. J. R., & Rocha, K. S. C. S. C. (2016). A responsabilidade civil das operadoras de cartão de crédito quanto aos clientes vítimas de estelionato e furto mediante fraude. *Revista Científica do Centro de Estudos em Desenvolvimento Sustentável da UNDB*, 1(4), 1-19.

Barros, J. M. (2015). *Lei n. 12.737*: a nova tipificação criminal de delitos informáticos. Artigo Científico de Pós Graduação em Direito, Escola da Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, RJ, Brasil.

Barros, M. P. (2020). *Crime de colarinho branco e género*. Dissertação de mestrado, Universidade do Porto, Porto, Portugal.

Bernardi, L. M. (2021). *E-commerce cactus*: processos e desenvolvimento. Artigo de graduação. Universidade Presbiteriana Mackenzie, São Paulo, SP, Brasil.

Besouchet, E. (2015). *Vitrine de natal da John Lewis*: uma colherada de alegria festiva. Recuperado em 02 março, 2021, de https://www.vitrinemaniablog.com.br/vitrine-de-natal-da-john-lewis-uma-colherada-de-alegria-festiva/.

Bicho, J. I. P. (2020). *A influência do turismo nos volumes crimes uma análise ao fenómeno do furto por carteirista na cidade de Lisboa*. Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, Portugal.

Bitencourt, C. R. (2009). *Tratado de Direito Penal*. (5a ed.). São Paulo: Saraiva.

Bitencourt, C. R. (2011). *Tratado de Direito Penal*: Parte especial. (7a ed.). São Paulo: Saraiva.

Bitencourt, C. R. (2014). *Tratado de Direito Penal*: Parte geral. (20a ed.). São Paulo: Saraiva.

Bitencourt, C. R. (2018). *Tratado de Direito Penal*. Parte especial (arts. 155 ao 212, Vol. 3, 14a ed.). São Paulo: Saraiva.

Bornia, A. C., Donadel, C. M., & Lorandi, J. A. (2006, outubro). A logística do comércio eletrônico do B2C (business to consumer). *Anais do Encontro Nacional de Engenharia da Produção*, Fortaleza, CE, Brasil, 26.

Cabette, E. L. S. (2018, novembro). Torpeza ou fraude bilateral no estelionato sob a ótica da vitimodogmática e da autoproteção. *Boletin IBCCrim*, São Paulo, 26(312), 7-8.

Caiado, R. A. R. (2020). *A aplicação do uso da força no ciberespaço*. Dissertação de mestrado, Universidade de Lisboa, Lisboa, Portugal.

Carvalho, A. B. de, & Silva, G. B. da. (2020). *Aluga office*: E-commerce para home office. Artigo de bacharelado, Centro Universitário do Planalto Central Aparecido dos Santos, Brasília, DF, Brasil.

Carvalho, D. (2018). *Portugal*: retalho do futuro. Dissertação de mestrado, Universidade Católica Portuguesa, Porto, Portugal.

Cerqueira, S. C., & Rocha, C. (2013). Crimes cibernéticos: desafios da investigação. *Cadernos Aslegis*, Brasília, (49), 131-136.

Chaffey, D. (2013). *Gestão de e-business e e-commerce*. Rio de Janeiro: Elsevier.

Chanana, N., & Goele, S. (2012). Future of e-commerce in India. *International Journal of Computing & Business Research*, 8, 1-8.

Chanes, T. M. (2015). *Estelionato Judiciário*. Monografia de bacharelado, Universidade Municipal de São Caetano do Sul, São Caetano do Sul, SP, Brasil.

Chaussard, C. (2015). *E-commerce*. Palhoça: Unisul.

Choi, J., & Nazareth, D. L. (2014). Repairing trust in na e-commerce and security context: an agent-based modeling approach. *Information Management & Computer Security*, 22(5), 490-512.

Coimbra, M. C. S. (2020). *Phishing e o código penal brasileiro*: como tipificar a conduta? Uma análise do acórdão em apelação criminal nº 5002347-69.2010.404.7000, do tribunal regional federal da 4ª Região, com base na *novatio legis in mellius*. Monografia de bacharelado, Universidade Federal Fluminense, Macaé, RJ, Brasil.

Comissão Europeia. (2013). *Estratégia da União Europeia para a cibersegurança*: um ciberespaço aberto, seguro e protegido. Bruxelas: JOIN.

Conflito de Competência 67343/GO. (2007, 11 dezembro). Relator: Ministra Laurita Vaz. Terceira Seção. *Diário de Justiça*. Recuperado em 21, abril, 2021 de https://stj.jusbrasil.com.br/jurisprudencia/8787855/conflito-de-competencia-cc-67343-go-2006-0166153-0/inteiro-teor-13863234.

Consoni, E. R. (2011). *Fraude contra credores*: estudo sobre as correntes doutrinárias acerca dos efeitos da ação pauliana. Monografia de Graduação, Universidade Extremo Sul Catarinense, Criciúma, SC, Brasil.

Copeto, R. (2016, 16 novembro). *Cibercriminalidade*. Recuperado em 08 junho, 2021, de https://www.lidadornoticias.pt/opiniao-rogerio-copeto-oficial-da-gnr-cibercriminalidade/.

Correia, P. M. A. R., & Jesus, I. O. A. (2016). Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas. *Revista Direito GV*, 12(2), 542-563.

Costa, C. R. S. (2017). *As proibições de prova e a prova digital - aproximação aos lugares-comuns de um instituto clássico em face de uma nova realidade*. Dissertação de mestrado, Universidade do Minho, Braga, Portugal.

Costa, D. O. (2019). *Crimes virtuais*: uma breve análise da legislação brasileira sobre o tema. Artigo científico de graduação, Faculdade Cesmac do Agreste, Arapiraca, AL, Brasil.

Costa, E. C. I. da. (2019). *As regras de aplicação da lei no tempo nos crimes tributários continuados*. Dissertação de mestrado, Universidade do Minho, Braga, Portugal.

Costa, M. A. R. (1995). *Crimes de informática*: Introdução e história do computador. Recuperado em 21 abril, 2021, de https://egov.ufsc.br/portal/sites/default/files/29402-29420-1-pb.pdf.

Costa, M. V. G. (2018, 02 novembro). *Fraude Bancária*: A tipicidade do crime. Gutenberg, Jornal Digital. Recuperado em 21 abril, 2021, de https://www.gutenberg.com.br/_files/200000391-85d8485d88/Bank%20Fraud-5.pdf.

Costa, P. S. V. (2018). *Aceitação e uso da tecnologia para a poupança individual em Portugal*: aplicação do modelo UTAUT2. Dissertação de mestrado, Universidade Nova de Lisboa, Lisboa, Portugal.

Crespo, M. X. F. (2011). *Crimes digitais*. São Paulo: Saraiva.

Cunha, R. S. (2014). *Manual de Direito Penal*. Parte especial (arts. 121 ao 361, 6a ed.). Salvador: Juspodivm.

Damasceno, L. G. B. (2007, abril). *Aspectos penais sobre as transações bancárias indevidas via internet banking*. Recuperado em: 21 abril, 2021, de https://jus.com.br/artigos/9697/aspectos-penais-sobre-as-transacoes-bancarias-indevidas-via-internet-banking.

Damiani, J. R. (2019). *Crimes cibernéticos*. Monografia de graduação, Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Três Passos, RS, Brasil.

Dantas, L. E. M. (2013). *Da aplicação do princípio da insignificância nos crimes de estelionato contra a previdência social*. Monografia de bacharelado, Universidade Federal do Ceará, Fortaleza, CE, Brasil.

Dapper, D. T. (2012). *Análise acerca do momento consumativo do crime de estelionato previdenciário*: exposição dos diferentes entendimentos expostos pela doutrina e jurisprudência e os reflexos jurídicos daí advindos. Monografia de graduação, Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Santa Rosa, RS, Brasil.

Decreto n. 7.962, de 15 de março de 2013. (2013, 15 março). Regulamenta a Lei no 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. *Diário Oficial da União*. Brasília.

Decreto-Lei n. 2.848, de 7 de dezembro de 1940. (1940, 7 dezembro). Código Penal. *Diário Oficial da União*, Brasília.

Dias, E. S. B. (2018). *Comércio eletrônico*: a vulnerabilidade de dados do consumidor. 2018, 22 f. Artigo de bacharelado, Faculdade Antonio Meneghetti, Restinga Sêca, RS, Brasil.

Dias, J. F. (1999). *Comentário conimbricense do código penal*. Tomo I e II. Coimbra: Coimbra.

Dias, J. F., & Andrade, M. C. (2013). *Criminologia*: o homem e a sociedade criminógena. Coimbra: Coimbra.

Dias, J. F., & Brandão, N. (2015). *O crime de burla tributária*. Estudos em homenagem a Rui Machete. Recuperado em 16 março, 2021, de https://eg.uc.pt/bitstream/10316/80402/1/JFD%20e%20NB%20-%20Burla%20Tribut%C3%A1ria%202015.pdf.

Diniz, L. L., Souza, L. G. A. de, Conceição, L. R. da, & Faustini, M. R. (2011, outubro). O comércio eletrônico como ferramenta estratégica de vendas para empresas. *Anais do Encontro Científico e Simpósio de Educação Unisalesiano*, Lins, SP, Brasil, 3.

Diniz, R. M. (2019). *O ordenamento jurídico brasileiro e as relações de consumo no comércio eletrônico*. Monografia de graduação, Universidade Católica de Salvador, Salvador, BA, Brasil.

Domingues, J. D. M. (2020). *A venda de falsos estupefacientes e substâncias psicotrópicas*. Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, Portugal.

Dutra, K. (2011, 11 julho). *A evolução do comércio eletrônico no Brasil*: social commerce. Recuperado em 01 março, 2021, de http://pnld.moderna.com.br/2011/07/11/a-evolucao-do-comercioeletronico-no-brasil-%E2%80%93-social-commerce/.

Ebit. (2017). *Webshoppers 2017*. Fecomercio. Recuperado em 01 março, 2021, de https://www.fecomercio.com.br/public/upload/editor/pdfs/webshoppers_35_edicao.pdf.

Ebit. (2019). *Webshoppers 2019*. Recuperado em 01 março, 2021, de http://www.medsobral.ufc.br/pdf/Webshoppers_39.pdf.

Ebitempresa (2015). *WebShoppers*: balanço 2014 e expectativas para 2015. Recuperado em 01 março, 2021, de http://img.ebit.com.br/webshoppers/pdf/31_webshoppers.pdf.

Eckert, A. Dal Bó, G., Sperandio, M., G., & Eberle, L. (2017). E-commerce: privacidade, segurança e qualidade das informações como preditores da confiança. *Revista Pensamento Contemporâneo em Administração*, 11(5), 49-69.

Ecommerce. (2014). *Vendas no comércio eletrônico do Brasil*: evolução da internet e do e-commerce. Recuperado em 03 março, 2021, de http://www.ecommerce.org.br.

Escóssia, R. Problemas genéricos do discurso jurídico-penal na [e sobre a] internet e outros ciberespaços: uma revisão narrativa de literatura sobre crimes digitais próprios e impróprios. In Rocha, L. R. L. et al. (coords.). *Crimes digitais*. Caderno de pós-graduação em direito (pp. 06-41). Brasília: UniCEUB/ICPD.

Eurocommerce. *The european ecommerce report 2018*: Relevant findings outlined. Recuperado em 02 março, 2021, de https://www.eurocommerce.eu/media/159952/2018.07.02%20-%20Ecommerce%20report_annex.pdf.

Farah, D. M. (2017). *A adequada tipificação criminal do saque em caixa eletrônico com a utilização de cartão clonado*: um confronto entre os postulados clássicos dos delitos de estelionato e furto qualificado mediante fraude com a realidade contemporânea. Monografia de bacharelado, Centro Universitário de Brasília, Brasília, DF, Brasil.

Faria, B. N. de. (2019). *As ações encobertas e a fase de Julgamento*. Monografia de mestrado, Universidade Nova de Lisboa, Lisboa, Portugal.

Ferraz, A. B. S. (2020). *O crime de tráfico de pessoas*: as insuficiências do artigo 160º do Código Penal à luz do atual contexto social. Dissertação de mestrado, Universidade Católica Portuguesa, Porto, Portugal.

Ferreira, E. V. (2011). Privação económica e criminalidade: o caso português (1993-2009). *Sociologia, Problemas e Práticas*, 67, 107-125.

Ferreira, I. (2018). *Infracções tributárias*: burla tributária no contexto dos crimes fiscais. Dissertação de mestrado, Instituto Politécnico de Lisboa, Lisboa, Portugal.

Ferreira, I. S. (2011). A criminalidade informática. In Ferreira, I. S. *Direito e internet*: aspetos jurídicos relevantes. Bauru: Edipro.

Fidalgo, M. (2017, janeiro). Burla relativa a trabalho ou emprego. *Revista Julgar*, [online], 1-31. Recuperado em 16 março, 2021, de http://julgar.pt/burla-relativa-a-trabalho-ou-emprego/.

Filipe, M. J. P. S. (2018). *A criminalidade económica e financeira*: o tipo legal de burla e os agentes do crime. Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, Portugal.

Fiorillo, C. A. P., & Conte, C. P. (2016). *Crimes no meio ambiente digital e a sociedade da informação*. (2a ed.) São Paulo: Saraiva.

Freitas, A. R. R. P. de. (2017). *QR Code - tendência de evolução comercial no ponto-de-venda físico de retalho*. Dissertação de mestrado, Universidade Europeia, Portugal.

Freitas, J. P. C. B. (2017). *Os meios de obtenção de prova digital na investigação criminal*: o regime jurídico dos serviços de correio eletrônico e de mensagens curtas. Dissertação de mestrado, Universidade do Minho, Braga, Portugal.

Garcia, M. M., & Rio, C. J. M. (2015). *Código Penal*. Parte geral e especial. (Vol. II, 2a ed.). Lisboa: Almedina.

Gasalho, J. M. S. (2013). *A burla tributária*: a norma incriminadora, as relações de concurso com a fraude fiscal e outras considerações. Monografia de mestrado, Universidade Católica Portuguesa, Lisboa, Portugal.

Geraldes, A. V. (2013). Phishing: fraude on line. *Revista da Faculdade de Direito da Universidade de Lisboa*, 54(1), 87-102.

Goberto, M. (2011). *As grandes vantagens de um comércio eletrônico*. Recuperado em 02 março, 2021, de http://ecommercenews.com.br/artigos/cases/as-grandes-vantagensde-um-comercio-eletronico.

Godara, R. (2016). Challenges and future scope of e-commerce in India. International. *Journal of Emerging Trends & Technology in Computer Science*, 5(2), 232-235.

Greco, R. (2011). *Código Penal comentado*. (5a ed.). Niterói: Impetus.

Greco, R. (2017). *Código Penal comentado*. (11a ed.). Niterói: Impetus.

Guarda Nacional Republicana. (2020). *Criminalidade Contra Idosos registada pela GNR, entre 2013-2019 (DI)*. Lisboa: GNR.

Guimarães, V. (2018, 16 julho). *7 motivos que levam ao crescimento do comércio eletrônico no Brasil.* Venda Mais. Recuperado em 02 março, 2021, de https://www.vendamais.com.br/7-motivos-que-levam-ao-crescimento-do-comercio-eletronico-no-brasil/.

Hobaica, R. C. (2016, 19 agosto). *Direito comparado*: crimes de furto, roubo e estelionato no Código Penal Brasileiro comparados a três países diferentes. Jusbrasil. Recuperado em 04 março, 2021, de https://rchobaica.jusbrasil.com.br/artigos/375193561/direito-comparado-crimes-de-furto-roubo-e-estelionato-no-codigo-penal-brasileiro-comparados-a-tres-paises-diferentes#:~:text=O%20C%C3%B3digo%20Penal%20Brasileiro%20difere,irris%C3%B3rio%2C%20na%20majora%C3%A7%C3%A3o%20das%20penas.

Humelnicu, I. V. (2016). Sextortion-The newest online threat. *AGORA International Journal of Administration Sciences*, 1(1), 7-13.

Hungria, N. (2012). *Comentários ao Código Penal*. Rio de Janeiro: Forense.

Hyochimoto, R. H. (2020). *A vulnerabilidade do consumidor no comércio eletrônico*. Monografia de bacharelado, Universidade Cesumar, Maringá, PR, Brasil.

Isaías, P., Sousa, I. D., Carvalho, L. C., & Alturas, B. (2017). *E-business e economia digital*: desafios e oportunidades num contexto global. Lisboa: Sílabo.

Jesus, D. de. (2014). *Direito penal, parte especial.* (Vol. 2, 34a ed.). São Paulo: Saraiva.

Kacen, J. J., Hess, J. D., & Chiang, W. Y. K. (2013). Bricks or clicks? Consumer attitudes toward traditional stores and online stores. *Global Economics and Management Review*, 18(1), 12-21.

Khan, A. G. (2016). Electronic commerce: a study on benefits and challenges in an emerging economy. *Global Journal of Management and Business Research*, 16(1-B), 18-22.

Khosla, M., & Kumar, H. (2017). Growth of e-commerce in India: an analytical review of literature. *IOSR Journal of Business and Management*, 19(6), 91-95.

Kotler, P. (2017). *Marketing 4.0*. Rio de Janeiro: Sextante.

Kumar, R., & Nagendra, A. (2018). An analysis of the rise of e-commerce in Índia. *Journal of Applied Management-Jidnyada*, 10(1), 12-20.

Kunrath, J. C. T. M. (2014). *A expansão da criminalidade no ciberespaço*: desafios de uma política criminal de prevenção ao cibercrime. Dissertação de mestrado, Universidade Federal da Bahia, Salvador, BA, Brasil.

Lei de 16 de dezembro de 1830. (1831, 07 janeiro). Manda executar o Código Criminal. *Diário Oficial da União*. Rio de Janeiro.

Lei n. 12.737, de 30 de novembro de 2012. (2012, 03 dezembro). Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. *Diário Oficial da União*. Brasília.

Lima, G. C. S. (2018). *Crimes informáticos*: análise dos processos de criminalização. Monografia de bacharelado, Universidade Federal do Rio Grande do Norte, Natal, RN, Brasil.

Liu, J., Travers, M., & Chang, L. Y. (2017). *Comparative criminology in Asia*. Switzerland: Springer International Publishing.

Lôbo, P. (2017). *Direito Civil 1*. Parte geral. São Paulo: Saraiva.

Lopes, J. J. G. (2017). *A aplicação do princípio da insignificância no crime de estelionato mediante cheque de pequeno valor sem provisão de fundos*. Monografia de bacharelado, Universidade Federal de Campina Grande, Sousa, PB, Brasil.

Lopes, P. A. (2020). Computação forense e a prova pericial. In Lóssio, C. J. B., Nascimento, L., & Tremel, R. (orgs.) *Cibernética jurídica*: estudos sobre direito digital. (pp. 262-270). Campina Grande: Eduepb.

Lunardi, G. (2018, 12 junho). *12 dados que comprovam o crescimento do e-commerce no Brasil*. E-commerce Brasil. Recuperado em 02 março, 2021, de https://www.ecommercebrasil.com.br/artigos/12-dados-que-comprovam-ocrescimento-do-e-commerce-no-brasil/.

Machado, A. M. D. C. (2014). *Fraude no medicamento*: burla. Dissertação de mestrado, Universidade do Porto, Porto, Portugal.

Machado, T. J. X. (2017). *Cibercrime e o crime no mundo informático*: a especial vulnerabilidade das crianças e dos adolescentes. Dissertação de mestrado, Universidade Fernando Pessoa, Porto, Portugal.

Maia, T. S. F. (2017). *Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro*. Monografia de bacharelado, Universidade Federal do Ceará, Fortaleza, CE, Brasil.

Mann, D. C. (2018). *Infiltração digital*: a validade como meio de prova e os limites éticos do estado-investigador. Dissertação de doutorado, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, Portugal.

Manzi, M. L. (2020). *Análise da importância da criação de um e-commerce para uma empresa goiana do ramo de vestuário feminino*. Monografia de graduação, Pontifícia Universidade Católica de Goiás, Goiás, GO, Brasil.

Marian, O. (2018). *Tendências de consumo de alimentos biológicos*: estudo do cliente do El Corte Inglés. Dissertação de mestrado, Universidade Nova de Lisboa, Lisboa, Portugal.

Marques, A. C. F. (2019). *Relatório de estágio curricular no Tribunal Judicial da Comarca de Lisboa, Juízo Central Criminal*. Monografia de mestrado, Universidade Nova de Lisboa, Lisboa, Portugal.

Martinez, T. H. (2019). *Os direitos fundamentais x segurança pública*: a admissibilidade de métodos ocultos de investigação criminal em ambiente digital. Dissertação de mestrado, Universidade de Lisboa, Lisboa, Portugal.

Martins, J. A. (2013). *Infracções fiscais*. Lisboa: OTOC.

Matos, F. (2016). *Crimes virtuais*: uma análise à luz do ordenamento jurídico pátrio. Monografia de bacharelado, Universidade de Passo Fundo, Lagoa Vermelha, RS, Brasil.

Maues, G. B. K., Duarte, K. C., & Cardoso, W. (2018). Crimes virtuais: uma análise sobre a adequação da legislação penal brasileira. *Revista Científica da Fasete*, 1(1), 166-180.

Melo. M. A. (2013). *Os mecanismos utilizados na fraude eletrônica inerente ao internet banking segundo Claudio Antônio de Paiva Simon*: *scam, phishing e pharming*.

Monografia de bacharelado, Universidade do Sul de Santa Catarina, Araranguá, SC, Brasil.

Meloto, G. J., Soares, A. B., & Chaia, R. R. (2020). In Amaral, A. J. et al. (coords.). *Anais do Congresso Internacional de Ciências Criminais – PUCRS*. Direito Penal. (vol. 3, pp. 231-241). São Paulo, SP, Brasil, 10.

Mesquita Filho, J. P. (2020) Crimes próprios e impróprios do meio digital. In Rocha, L. R. L. et al. (coords.). *Crimes digitais*. Caderno de pós-graduação em direito (pp. 42-57). Brasília: UniCEUB/ICPD.

Mirabete, J. F., & Fabbrini, R. N. (2008). *Manual de direito penal*. (25a ed.). São Paulo: Atlas.

Nakamura, A. M. (2011). *Comércio eletrônico riscos nas compras pela internet*. Dissertação de graduação, Faculdade de Tecnologia de São Paulo, São Paulo, SP, Brasil.

Nascimento, H. A. S. (2014). *Fraude contra seguro*. Monografia de bacharelado, Centro Universitário Eurípides, Marília, SP, Brasil.

Nova, L. R. V., & Santos, V. C. A. (2019). *Efeitos típicos da torpeza bilateral no crime de estelionato*. Monografia de bacharelado em Direito) – Universidade de Uberaba, Uberaba, SP, Brasil.

Ntech. (2020, 20 abril). *Comércio eletrônico*: Portugal continua na cauda da Europa. Recuperado em 25 fevereiro, 2021, de https://www.ntech.news/comercio-eletronico-portugal-continua-na-cauda-da-europa/.

Nucci, G. S. (2003). *Código penal comentado*. (4a ed.). São Paulo: Revista dos Tribunais.

Observador. (2016, 22 janeiro). Burla com taxas moderadores através de SMS. Recuperado em 21 abril, 2021, de https://observador.pt/2016/01/22/burla-taxas-moderadores-atraves-sms/.

Oliveira, E. (2014, 20 outubro). *Vantagens e desvantagens de cria um e-commerce*. Atitude e Negócio. Recuperado em 01 março, 2021, de http://atitudeenegocios.com/vantagens-e-desvantagens-do-e-commerce/.

Oliveira, F. M. de. (2013). *Pseudo*: uma análise sociocognitiva sobre insinceridades, mentiras e crimes de fraude. Tese de doutorado, Universidade Federal do Rio Grande do Norte, Natal, RN, Brasil.

Panda, R., & Swar, B. N. (2013). Online shopping: An exploratory study to identify the determinants of shopper buying behaviour. *International journal of business insights & transformation*, 7(1), 52-59.

Pecenec, I., & Zoroja, J. (2018). Study on e-commerce in Croatia: customers' preferences. *Entrenova*, 6(8), 397-403.

Pedra, C. G. (2019). *Crime de burla informática e nas comunicações*: enquadramento jurídico, prática e gestão processual. In: Pereira, L. M. C. S. *et al*. (orgs). O crime de abuso de cartão de garantia e crédito e o crime de burla informática. (Coleção Formação. Ministério Público, pp. 11-38). Lisboa: Centro de Estudos Judiciários.

Pedra, C. G. (2019). Crime de burla informática e nas comunicações: enquadramento jurídico, prática e gestão processual. In *O crime de abuso de cartão de garantia e crédito e o crime de burla informática*. Coleção formação. Ministério Público. (Trabalhos do 2º ciclo do 32º curso, pp. 11-38). Lisboa: Centro de Estudos Judiciários.

Pereira, A. M. M. S. (2018). *As relações entre o crime de tráfico de pessoas e o crime de escravidão.* Dissertação de mestrado, Universidade Católica Portuguesa, Porto, Portugal.

Pereira, D. F. M. (2020, 09 janeiro). *Modificações ao Artigo 171 do Código Penal (Crime de Estelionato) Realizadas Através da Lei 13.964/2019 (Pacote Anticrime) – Repercussões na Atividade de Investigação da Polícia Civil*. Recuperado em 21 abril, 2021, de http://www.adpeb.com.br/v18/wp/wp-content/uploads/2020/01/Altera%C3%A7%C3%A3o-do-art.-171-Lei-anticrime.pdf.

Pereira, F. D. Q. (2018). *A recuperação da informação em sites de comércio eletrônico*. Monografia de bacahrelado, Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, Brasil.

Pereira, N. F. R. (2020). O regulamento geral de proteção de dados e osint. In Lóssio, C. J. B., Nascimento, L., & Tremel, R. (orgs.) *Cibernética jurídica*: estudos sobre direito digital. (pp. 229-240). Campina Grande: Eduepb.

Pereira, V. S., & Lafayette, A. (2014). *Código Penal*: anotado e comentado: legislação conexa e complementar. (2a ed.). Lisboa: Quid Juris.

Peres, R. (2010). *A guerra no Ciberespaço*: princípios da guerra clássica aplicados na Ciberguerra. Dissertação de Mestrado, Academia Militar, Lisboa, Portugal.

Ponceano, I. I. B. (2018). *Um estudo sobre a atratividade da compra online e do serviço drive - Hipermercado Jumbo de Portimão*. Dissertação de mestrado, Universidade do Algarve, Algarve, Portugal.

Portugal. (2020). *Relatório cibersegurança em Portugal*: Riscos & Conflitos. Observatório de Cibersegurança do Centro Nacional de Cibersegurança. Lisboa: CNCS.

Prado, L. R. (2011). *Curso de Direito Penal brasileiro*. (Vol. 2, 10a ed.). São Paulo: Revista dos Tribunais.

Prado, L. R. (2013). *Curso de direito penal brasileiro*: parte especial. (Arts. 121 a 249, Vol. 2, 11a ed.). São Paulo: Revista dos Tribunais.

Ramalho, D. S. (2017). *Métodos ocultos de investigação criminal em ambiente digital*. Coimbra: Almedina.

Ramos, E. D. (2017). *Crimes cibernéticos*: análise evolutiva e legislação penal brasileira. Monografia de Graduação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, Brasil.

Ray, S. (2011). Emerging trend of e-commerce in India: some crucial issues, prospects and challenges. *Computer Engineering and Intelligent Systems*, 2(5), 17-35.

Recurso em Sentido Estrito 608/RS. (2007, 21 novembro). Relator Desembargador Federal Luiz Fernando Wowk Penteado. Oitava Turma. *Diário de Justiça*. Recuperado em 21 abril, 2021, de https://trf-4.jusbrasil.com.br/jurisprudencia/1264171/recurso-em-sentido-estrito-rse-608-rs-20077100000608-6/inteiro-teor-9712083?ref=juris-tabs

Recurso em Sentido Estrito 7720/SP. (2011, 16 agosto). Relator: Desembargador Federal Cotrim Guimarães. Segunda Turma. *Diário de Justiça*. Recuperado em 21 abril, 2021, de https://trf3.jus.br.

Reis, E. S. R. P. (2019). *Apropriação indevida de identidade*: enquadramento jurídico-penal. Dissertação de mestrado, Universidade de Lisboa, Lisboa, Portugal.

Ribeiro, A. S. (2018). *Crimes informáticos*: As dificuldades jurídicas em se conter a criminalidade na internet. Monografia de bacharelado, Centro Universitário Católico Salesiano *Auxilium*, Lins, SP, Brasil.

Ribeiro, E. S. (2019). Crime de estelionato: uma análise da evolução sob a égide da impunidade na cidade de Manaus. *Revista Científica*, 1(169), 1-16.

Ribeiro, M. I., Fernandes, A., & Lopes, I. (2019). Comércio eletrônico: A percepção e a experiência de jovens e-buyers do ensino superior português. *Revista Risti*, (e24), 16-31.

Ribeiro, S. A. (2009, 30 outubro). *Os pioneiros da Internet em Portugal*. Em Público. Recuperado em 08 junho, 2021, de https://www.publico.pt/2009/10/30/tecnologia/noticia/os-pioneiros-da-internet-em-portugal-1407629.

Rocha, M. A. L. (1996). *A revisão do código penal*: soluções de neocriminalização. Lisboa: Centro de Estudos Judiciários.

Rocha, S. L. S. (2019). *Fatores que influenciam os consumidores portugueses na compra online*. Dissertação de mestrado, Universidade Lusófona de Humanidades e Tecnologias, Lisboa, Portugal.

Rodrigues, J. H. D. (2017, 3 abril). Advogado brasileiro em Portugal, advogado português no Brasil: panorama histórico e atual do regime de reciprocidade. *Revista Jus Navigandi*. Recuperado em 04 março, 2021, de https://jus.com.br/artigos/56788.

Rosa, F. (2007). *Crimes de Informática*. (3a ed.) Campinas: Bookseller.

Sá, A. A. G. (2017). *As representações sociais dos estudantes da Universidade do Minho sobre o fenómeno do cyberbullying*. Tese de mestrado, Universidade do Minho, Braga, Portugal.

Sanda, D. D. (2019). *Crime de estelionato no ambiente online*. Artigo de graduação, Centro Universitário de Maringá, Maringá, PR, Brasil.

Santos, A. L. B. (2018). *Vitimação por cyberstalking*: prevalência, impacto e fatores de risco em jovens adultos universitários. Dissertação de mestrado, Universidade do Porto, Porto, Portugal.

Santos, K. H. F. (2020). Cibercrime: uma breve análise dos sujeitos e principais delitos virtuais. In Rocha, L. R. L. et al. (coords.). *Crimes digitais*. Caderno de pós-graduação em direito (pp. 58-84). Brasília: UniCEUB/ICPD.

Santos, L. R. (2011). *Crimes virtuais e tutela penal*. Dissertação de mestrado, Universidade Estácio de Sá, Campos dos Goytacazes, RJ, Brasil.

Santos, P. C. S. (2019). *Estelionato previdenciário nos tribunais superiores*: uma análise de julgados para a aplicação e diferenciação da pena em crimes de natureza permanente, continuado e instantâneos de efeitos permanentes. Monografia de graduação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, Brasil.

Santos, R. C. (2005). *O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos - Studia Jurídica n. 82*. Coimbra: Coimbra.

Santos, V. S. (2017). *A fraude contra a segurança social e os crimes tributários, em especial o problema do concurso de crimes*. Dissertação de mestrado, Universidade de Coimbra, Coimbra, Portugal.

Sarkar, A. (2011). Impact of utilitarian and hedonic shopping values on individual's perceived benefits and risks in online shopping. *International Management Review*, 7(1), 58-65.

Saxena, R. P. (2019). Online shopping Behavior in west and esat: a comparative analysis if USA and UAE Shoppers. *Academy of Marketing Studies Journal*, 23(1), 1-26.

Shahariari, S., Shahariari, M., & Gheiji, S. (2015). Ecommerce and its impact on global trend and Market. *International Journal of Research -Granthalayah*, 3(4), 49-55.

Silva, G. M. da. (2009). *Direito penal tributário*: sobre as responsabilidades das sociedades e dos seus administradores conexas com o crime tributário. Lisboa: Universidade Católica Portuguesa.

Silva, G. O. S. (2017). *Dos crimes virtuais e as consequências jurídicas*. Dissertação de mestrado, Centro Universitário de Maringá, Maringá, PR, Brasil.

Silva, N. D. (2014). Estratégias discursivas para a percepção de fraude em e-mail. *Revista Tecnologia Educacional*, 31(206), 84-96.

Silva, R. C. (2015, 16 setembro). *Planejamento de interiores comerciais*. Recuperado em 02 março, 2021, de https://prezi.com/y5v-6-trz892/planejamento-de-interiores-comerciais/.

Silva, T. da. (2017). *A logística reversa no e-commerce*. Artigo de pós-graduação, Universidade do Sul de Santa Catarina, Tubarão, SC, Brasil.

Simas, D. (2014). *O cibercrime*. Dissertação de mestrado, Universidade Lusófona de Humanidades e Tecnologias, Lisboa, Portugal.

Smith, K. T. (2011). Consumer perceptions regarding E-commerce and related risks. *B>Quest*, (Spec. Sect.), 1-20.

Sonda, D. D. (2019). *Crime de Estelionato no ambiente online*. Artigo de graduação, Centro Universitário de Maringá. Maringá, PR, Brasil.

Souza Neto, P. A. (2009). *Crimes de informática*. Monografia de bacharelado, Universidade Vale do Itajaí, Itajaí, SC, Brasil.

Souza, G. A. de. (2002). *Fraude à execução e o direito de defesa do adquirente*. São Paulo: Juarez de Oliveira.

Souza, T. L. E. (2020). O crime de lavagem de dinheiro por meio da internet no Brasil: como prevenir diante das novas tecnologias? In Lóssio, C. J. B., Nascimento, L., & Tremel, R. (orgs.) *Cibernética jurídica*: estudos sobre direito digital. (pp. 47-63). Campina Grande: Eduepb.

Sydow, S. T. (2015). *Crimes informáticos e suas vítimas*. São Paulo: Saraiva.

Teixeira, A. (2020, 06 maio). *Como está a evoluir o e-commerce em Portugal em 2020*. Recuperado em 25 fevereiro, 2021, de https://digitalks.pt/artigos/a-evolucao-do-e-commerce-em-portugal/.

Theodoro Júnior, H. (2001). *Fraude contra credores*: a natureza da sentença pauliana. (2a ed.). Belo Horizonte: Del Rey.

Thomas, E. (2010, 13 agosto). *Crimes informáticos*: legislação brasileira e técnicas de forense computacional aplicadas a essa modalidade de crime. Recuperado em 08 junho, 2021, de https://artigos.etc.br/crimes-informaticos-legislacao-brasileira-e-tecnicas-de-forense-computacional-aplicadas-a-essa-modalidade-de-crime.html.

Turchi, S. R. (2018). *Estratégias de marketing digital e e-commerce*. São Paulo: Atlas.

Valente, M. M. (2017). Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias". *Revista Brasileira de Direito Processual Penal*, 3(2), 473-482.

Vellozo, J. P. B. (2015). *Crimes informáticos e criminalidade contemporânea*. Monografia de bacharelado, Universidade Luterana do Brasil, Gravataí, RS, Brasil.

Verdelho, P. (2009). Phishing e outras formas de defraudação nas redes de comunicação. *Direito da Sociedade da Informação*, 8, 407-419.

Vianna, T., & Machado, F. (2013). *Crimes Informáticos - Conforme a Lei n.º 12737/2012*. Belo Horizonte: Fórum.

Vieira, S. J. S. (2019). *Fatores que influenciam a intenção de compra de online groceries em Portugal*: o caso dos hipermercados portugueses online. Dissertação de mestrado, Instituto Politécnico de Coimbra, Coimbra, Portugal.

Vikram, A. M. A. (2012). *E-commerce*: opportunities and challenges. National Conference, At Bangalore.

Waghmare, G. T. (2012). E-commerce: a business review and future prospects in Indian business. *Indian Streams Research Journal*, 2(4), 1-4.

Wendt, E. (2010, 26 junho). *Compras online e o "estelionato virtual"*. Recuperado em 21 abril, 2021, de http://www.emersonwendt.com.br/2010/06/compras-online-e-estelionato-virtual.html.

Yulihasri, E., Islam, A., & Daud, A. K. (2011). Factors that influence customers' buying intention on shopping online. *International Journal of marketing studies*, 3(1), 128.

8 REFERÊNCIAS CONCLUSÃO

ECOMMERCE BRASIL. Comércio eletrônico cresce 21% em fevereiro com 1,49 bilhão de acessos. 24 mar. 2021. Disponível em: https://www.ecommercebrasil.com.br/noticias/comercio-eletronico-brasileiro-cresce-fevereiro/. Acesso em: 11 jun. 2021.

SOUZA, Joana Rita. Ecommerce em Portugal. 2021. Disponível em: https://activemedia.pt/ourjournal/ecommerce/. Acesso em: 11 jun. 2021.

BARROS, Joana Andreia Silva Moleiro. **Estudo de mercado sobre a atratividade da compra online e da App Auchan**: hipermercado Auchan de Faro. 2020. Tese de Doutorado em gestão de marketing. Universidade de Algarve, 2020.

Grande Consumo (2020). E-commerce em Portugal acelera por causa pandemia de Covid-19. Disponível em: https://grandeconsumo.com/e-commerce-em-portugalacelera-por-causa-pandemia-de-covid-19/#.X9Pl7tj7TIW. Acesso em 11 jun. 2021.

PROCON-SP. **Crescem reclamações contra compras online**. 14 jan. 2021. Disponível em: https://www.procon.sp.gov.br/crescem-reclamacoes-contra-compras-online/. Acesso em: 11 jun. 2021.

RECLAME AQUI. **2020 tem disparada em reclamações por atraso na entrega de produtos**. 21 jan. 2021. Disponível em: https://noticias.reclameaqui.com.br/noticias/2020-tem-disparada-em-reclamacoes-por-atraso-na-entrega-de-p_4111/. Acesso em: 11 jun. 2021.

PPLWARE. Que se passa com as compras online? Reclamações disparam 114%. 25 abr. 2021. Disponível em: https://pplware.sapo.pt/internet/que-se-passa-com-as-compras-online-reclamacoes-disparam-114/. Acesso em: 11 jun. 2021.

LIMA, Bruno de. **Fraudes no e-commerce cresceram 53% em 2020**. 10 fev. 2021. Disponível em: https://www.consumidormoderno.com.br/2021/02/10/fraudes-no-e-commerce-cresceram-53-em-2020. Acesso em: 11. Jun. 2021.

ECOMMERCE BRASIL. Fraudes no e-commerce podem gerar prejuízo de US$ 20 bilhões em 2021. 27 abr. 2021. Disponível em: https://www.ecommercebrasil.com.br/noticias/fraudes-no-e-commerce-podem-gerar-prejuizo-de-us-20-bilhoes-em-2021/. Acesso em: 11 jun. 2021.

PORTAL DA QUEIXA. **Sobre nós**. Disponível em: https://portaldaqueixa.com/about-us. Acesso em: 11 jun. 2021.

PORTAL DA QUEIXA. Quais as 5 principais formas de burla em ambiente digital? 21 maio 2021. Disponível em: https://portaldaqueixa.com/news/mais-de-2700-

reclamacoes-em-2021-quais-as-5-principais-formas-de-burla-em-ambiente-digital. Acesso em: 11 jun. 2021.