PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

FACULDADE DE DIREITO

ANDRÉ SCHICARIOL MAGRI

VITIMIZAÇÃO POR *PHISHING*: Uma análise no contexto dos crimes patrimoniais e das medidas de prevenção, assistência e reparação oferecidas pelo sistema jurídico para as vítimas.

São Paulo

2024

ANDRÉ SCHICARIOL MAGRI

VITIMIZAÇÃO POR *PHISHING*: Uma análise no contexto dos crimes patrimoniais e das medidas de prevenção, assistência e reparação oferecidas pelo sistema jurídico para as vítimas.

Dissertação apresentada à banca examinadora da **Pontifícia Universidade Católica de São Paulo**, como exigência parcial para obtenção do título de **BACHAREL** em **Direito**, sob a orientação da Profa. Dra. – **Greice Patrícia Fuller**.

São Paulo

2024

RESUMO

MAGRI, André Schicariol. **Vitimização por Phishing**: Uma análise no contexto dos crimes patrimoniais e das medidas de prevenção, assistência e reparação oferecidas pelo sistema jurídico para as vítimas.

O presente trabalho aborda o fenômeno do *phishing*, uma das práticas mais comuns e insidiosas no contexto dos crimes cibernéticos. A partir de estudos sobre o tema, busca-se compreender as técnicas de engenharia social utilizadas pelos criminosos para manipular as vítimas, explorando vulnerabilidades psicológicas e técnicas. O estudo da vitimização é central, analisando o papel da vítima no processo delitivo e destacando como ela, muitas vezes, participa ativamente, ainda que de forma inconsciente, para a concretização do crime.

Com base na vitimologia, ciência que estuda a vítima e seu processo vitimizatório, o trabalho explora classificações tradicionais de vítimas e aplica essas categorias ao contexto do *phishing*. Não obstante, discute-se a problemática da culpabilização da vítima, frequentemente estigmatizada pela sociedade, o que pode reforçar ciclos de vitimização e impedir a busca por reparação.

O trabalho também analisa o panorama legislativo brasileiro, apontando lacunas e desafios no enfrentamento aos crimes digitais. Embora leis como a Lei Carolina Dieckmann e o Marco Civil da Internet tenham representado avanços, a ausência de uma tipificação específica para o *phishing* gera insegurança jurídica e limita a eficácia do sistema penal. Por fim, são propostas medidas integradas para solução e/ou combate à problemática.

Assim, este estudo busca contribuir para a ampliação do debate jurídico e social sobre os crimes cibernéticos, enfatizando a necessidade de uma abordagem multidisciplinar para enfrentar a crescente complexidade das práticas criminosas no ambiente digital.

Palavras-chave: phishing; engenharia social; crimes cibernéticos; vitimologia; processo vitimizatório.

ABSTRACT

MAGRI, André Schicariol. **Vitimização por Phishing**: Uma análise no contexto dos crimes patrimoniais e das medidas de prevenção, assistência e reparação oferecidas pelo sistema jurídico para as vítimas.

This study examines phishing as a cybercrime based on social engineering techniques that exploit human and technological vulnerabilities to obtain sensitive information. Through the lens of victimology, it analyzes the victim's role in the criminal process, the consequences of phishing, and the challenges in its prevention and prosecution. The research highlights gaps in Brazilian legislation, particularly the absence of specific legal provisions for phishing, and discusses solutions involving digital education, public awareness, and legislative modernization. By addressing these issues, the study aims to contribute to the legal and social debate on protecting victims of cybercrimes and developing integrated strategies to combat these increasingly sophisticated criminal practices.

Keywords: phishing; social engineering; cybercrimes; victimology; victimization process.

Sumário

Introdução

A internet é um advento relativamente recente na história do homem, que tomou proporções inimagináveis, tornando-se o maior meio de comunicação e compartilhamentos de dados utilizado pelo ser humano em todas as partes do mundo contemporâneo. Por ser uma ferramenta emergente em constante ascensão, que se melhora e modifica a cada dia que passa, a maior parte da população mundial, mesmo se utilizando diariamente da ferramenta, ainda assim, não possui o preparo e a educação digital necessária para lidar com as armadilhas e programas maliciosos engendrados por criminosos que se utilizam do meio digital com a finalidade de aplicar golpes e usurpar dados pessoais dos usuários do ciberespaço.

Tais ferramentas e meios escusos, utilizados por esses criminosos digitais, se aperfeiçoam e evoluem no mesmo ritmo ou até mais rapidamente do que as novas tecnologias digitais e ferramentas convencionais de uso comum disponíveis na rede mundial de computadores, o que dificulta ainda mais seu enfrentamento, tanto pelas forças policiais, quanto pela legislação e ordenamento jurídico como um todo.

Dentre os diversos meios existentes para o cometimento de crimes no meio digital, busca a presente monografia, se aprofundar no estudo das espécies e formas de aplicabilidade do *phishing*, que em apertada síntese, consiste na utilização de técnicas de engenharia social, se aproveitando do analfabetismo digital geral da população, para ludibriar as vítimas e fazer com que estas, revelem, forneçam ou até mesmo permitam o acesso dos criminosos à informações sigilosas e pessoais, como nome de usuário, senhas, número de documentos pessoais, detalhes do cartão de crédito, dados bancários, entre outros.

Nesta senda, o objetivo de estudo principal deste trabalho, será investigar de forma aprofundada o papel da vítima – sua função e importância para a aplicabilidade do ilícito – no contexto e âmbito dos crimes que estão diretamente relacionados à prática do *phishing*. Será analisado o papel da vítima e seu processo vitimizatório, ou seja, o meio pelo qual a vítima contribui e se torna propriamente vítima do crime. Além disso, serão também avaliados quais os meios e medidas de prevenção, reparação e assistência às vítimas são oferecidos ou deixados de serem oferecidos pelo Estado e pelo ordenamento

jurídico pátrio, bem como, a eficácia e suficiência desses meios para, não só dirimir e evitar a prática criminosa, como também mitigar e até mesmo solucionar o processo de repetição do sofrimento das vítimas ao longo da persecução penal, e posteriormente, face à exposição perante o seio social e seus preconceitos já enraizados por meio da cultura brasileira.

Para tanto, a confecção do presente trabalho se alicerçará no método de pesquisa exploratório dedutivo, baseando-se principalmente no estudo de literatura doutrinária acerca do tema, coadunado com pesquisas realizadas por diversos meios e plataformas, análise dos dados coletados, análise informacional e jornalística e construção lógico-sistemática de conclusões, partindo-se de ideias formadas a partir dos conceitos de vitimologia, meios de prática do *phishing*, bem como, dos dados coletados nas pesquisas realizadas pelas diversas plataformas.

Por fim, espera-se apresentar possíveis propostas e medidas a serem tomadas para a resolução, ou ao menos, da mitigação da problemática.

Capítulo 1: Crimes Digitais

1.1 Nascimento Do Ciberespaço

Antes de abordar e dissecar o tema central do presente trabalho – o estudo do processo vitimizatório nos crimes em que é empregada a prática de *phishing* -, é necessário, inicialmente, estudar o surgimento do ciberespaço e compreender como essa ferramenta emergente, progressivamente evoluiu e se ampliou de tal forma que se tornou um instrumento de uso amplamente difundido e acessível ao público em geral.

Originalmente essa ferramenta fora idealizada para ser um meio de comunicação e compartilhamento de informações entre pesquisadores e instituições acadêmicas, mas em razão dessa evolução desenfreada e ampla disseminação ao público em geral, sua finalidade primária de uso foi quase que completamente deturpada.

Não obstante, o estudo do surgimento do ciberespaço nos permitirá também entender como o crescimento desenfreado e irregular da internet, coadunado com sua disseminação generalizada e irrestrita ao grande público, contribuiu para o surgimento e desenvolvimento concomitante de novas formas de criminalidade que exploram principalmente a vulnerabilidade dos usuários da rede mundial de computadores, os quais, em sua grande maioria, não possuem desenvoltura e educação digital suficientes para prevenir-se e evitar tais práticas maliciosas.

O ciberespaço, além de facilitar o acesso à informação e o compartilhamento de dados em escala global — funcionando como uma espécie de "espaço sem fronteiras" —, também propicia uma vasta gama de possibilidades para fraudes e crimes cibernéticos, que crescem exponencialmente a cada dia, principalmente porque esse ambiente virtual possibilita o anonimato de seus usuários e, por muito tempo, permaneceu sem regulamentação adequada ou fiscalização eficaz.

Por mais que a proposta inicial da internet tenha se desvirtuado, ela ainda é, atualmente, uma ferramenta de uso comum, integrada a praticamente todos os aspectos da vida moderna. Ou seja, sua principal função, idealizada nos primórdios de sua concepção, permanece intacta: o compartilhamento de informações.

O ciberespaço nada mais é do que a interconexão entre distintos e diversos bancos de dados ou computadores, com o intuito de compartilhar informações entre si.

O termo “rede mundial de computadores” se deve ao fato, de literalmente os computadores estarem interligados uns aos outros, seja por ondas de rádio, seja por cabeamento físico, seja por rede elétrica, seja por sinal de satélite, formando, dessa maneira, uma espécie de “rede invisível”, em que cada computador do mundo se conecta a outro, e esse outro se conecta a outros dois, esses outros dois se conectam a outros três e assim sucessivamente, até que exista um emaranhado de conexões e “nós” que permitem um incessante compartilhamento de informações.

O desenvolvimento e surgimento da internet se deu de forma muito parecida com a do computador. Ambas as “tecnologias” foram criadas a partir de inúmeras concepções e idealizações engendradas por indivíduos e grupos distintos, alocados em diferentes partes do mundo. Apesar disso, esses indivíduos e grupos, espalhados pelo globo terrestre, desenvolveram tais tecnologias de forma paralela, muitas vezes reaproveitando protótipos e estudos previamente realizados por outros criadores e inventores.

Assim, o início do desenvolvimento e criação tanto da internet quanto do computador teve origem em múltiplos pontos de partida, funcionando como uma espécie de processo que ocorreu de forma simultânea em várias regiões do mundo, demonstrando um esforço coletivo e colaborativo, em que pesquisadores, matemáticos, empresários, políticos e cientistas de diversas partes do mundo, em diferentes épocas, contribuíram para o avanço e desenvolvimento dessas tecnologias, aprimorando e aperfeiçoando invenções e criações pré-existentes.

Por essa razão, são inúmeras as histórias e nomes que contribuíram e participaram de alguma forma na idealização e construção do computador e da internet, tão numerosos que seria necessário um trabalho à parte para explorá-los como um todo. Portanto, para confirmar e exemplificar essa afirmação, bem como explicitar as afirmações elencadas anteriormente, exploraremos apenas algumas dessas histórias, com foco no surgimento do computador, visto que o engendramento dessa máquina está diretamente relacionado ao da internet.

O primeiro idealizador de um dispositivo que poderia ser considerado um computador, ao que se tem registro, é o matemático e pioneiro da ciência da computação Charles Babbage, que projetou a Máquina Analítica, um protótipo de computador que incorporava uma unidade lógica aritmética capaz de realizar cálculos complexos, basicamente uma “super calculadora gigante mecânica”.

Babbage, junto de Ada Lovelace, realizaram conjecturas de uma máquina que se aproxima muito do conceito de um computador moderno, mas nunca puderam transpor todas essas ideias para fora do papel e confeccionar essa máquina em razão da limitação tecnológica do século XIX, pois como o ex-diretor da Apple afirma em sua obra: “Babbage nomeou essa máquina proposta de *Analytical Engine*. Ele estava cem anos à frente de seu tempo.” (ISAACSON, 2014, p. 23, tradução nossa).[1]

Depois de Babbage e Ada Lovelace, vários outros pesquisadores e estudiosos, como Henry Prevost Babbage, Georg Scheutz, Edvard Scheutz, Howard Hathaway Aiken, Grace Hopper, entre outros (DEMENTSHUK; HENRIQUES, 2019, p. 30 e 39-41), criaram outros modelos e tipos de aparelhos, trabalhando e desenvolvendo essa ideia de uma máquina que poderia fazer cálculos, ler e armazenar informações. Uma dessas invenções que explorou melhor essa característica, foi a “máquina tabuladora”, criada por Herman Hollerith e patenteada em 1884, considerada como um dos primeiros aplicativos de informática da história.

A máquina “lia” cartões de papel perfurados e aplicava uma lógica parecida com a do BCD (*Binary Coded Decimal*, ou código binário), efetuando dessa maneira a contagem da informação referente à perfuração, a qual era utilizada para a coleta de dados, principalmente para a leitura de censos (DEMENTSHUK; HENRIQUES, 2019, p. 32), sendo utilizada amplamente nos Estados Unidos para a realização do censo do país no ano de 1890, além de também ter sido muito bem explorada pelo exército Alemão, que obtinha com a ajuda da máquina, informações com riquezas de detalhes sobre o nome, moradia, amizades, locais frequentados, relacionamentos dentre outras informações de toda a população civil da Alemanha. Nesse sentido:

[1] “Babbage named this proposed machine the Analytical Engine. He was one hundred years ahead of his time”

> Um dos primeiros atos de Adolf Hitler ao ser nomeado chanceler da Alemanha, em janeiro de 1933, foi realizar um censo da população. A tecnologia mais eficaz para essa tarefa eram as máquinas Hollerith da IBM. [...] O autor do livro IBM e o Holocausto, Edwin Black, chama a atenção para a extrema habilidade do exército alemão em saber, com riqueza de detalhes, quem era, onde morava e a qual grupo pertencia a pessoa fadada a ser exterminada entre a população civil. As informações vinham das máquinas de Hollerith. (DEMENTSHUK; HENRIQUES, 2019, p. 34)

Após, na década de 1940, o inventor, engenheiro e político estadunidense Vannevar Bush, ao perceber a crescente exponencial da população e o montante de informação que seria produzido por ela, começou a preocupar-se com o armazenamento de todo esse conteúdo, o que o levou a idealizar um equipamento que seria capaz de coletar todo esse conhecimento e armazená-lo, mas que também permitisse que qualquer indivíduo tivesse acesso a essas informações quando necessário.

Nesse ínterim, Bush em 1945 publicou sua ideia em um artigo na revista *The Atlantic Monthly*, dando o nome à sua invenção de *Memex* (*Memory Extension*), o que trazia a ideia de uma espécie de extensão da mente humana. Infelizmente a máquina idealizada por Bush nunca veio a existir, porém inspirou diversas outras criações, dentre elas a da própria internet. Acerca da história do Memex, compila Walter Isaacson**:**

> Ele escreveu um ensaio para a edição de julho de 1945 da revista Atlantic intitulado "As We May Think" ("Como Podemos Pensar"). Nele, ele evocou a possibilidade de uma máquina pessoal, que ele chamou de memex, que armazenaria e recuperaria palavras, imagens e outras informações de uma pessoa: "Considere um dispositivo futuro para uso individual, que seja uma espécie de arquivo e biblioteca privada mecanizada... Um memex é um dispositivo no qual um indivíduo armazena todos os seus livros, registros e comunicações, e que é mecanizado de forma que possa ser consultado com extrema rapidez e flexibilidade. É um suplemento íntimo ampliado à sua memória." (ISAACSON, 2014, p. 263, tradução nossa)[2]

Mesmo que Bush não tenha conseguido dar continuidade à sua ideia e construir a máquina *Memex*, ainda assim, foi de extrema importância para o

[2] "he wrote an essay for the July 1945 issue of the Atlantic titlet "As We May Think." In it he conjured up the possibility of a personals machine, which he dubbed a memex, that would store and retrieve a person's words, pictures, and Other information: "Consider a future device for individual use, which is a sorto f mecanize private file and library.... A memex is a device in which an individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility. It is an enlarged intimate supplement to his memory"

desenvolvimento e criação de outras invenções, sendo um dos principais indivíduos a direcionar o governo americano a investir e desenvolver a área de pesquisas científicas, beneficiando diretamente a próxima geração de cientistas e pesquisadores.

Outros projetos que também merecem ser destacados, são o ENIAC (*Eletronic Numerical Integrator and Computer*) que foi o primeiro computador digital eletrônico de grande escala da história, e seu sucessor, o EDVAC (*Eletronic Discrete Variable Automatic Computer*), um dos primeiros computadores eletrônicos da história.[3]

O computador ENIAC começou a ser desenvolvido em meio à Segunda Grande Guerra Mundial, em meados de 1943 (mas somente foi concluído e tornou-se operacional após o grande conflito), sob influência e interesse quase que exclusivamente militar, sob o codinome “projeto PX”, e tinha como objetivo principal, computar trajetórias e dados balísticos de artilharia por meio de cálculos realizados em grande velocidade, por meio de uma codificação decimal e reaproveitando a tecnologia de leitura à base dos cartões perfurados[4] (a mesma tecnologia idealizada por Babbage).

Já o projeto EDVAC, foi uma “evolução tecnológica” do computador ENIAC, e diferentemente deste último, foi projetado para se utilizar de códigos binários e superar a capacidade de armazenamento de memória de seu predecessor, além de ter uma arquitetura considerada revolucionária, que veio a ser padronizada para os futuros modelos de computadores.

Foi nessa época também, durante e após a segunda grande guerra mundial, que os militares deram o pontapé inicial para o efetivo surgimento da internet, tendo-se em vista que se conjecturavam meios de se resguardar e proteger dados e informações sensíveis dessa categoria, ou seja, a ideia inicial de internet surgiu com a finalidade de servir como uma espécie de back up (cópia de segurança de dados digitais) de dados de bases militares.

Para ilustrar isso, podemos destacar nos Estados Unidos da América, a atuação da organização militar de defesa americana ARPA (Advanced Research Projects Agency), que a fim de investir na interligação dos departamentos de

[3] Para confirmar, ver ISAACSON (2014, p. 72-75 e 108-116)
[4] Para confirmar, ver DEMENTSHUK (2019, p. 34)

pesquisa dos Estados Unidos e na transmissão de dados militares sigilosos como forma de defesa militar e informacional contra-ataques nucleares, financiou pesquisas para a expansão dessa rede de comunicação. Ainda que o primeiro passo para o surgimento do ciberespaço tenha sido por meio da iniciativa militar, foi somente no contexto acadêmico que ele se disseminou.

No decorrer do desenvolvimento dos mais diversos aparatos e tecnologias que foram sendo aprimorados ao longo das décadas, apenas em 1950 que os “computadores”, ou melhor dizendo, as máquinas de cálculos utilizadas até então, foram “aprimoradas” com o objetivo de suprir as necessidades de cientistas, engenheiros e principalmente de bibliotecários e acadêmicos, deixando cada vez menos as características de máquina de cálculos, e se aproximando mais de um tipo de máquina de processamento e armazenamento de dados e informações.[5]

De maneira crescente, atendendo as demandas dessa classe, o computador emergiu como uma ferramenta com potencial para solucionar uma problemática despontante, a necessidade de não só armazenar uma quantidade inacreditável de informação, mas também da comunicação e escambo informacional em grandes volumes – o que até então os meios de comunicação da época, como telégrafo, rádio ou até mesmo o telefone, não eram capazes de fazer em razão do grande volume de dados -, surgindo a demanda latente de se criar uma interconexão entre as diversas universidades e centros de pesquisas espalhados pelo mundo, o que culminará no desenvolvimento e elaboração do que chamamos de *world wide web*[6].

Assim, a internet se desenvolveu em virtude da criação do computador, mas mais importante que isso, se desenvolveu de forma semelhante a ele, herdando características e funções de outras tecnologias predecessoras, que foram desenvolvidas paralelamente por diferentes grupos de indivíduos alocados em diferentes partes do mundo, com a majoritária diferença de que o ciberespaço tomou forma com a interconexão de distintas redes e ligamentos

[5] Para confirmar, ver DEMENTSHUK (2019, p. 45)
[6] PHOENIXNAP. Definição de rede mundial. PhoenixNAP Glossário, 2024. Disponível em: https://www.phoenixnap.pt/gloss%C3%A1rio/defini%C3%A7%C3%A3o-de-rede-mundial. Acesso em: 23 out. 2024.

entre computadores e servidores alocados em diversas universidades de vários países.

Inicialmente foi criado o sistema *host-to-host*, que de forma simplificada, é a conexão direta entre dois sistemas informacionais ou computadores, isto é, os centros acadêmicos foram interligados através de fios, permitindo a transmissão de dados de uma universidade para outra.

Posteriormente, além da conexão por cabeamento (ARPAnet), advieram outros meios de conectar e interligar esses centros de pesquisas e universidades, como a ligação por meio de satélite (SATnet), por rádio (PRnet) e muitos outros meios. E com o tempo foram criados meios de convergir todas essas redes em um único grande emaranhado de conexões e nós (DEMENTSHUK; HENRIQUES, 2019, p. 109-112).

Destarte, com a evolução tecnológica cada vez mais pungente, logo tornou-se viável a utilização do computador e consequentemente da internet, não somente em meio acadêmico e militar, mas também em outros setores da sociedade, estendendo seu uso para o meio empresarial e diversos setores governamentais.

Mas foi somente a partir de meados dos anos 1980 que a disseminação dos computadores pessoais e o subsequente barateamento das tecnologias de comunicação, propiciou a disseminação da internet para o público em geral, fator este que impulsionou e expandiu o ambiente virtual de forma completamente descontrolada e imprevisível, fazendo com que a internet deixasse de ser apenas uma ferramenta de especialistas e estudiosos, para se tornar parte do cotidiano de milhões de pessoas ao redor do mundo, democratizando o acesso à informação e transformando profundamente a sociedade. Afirmando o que fora dito, temos:

> De 1982 em diante o que se viu foi uma expansão exuberante, que se inicia na área acadêmica, mas em pouco tempo atingiu a sociedade como um todo, ajudada pela rápida disseminação de computadores pessoais e pela evolução da tecnologia em Informática e em Comunicações, acompanhadas da correspondente queda nos preços de equipamentos e infraestrutura. (...) A partir de 1993, com a chegada da *Web*, a rede passou a atrair novos integrantes, aos milhões. Com a *Web* servindo de plataforma para que todos pudessem publicar conteúdos e com o advento das redes sociais, levas e levas de novos usuários, provenientes de qualquer local e das mais diferentes culturas, popularam a Internet. (DEMENTSHUK; HENRIQUES, 2019, p. 12)

Acontece que essa expansão foi demasiadamente acelerada e descontrolada, visto que os próprios usuários passaram a expandir a rede e aprimorá-la por meio de sistemas operacionais abertos e gratuitos, fazendo com que surgissem novas funcionalidades e usos para o espaço cibernético. Mas podemos dizer que foi com o advento das redes sociais que a internet se tornou avassaladora e presente no cotidiano de todos como o é atualmente.

O primeiro computador pessoal, o Apple I, foi criado em 1976[7] e o Facebook, uma das primeiras e mais notórias redes sociais, começou a operar oficialmente em 2004[8], um lapso temporal, respectivamente, de apenas 48 e 20 anos da elaboração do presente trabalho.

É fato que a internet é uma tecnologia nova, que se desenvolveu de forma extremamente acelerada e descontrolada, não só isso, mas também se desenvolveu de forma muito distante da idealizada inicialmente, portanto, a utilização dessa ferramenta e o ambiente em si, se transfiguraram completamente, o que antes era um ambiente dominado por pesquisadores e intelectuais, tornou-se acessível a milhões de pessoas que naturalmente não têm o preparo necessário para lidar com essa ferramenta e estilo de vida criado a partir do ciberespaço, completamente experimentais e inovadores.

Naturalmente, com a expansão e disseminação para o grande público, eclodiram diversos meios para usurpação de dados dos usuários e cometimento de crimes nesse novo ambiente que chamamos de ciberespaço.

[7] https://olhardigital.com.br/2021/04/11/reviews/apple-1-o-primeiro-produto-da-historia-da-apple-computers-faz-45-anos/

[8] https://www.techtudo.com.br/noticias/2024/02/20-anos-de-facebook-relembre-a-trajetoria-da-rede-social-de-mark-zuckerberg-edsoftwares.ghtml

1.2 Definição de Crimes Digitais

Da mesma forma que a internet e os computadores se tornaram ferramentas indispensáveis e amplamente disseminadas no cotidiano da sociedade global, não demorou para que surgissem meios escusos e ilícitos de utilização dessas tecnologias.

Embora seja difícil determinar com precisão o momento e o local exatos em que ocorreu o primeiro delito cibernético, há relatos curiosos que remontam a incidentes iniciais. Um dos mais conhecidos — ainda que envolto em caráter anedótico — sugere que o primeiro crime cibernético registrado teria sido cometido por um jovem que, ao invadir o sistema da Universidade de Oxford, teria invadido o banco de dados da instituição para buscar uma prova que estaria armazenada no depositório de dados. Acerca do caso destaca-se:

> o primeiro caso de que se tem notícia sobre hacking no ano de 1978, na Universidade de Oxford, onde um estudante copiou de uma rede de computadores uma prova. Uma invasão seguida de uma cópia. Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. A Flórida, no mesmo ano, foi o primeiro Estado americano a formular leis sobre informática. (JESUS; MILAGRE, 2016, p. 09).

Este caso, verdadeiro ou não, simboliza o surgimento de uma nova era, na qual a manipulação indevida de sistemas informatizados passou a ser uma ameaça crescente e um desafio para as autoridades e legisladores, surgindo, dessa maneira, os crimes cibernéticos.

Crimes cibernéticos, nada mais são que condutas ilícitas praticadas no ambiente digital, utilizando-se de dispositivos eletrônicos, redes de computadores ou a internet, com o intuito de violar bens jurídicos protegidos pelo Direito. Esses delitos abrangem uma vasta gama de práticas, desde fraudes e roubos digitais até a invasão de privacidade e o ataque a sistemas de dados.

Tais crimes, não se limitam ao prejuízo patrimonial, mas principalmente, atingem bens jurídicos imateriais, como a privacidade, a honra e a segurança de informações pessoais.

Assim, podemos traçar o conceito de crimes digitais conforme àquele trazido pelos professores Damásio e José Antônio:

> Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um

> ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal. (JESUS; MILAGRE, 2016, p. 20).

A tipificação e a regulamentação dos crimes cibernéticos, em razão de seu surgimento relativamente recente, ainda constituem um campo embrionário e em constante desenvolvimento.

No Brasil, mesmo que a confecção de uma legislação específica tenha se dado de forma tardia, a discussão sobre a necessidade de sua criação, já é relativamente antiga, visto que o Brasil desde os anos 2000, sempre esteve como um dos países que mais enviam spam na história[9], principalmente em razão da lacuna legislativa e da pouca fiscalização do país acerca dessa prática.

Salienta-se, em apertada síntese, que a prática do spam, consiste no envio massivo e não solicitado de mensagens, geralmente de natureza comercial, para uma grande quantidade de destinatários.[10] Ocorre que muitas vezes a mensagem que é considerada como inofensiva, pode carregar consigo um vírus ou *malware* malicioso com a capacidade de infectar, invadir e danificar o computador do destinatário do spam ou até mesmo usurpar seus dados, portanto, o spam pode servir como veículo para ataques cibernéticos.

Não obstante, muitos países ao longo das décadas, se utilizaram da lacuna legislativa e da falta de fiscalização existente em território tupiniquim, para utilizar os computadores brasileiros como servidores de envio de spam, o que potencializou tal prática em território nacional. Nesse sentido:

> As mensagens saíam de outros países e usavam computadores no Brasil de forma a burlar a origem (...) A partir do ano 2000, havia, no Brasil, uma banda larga razoável e nenhum controle técnico de segurança sobre os serviços de envio de e-mails partindo dos usuários nas suas casas. **Os spammers se aproveitavam dessas condições e usavam os computadores de internautas brasileiros como "servidores de e-mail"**. (DEMENTSHUK; HENRIQUES, 2019, p. 550-551)

---

[9] KASPERSKY LAB. Kaspersky Lab revela que Brasil é o décimo país que mais envia *spam* no mundo. *Kaspersky Lab*, 28 jul. 2017. Disponível em: https://www.kaspersky.com.br/about/press-releases/kaspersky-lab-revela-que-brasil-e-o-decimo-pais-que-mais-envia-spam-no-mundo. Acesso em: 23 set. 2024.

[10] TRIBUNAL DE JUSTIÇA DE SANTA CATARINA. Saiba identificar uma mensagem eletrônica indesejada. *TJSC*, 2024. Disponível em: https://www.tjsc.jus.br/*web*/servidor/dicas-de-ti/-/asset_publisher/0rjJEBzj2Oes/content/saiba-identificar-uma-mensagem-eletronica-indesejada#:~:text=Spam%20%C3%A9%20o%20termo%20usado,remetente%20na%20lista%20de%20destinat%C3%A1rios. Acesso em: 23 set. 2024.

Nesse ínterim, visto que o Brasil sempre esteve grandemente vinculado a esse tipo de prática, já existiam discussões acerca da necessidade de elaboração de uma legislação específica para crimes informáticos, bem como a regulamentação das redes.

Ocorre que a efetiva criação de uma legislação específica para tratar sobre os possíveis crimes cometidos nesse ambiente, só se concretizou após dois episódios de grande repercussão nacional: (i) o primeiro, diz respeito a ataques hackers perpetrados contra *site*s relacionados ao governo e à políticos brasileiros[11], e (ii) o segundo, envolve a extorsão e exposição de uma celebridade após ela ter sido vítima de uma mensagem spam.

O primeiro incidente está diretamente relacionado ao grupo ativista hacker de nome LulzSec[12], responsável por ataques em massa contra *website*s do governo federal brasileiro. Utilizando bots (robôs), os hackers promoveram acessos massivos e repetitivos a esses *website*s, o que resultou na sobrecarga dos servidores e na queda temporária das páginas de internet.

Mesmo que o grupo não tenha obtido sucesso em invadir, usurpar ou corromper o banco de dados de nenhuma instituição ou político que fora alvo dos ataques, ainda assim, o ocorrido causou estardalhaço suficiente para alertar as autoridades e políticos brasileiros, o que reavivou o projeto que já tramitava a mais de 11 anos no Congresso Nacional, o famigerado AI-5 digital ou Projeto de Lei n. 84/1999.[13]

O supracitado projeto foi uma das primeiras tentativas de regulamentar o uso da internet no Brasil e de criar um tipo penal capaz de criminalizar condutas relacionadas a fraudes, invasão de dispositivos informáticos, disseminação de vírus, entre outras práticas escusas que vinham se disseminando no meio digital.

Ocorre que o projeto encontrou forte resistência e rejeição por parte da sociedade, em razão do medo de uma possível regulamentação excessiva ou

---

[11] EXTRA. Hackers atacam *site*s da Presidência, do governo brasileiro e da Petrobras. *Extra*, 23 jun. 2011. Disponível em: https://extra.globo.com/noticias/celular-e-tecnologia/hackers-atacam-*site*s-da-presidencia-do-governo-brasileiro-da-petrobras-2089754.html. Acesso em: 23 set. 2024.

[12] G1. Conheça o LulzSec, o grupo hacker que desafiou o governo dos EUA. *G1*, 27 jun. 2011. Disponível em: https://g1.globo.com/tecnologia/noticia/2011/06/conheca-o-lulzsec-o-grupo-hacker-que-desafiou-o-governo-dos-eua.html. Acesso em: 23 set. 2024.

[13] OBSERVATÓRIO DA IMPRENSA. O AI-5 digital. *Observatório da Imprensa*, 19 nov. 2019. Disponível em: https://www.observatoriodaimprensa.com.br/e-noticias/o-ai-5-digital/. Acesso em: 23 set. 2024.

até vigilantismo estatal das redes sociais, fazendo inclusive com que o projeto ganhasse a alcunha de AI-5 digital.

Não obstante, o incidente de ataque hacker causou tanto rebuliço, que após 11 anos, o projeto, em partes, deu origem à Lei n. 12.735/2012, a qual tinha como objetivo promover alterações no Código Penal e no Código Penal Militar, mas em razão dos diversos vetos realizados por parte do presidente da república, acabou por não acrescentar nenhum tipo penal, conforme lecionam os professores Damásio e José Antônio:

> A legislação, apesar de prever em seu preâmbulo que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, contra sistemas informatizados e similares, na verdade não acrescentou tipo penal algum ao ordenamento jurídico. (JESUS; MILAGRE, 2016, p. 31)

Já o segundo episódio de grande repercussão nacional, por outro lado, está relacionado à atriz Carolina Dieckmann, a qual teve sua conta de e-mail e, posteriormente, seus dispositivos eletrônicos comprometidos, após receber e clicar em um e-mail do tipo spam, e como veremos mais afrente, está diretamente relacionado à prática de *phishing*. Nesse diapasão:

> Outro caso que obteve grande repercussão na mídia brasileira foi a obtenção das fotos da atriz Carolina Dieckmann, situação que envolveu o uso de *phishing* por meio de spam e consequente inserção de um trojan no sistema informático da vítima. (D'AVILA; AMARAL, 2022, p. 39)

O spam continha um *link* que, ao ser acessado, permitiu a instalação de um *software* malicioso e nocivo em seu computador pessoal, possibilitando que os criminosos obtivessem acesso indevido a seus dados e informações pessoais que estavam armazenados tanto no e-mail comprometido, quanto no computador e demais dispositivos eletrônicos com acesso à internet e e-mail da atriz.

Os criminosos, localizaram algumas fotos sensuais da atriz que estavam armazenadas em seu computador e utilizaram essas fotos para extorquir e chantagear a atriz, exigindo o montante de R$ 10.000,00 para não divulgar as fotografias, além de terem vazado e publicado essas imagens em *site*s de conteúdo pornográfico de domínio de um dos próprios criminosos.[14]

[14] G1. Suspeitos do roubo das fotos de Carolina Dieckmann são descobertos. G1, 7 maio 2012. Disponível em: https://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html. Acesso em: 23 set. 2024.

Esse episódio, que ocorreu em meados de maio de 2012, gerou tanta repercussão midiática, que ensejou a finalização acelerada – para não dizer forçada e às pressas - do projeto de Lei n. 2.793/2011, o qual ainda estava sob análise à época, mas que apressadamente, em novembro de 2012, no período de apenas um ano, se transformou na Lei n. 12.737/2012, que ficou popularmente conhecida como “Lei Carolina Dieckmann”.

O diploma legal trouxe importantes mudanças ao Código Penal Brasileiro e inseriu novos tipos penais. Por meio do artigo 154-A, tipificou a conduta de invasão a dispositivos informáticos, estabelecendo sanções para quem, sem autorização ou com violação de mecanismos de segurança, acessar indevidamente dispositivos como computadores, tablets ou smartphones, com o objetivo de obter, adulterar ou destruir dados. E mediante o artigo 154-B, tratou do tipo de ação penal e da competência para o tipo penal introduzido pelo artigo anterior.

A inserção do artigo 154-A é uma marca importantíssima e uma vitória para o combate de crimes cibernéticos, mas ainda assim, o dispositivo, isoladamente, não tem a capacidade de agasalhar todos os ilícitos cometidos no ambiente virtual.

Ademais, ao nosso ver, o dispositivo já foi inserido no ordenamento jurídico com uma aparente falha – isso em vista de que não há uma legislação robusta que acabe abrangendo outras práticas e ilícitos possíveis no ambiente virtual -, na medida em que não há sanção para a instalação de qualquer vulnerabilidade ou programa malicioso no dispositivo informático de outrem, caso não haja efetivamente a violação de dados. A instalação de programas ou softwares maliciosos, é considerada como sendo mera preparação. Nesse sentido, assevera o professor Guilherme de Souza Nucci:

> Nota-se que a mera instalação de vulnerabilidade (ex.: softwares mal-intencionados, que permitem o acesso ao conteúdo do dispositivo informático tão logo seja conectado à rede) não causa a violação, mas é nitidamente o seu preparo. Optou o legislador por equiparar a preparação e a execução em igual quilate, para fins de criminalização. Assim, o autor pode apenas instalar vulnerabilidade o dispositivo informático para que, no futuro, outrem dele se valha, como também pode, ele mesmo, utilizar o mecanismo de espionagem para a violação de dados e informes. Se o mesmo agente instalar a vulnerabilidade e, depois, invadir o dispositivo informático cometerá um só crime. (NUCCI, 2023, p. 635-636)

A Lei n. 12.737/2012, também inseriu no artigo 266 do Código Penal dois novos parágrafos, o §1º e o §2º. Esses parágrafos tratam especificamente de crimes que envolvem a interrupção ou a tentativa de impedir que um serviço de comunicação digital (como internet, sistemas de telecomunicação ou outros serviços online), seja restabelecido, bem como qualquer informação de utilidade pública que esteja sendo transmitida.

Essencialmente, a lei passou a prever punição não só para quem interrompe serviços essenciais, como os de telefonia ou internet, mas também para quem tenta atrapalhar ou retardar o processo de restabelecimento desses serviços. Nesse sentido, podemos verificar na confecção dessas alterações, claro reflexo e influência dos supramencionados ataques hackers perpetrados contra *site*s governamentais.

Por fim, a Lei Carolina Dieckmann, também trouxe alterações quanto ao artigo 298 do Código Penal, criando no parágrafo único, equiparação de cartão de crédito ou débito, a documento particular, na falsificação desse documento.

É necessário salientar que a importância da Lei n. 12.737/2012, não se restringe ao seu pioneirismo no âmbito digital-criminal, mas também à sua capacidade de inaugurar um novo paradigma no combate aos crimes cibernéticos no Brasil.

O diploma legal abriu caminho para o reconhecimento da vulnerabilidade dos dispositivos eletrônicos e da necessidade de proteção jurídica específica para dados e informações armazenadas ou transmitidas por esses meios. Além disso, sinalizou a relevância da preservação e proteção da privacidade digital, tema que será melhor discutido posteriormente por meio do Marco Civil da Internet (Lei n. 12.965/2014) e da Lei Geral de Proteção de Dados (Lei n. 13.709/2018).

Em apertada síntese, o Marco Civil da Internet visou estabelecer diretrizes fundamentais para o uso da internet no país, buscando garantir direitos básicos dos usuários, regular a atuação dos provedores de serviços e proteger o ambiente digital como um espaço democrático e seguro, ampliando diversos direitos e garantias fundamentais, já abarcados pela Constituição Federal, ao ambiente digital. Por essa razão, ficou popularmente conhecido como a “Constituição da Internet”.

Salienta-se, que para fins criminais e de investigação dos delitos digitais, o Marco Civil da internet é relevante, na medida em que estabeleceu normas claras para o armazenamento de registros de acesso a aplicações e serviços de internet, além de definir a responsabilidade dos provedores em relação à disponibilização desses dados.

Antes da promulgação da Lei nº 12.965/2014, não havia uma regulamentação tão precisa sobre como os dados de conexão e de navegação dos usuários deveriam ser armazenados e fornecidos às autoridades.

Já a Lei Geral de Proteção de Dados (LGPD), garante a proteção dos dados pessoais dos usuários de internet, protegendo sua privacidade e garantindo a transparência no tratamento dos dados. O instrumento normativo regulamentou a coleta, armazenamento e uso de dados dos usuários por empresas e provedores de internet.

Assim, por mais que a LGPD não trate diretamente acerca dos crimes cibernéticos, ela auxilia a dirimir e evitar muitos dos ilícitos cometidos em meio digital, pois, como veremos mais à frente no presente trabalho, muitas das técnicas escusas para o cometimento de ilícitos, incluindo-se a prática do *phishing*, utilizam-se de dados e informações sensíveis dos usuários que são coletadas de forma irregular ou até mesmo regular no ambiente digital e são utilizadas para fins escusos.

Oportuno também mencionar acerca da Lei n. 13.441/2017, criada com o objetivo de aprimorar os mecanismos de combate aos crimes de exploração sexual infantil, incluindo a inserção do agente infiltrado virtual no Código de Processo Penal Brasileiro. Assim, permite que, mediante autorização judicial, agentes policiais se infiltrem em redes de comunicação pela internet com o intuito de investigar e identificar criminosos que praticam crimes de abuso e exploração sexual de crianças e adolescentes.

E ainda sobre a Lei n. 14.155/2021, que alterou dispositivos do Código Penal, para melhor adequá-los à realidade digital, agravando as penas dos crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet.

Dessa forma, como verificamos, o Brasil ainda carece de uma legislação penal específica para tratar exclusivamente sobre crimes cibernéticos, ou melhor dizendo, há uma lacuna legislativa, mais especificamente quando tratamos sobre

“crimes informáticos próprios” – assim classificado pela doutrina -, que são basicamente crimes “em que o bem jurídico ofendido é a tecnologia da informação em si” (JESUS; MILAGRE, 2016, p. 22), ou seja, são aqueles que só podem ser cometidos no ambiente digital, como a invasão de computadores (art. 154-A do CP) ou os ataques de negação de serviço (§ 1º do art. 266 do CP).

Até recentemente, o legislador brasileiro não demonstrou preocupação em criar uma tipificação específica para cada delito informático. Isso se deve, em grande parte, ao fato de que muitos crimes cometidos por meio da internet já são abarcados por condutas tipificadas no Código Penal.

Em diversas situações, a internet é utilizada apenas como um meio para a prática do crime, sendo que o delito em si já está previsto e contemplado pela legislação vigente. Assim, esse tipo de crime informático, é classificado pela doutrina como “crime informático impróprio”, que nas palavras do professor Damásio, são crimes “em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro” (JESUS; MILAGRE, 2016, p. 22).

Salienta-se também a classificação dos “crimes informáticos mistos”, que são:

> (...) crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico (JESUS; MILAGRE, 2016, p. 22).

Muitos defendem a ideia de que é possível continuar se utilizando dos delitos já existentes no Decreto-Lei n. 2.848/1940, não havendo necessidade de uma legislação própria para crimes cibernéticos.

No entanto, considerando as diversas práticas ilícitas que envolvem condutas reprováveis que visam a deterioração e a destruição não só do patrimônio alheio, mas também à ofensa de outros bens jurídicos, como a intimidade e a privacidade, é evidente que há lacunas a serem preenchidas. Nesse sentido:

> Como sabemos, a informática trouxe em seu bojo novas formas de realizar velhos crimes. Ameaça será sempre ameaça, difamação sempre será difamação, estelionato sempre será estelionato, não importando se praticados por intermédio do computador ou não. Sob outro aspecto, também é inegável que crimes informáticos puros hoje atentam contra bens jurídicos não protegidos pelo Direito Penal. A necessidade de enquadramento penal sempre foi debatida entre operadores do Direito

> Penal, especificamente se devemos conceber leis específicas ou adaptarmos a legislação vigente. (JESUS; MILAGRE, 2016, p. 25).

Assim sendo, em casos específicos como o de spam ou *phishing*, observa-se a inadequação da aplicação de outros tipos penais que não se ajustam plenamente a essas práticas, o que configura o uso, da analogia in malam partem, em razão da lacuna legislativa existente. Para alinhar uma determinada conduta ilícita a um tipo penal, a tática utilizada por promotores e outros operadores do direito tem sido a aplicação da analogia, visando adequar a conduta a determinado tipo penal pré-existente no ordenamento jurídico. Nessa linha:

> Em que pese existirem tipos penais que possam criminalizar aquele que adultera ou destrói dados informatizados (art. 163 do Código Penal), ou mesmo aquele que copia ou move indevidamente informações (art. 155 do Código Penal) é inegável que tais “enquadramentos forçosos” sempre foram objeto de muitos e acalorados debates sob o prisma da “analogia in malan partem” e do princípio da reserva legal. (JESUS; MILAGRE, 2016, p. 35).

Ocorre que tal prática, em muitos dos casos, vai de encontro com os princípios da legalidade estrita e da reserva legal e pode gerar graves implicações para os direitos e garantias fundamentais. O princípio da legalidade estrita, consagrado no artigo 5º, inciso XXXIX, da Constituição Federal, estabelece que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", ou seja, uma conduta só pode ser punida se previamente tipificada por lei. Da mesma forma, a reserva legal impede a criação de crimes ou penas por meio de analogia ou interpretação extensiva em desfavor do réu (in malam partem).

Assim, a aplicação da analogia in malam partem, nesses casos, fere a segurança jurídica e a previsibilidade, alicerces fundamentais do Direito Penal.

Deste modo, torna-se evidente a necessidade de criação e implementação de uma tipificação específica para ilícitos como a prática de *phishing*.

1.3 *Phishing*

Até o presente momento, mencionamos o *phishing* como uma prática ilícita, com o intuito criminoso de obter e surrupiar dados pessoais e sensíveis de usuários da internet, por meio de técnicas que enganam as vítimas e as induzem ao erro. Agora, nos aprofundaremos na análise de tal prática, melhor entendendo seu conceito e funcionamento.

A origem do termo, deriva da palavra de língua inglesa "fishing" (pescar), fazendo alusão à ideia de "lançar uma isca" na esperança de que a vítima "morda" e forneça acesso às informações desejadas pelo criminoso. Sobre a origem do termo, destacamos a colocação da professora Patrícia Peck Pinheiro:

> Traduzido livremente como “pescaria” ou “golpe de pescaria”, consiste em uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um *link* falso, acesse uma página falsa ou execute algum arquivo para que haja furto de dados, ou acesso e elevação de privilégios. É uma técnica de engenharia social (PINHEIRO, 2024, p. 15)

Também nos utilizaremos do que é lecionado no Roteiro de Atuação de Crimes Cibernéticos do Ministério Público Federal:

> A palavra "*phishing*" é uma variação de fishing (“pescaria”) e seu uso foi registrado pela primeira vez em 1996, provavelmente influenciado pelo termo “phreaking”. Neste tipo ação, são enviadas “iscas” (e-mails), que tentam se passar por instituições reputadas com o intuito de “pescar” senhas ou outras informações sensíveis de Internautas. (BRASIL, 2016, p. 204)

Da mesma forma como na pesca tradicional, os cibercriminosos colocam várias “iscas” e aguardam que uma ou várias vítimas “caiam na armadilha”, permitindo, assim, o acesso não autorizado a informações sigilosas e pessoais - como nome de usuário, senhas, número de documentos pessoais, detalhes do cartão de crédito, dados bancários, entre outros -, ou, até mesmo, o acesso remoto aos dispositivos pessoais das vítimas.

Portanto, o *phishing* não é apenas uma técnica escusa e fraudulenta de cometimento de ilícitos que depende exclusivamente de falhas técnicas para seu sucesso. O *phishing* é, essencialmente, uma técnica de engenharia social, que lida principalmente com a exploração da vulnerabilidade humana.

Na prática, os criminosos se passam por indivíduos ou entidades confiáveis – como bancos, operadoras de créditos, empresas multinacionais, instituições governamentais ou até mesmo por pessoas físicas conhecidas ou

desconhecidas pela vítima - e utilizam mensagens ou *website*s aparentemente legítimos para induzir o usuário a fornecer voluntariamente suas informações.

Esse processo de manipulação explora a confiança natural que o indivíduo deposita em entidades ou contatos que parecem legítimos, o que torna o *phishing* uma das formas mais insidiosas e perigosas de crime cibernético, visto que atua diretamente sobre a confiança e explora o erro humano.

Neste contexto, é relevante abordar o conceito de engenharia social apresentado pela professora Patrícia Peck Pinheiro, que define essa prática como:

> [...] um conjunto de práticas e ações aplicadas na busca de informações sigilosas ou de grande importância e valor, pertencentes a uma pessoa ou a uma empresa, de maneira que essas práticas utilizam a manipulação, a persuasão e a influência sobre o comportamento humano como estratégia de ataque. (...) Como se pode notar, a engenharia social é um mecanismo adotado pelos invasores que buscam a obtenção de informações protegidas mediante desenvolvimento e aplicação de estratégias para corromper o comportamento humano. (PINHEIRO, 2024, p. 96).

Portanto, a engenharia social, e consequentemente o *phishing*, baseia-se em explorações psicológicas, tirando proveito de elementos como curiosidade, medo, urgência e autoridade, para induzir as vítimas ao erro.

Essa técnica de manipulação psicológica pode ser executada de diversas maneiras e por diferentes meios, ajustando-se ao perfil da vítima e à forma de comunicação utilizada, explorando tanto vulnerabilidades técnicas quanto comportamentais.

Nesse sentido, o *phishing* é altamente versátil e adaptável, possuindo diferentes tipos e variações conforme a forma e o meio pelo qual é perpetrado. Os ataques podem ocorrer por e-mail (*Phishing* Scam), mensagens de texto (Smishing), chamadas telefônicas (Vishing), por *Pop-ups* de propaganda em *website*s (*Pop-up phishing*), entre muitos outros meios e formas[15]. Além disso, podem ser massificados (*Phishing* tradicional e Pharming), com o objetivo de atingir um grande número de pessoas simultaneamente, ou altamente

[15] NORTON. Types of *phishing*. *Norton*, 2024. Disponível em: https://us.norton.com/blog/online-scams/types-of-*phishing*. Acesso em: 15 out. 2024.

personalizados, focando em um grupo ou indivíduo específico (Spear *phishing* e Whaling).[16]

Assim, a depender das características e complexidade empregados na prática do *phishing*, será utilizada uma nomenclatura para distinguir as diferentes técnicas e formas dessa prática. No presente trabalho, vamos focar na generalidade, abordando principalmente o *phishing* scam ou *phishing* tradicional.

O referido termo é utilizado comumente para se referir à prática de *phishing* como um todo, mas também pode se referir especificamente à prática de "pescaria" massificada, sem objetivar uma vítima ou alvo específico. O termo também é comumente associado ao envio de spam por meio de correio eletrônico, ou e-mail, que é o canal mais simples e amplamente utilizado para a execução dessa prática fraudulenta.

Para exemplificar, consideremos o caso do e-mail: o criminoso envia mensagens fraudulentas que imitam comunicações legítimas de empresas conhecidas, como bancos, redes sociais ou provedores de serviços. Esses e-mails geralmente contêm *links* ou anexos maliciosos, que, quando clicados, redirecionam a vítima para um *site* falso ou instalam *malwares* em seu dispositivo eletrônico, comprometendo sua segurança.

Da mesma forma, esse tipo de ataque também ocorre por outros métodos, como por meio de propagandas e *pop-ups* que aparecem como falsos avisos de segurança ou ofertas comerciais enquanto o usuário navega na internet. Esses pop-ups, propagandas, *links* e avisos podem parecer legítimos, mas ao clicar, a vítima pode permitir a instalação de vírus ou outros programas maliciosos, ou ainda ser redirecionada para versões falsas de *site*s, onde será induzida a fornecer informações pessoais e sensíveis.

---

[16] BLOCKBIT. Fique alerta para os tipos comuns de *phishing*. *Blockbit Blog*, 2023. Disponível em: https://www.blockbit.com/pt/blog/fique-alerta-para-os-tipos-comuns-de-*phishing*/. Acesso em: 23 set. 2024
TREND MICRO. Tipos de *phishing*. *Trend Micro*, 2024. Disponível em: https://www.trendmicro.com/pt_br/what-is/*phishing*/types-of-*phishing*.html. Acesso em: 23 set. 2024.
AFFINITY TECH PARTNERS. Scam alert: what you need to know about pop-up *phishing*. *Affinity Tech Partners*, 3 maio 2018. Disponível em: https://www.affinitytechpartners.com/3n1blog/2018/5/3/scam-alert-what-you-need-to-know-about-pop-up-*phishing*#:~:text=What%20is%20Pop%2DUp%20*Phishing*,as%20the%20following%20example%20illustrates. Acesso em: 23 set. 2024.

Trazendo o exemplo de um caso concreto, podemos citar o supramencionado caso da atriz Carolina Dieckmann, que foi vítima de *phishing*, por meio de um e-mail spam. A atriz recebeu em seu correio eletrônico uma mensagem que continha um *link* malicioso, que ao ser clicado, instalou no computador da atriz um *Malware* do tipo cavalo de troia, que permitiu aos hackers, acesso ao computador da atriz.[17]

Outro caso, mais recente e de grande notoriedade, refere-se à decisão do Ministro do Supremo Tribunal Federal, Alexandre de Moraes, que suspendeu a operabilidade da plataforma "X". Em sua decisão, o magistrado do Supremo Tribunal Federal impôs uma multa diária aos cidadãos que acessassem a plataforma da rede social "X", visando coibir o uso da rede durante o período de bloqueio. Aproveitando-se dessa situação, muitos criminosos utilizaram essa medida como oportunidade para aplicar golpes, enviando mensagens fraudulentas por e-mail (*phishing* scam) ou SMS (smishing), cobrando indevidamente o valor da multa imposta.[18]

Esses casos, assim como todo o contexto apresentado, ressaltam a facilidade com que o *phishing* pode ser empregado por criminosos. Não é por acaso que tal prática se consolidou como uma das formas mais comuns e disseminadas de crimes cibernéticos, registrando um aumento significativo nos últimos anos.[19]

No Brasil, por exemplo, o número de ataques cresceu mais de cinco vezes no último ano, evidenciando a gravidade do problema. De acordo com um relatório da Kaspersky[20], em 2023, foram bloqueadas mais de 286 milhões de tentativas de *phishing*, o que equivale a uma média impressionante de 544

---

[17] O GLOBO. Especialistas explicam como computador de Carolina Dieckmann foi hackeado. *O Globo*, 13 maio 2012. Disponível em: https://oglobo.globo.com/rio/especialistas-explicam-como-computador-de-carolina-dieckmann-foi-hackeado-4895771. Acesso em: 23 out. 2024.

[18] G1. Anatel diz que são golpe e-mails falsos notificando de multas por acesso ao X por VPN. *G1*, 4 set. 2024. Disponível em: https://g1.globo.com/politica/noticia/2024/09/04/anatel-diz-que-sao-golpe-e-mails-falsos-notificando-de-multas-por-acesso-ao-x-por-vpn.ghtml. Acesso em: 05 out. 2024.

[19] TI INSIDE. 35 milhões de brasileiros foram vítimas de *phishing* em 2023, estima Redbelt Security. *TI Inside*, 1 out. 2024. Disponível em: https://tiinside.com.br/01/10/2024/35-milhoes-de-brasileiros-foram-vitimas-de-*phishing*-em-2023-estima-redbelt-security/. Acesso em: 23 out. 2024.

[20] A Kaspersky é uma empresa global de cibersegurança, conhecida por desenvolver soluções de segurança digital, como antivírus, proteção contra *malware*, *ransomware* e ameaças cibernéticas em geral. Fundada em 1997 por Eugene Kaspersky, a empresa oferece uma variedade de produtos para proteger tanto usuários individuais quanto empresas e organizações que combatem ataques virtuais, espionagem e roubo de dados.

ataques por minuto. Segundo a empresa russa, o aumento no número de bloqueios foi de expressivos 617% em relação aos 12 meses anteriores.[21]

Além disso, pesquisas indicam que o *phishing* é um dos principais e mais predominantes vetores de ataque inicial para a violação de dados no ambiente digital. Segundo a IBM (*International Business Machines Corporation*[22]), os ataques perpetrados por meio de *phishing* resultaram em prejuízos com um custo médio de US$ 4,88 milhões por violação bem-sucedida entre 2023 e 2024.[23]

Se assimilarmos essas informações sobre o crescimento da prática de *phishing* àquela já mencionada no início do capítulo, de que o Brasil sempre liderou os rankings dos países que mais enviam spam[24], podemos chegar à simples conclusão de que, cedo ou tarde, o *phishing* se tornará uma grande problemática a ser enfrentada pelo sistema jurídico brasileiro.

Essa problemática se intensifica ainda mais, pelo fato de que, como verificamos anteriormente, o Brasil carece de um acervo normativo robusto que trate especificamente de crimes digitais e busca tratar esses delitos por meio da aplicabilidade de tipos penais já existentes no ordenamento jurídico brasileiro.

Nesse sentido, o *phishing* pode ser abordado tanto como um crime informático impróprio, quanto um crime informático próprio, visto que não há legislação específica que trate dessa prática criminosa.

Não obstante, o debate doutrinário demonstra que a classificação jurídica do *phishing* não é pacífica, pois sua caracterização pode variar conforme a modalidade adotada e os elementos que integram a conduta.

Uma primeira corrente doutrinária defende que o *phishing* não se enquadra no tipo penal previsto no art. 154-A, argumentando que, nos casos em

---

[21] KASPERSKY. Panorama de ciberameaças 2023: principais ameaças à cibersegurança no Brasil. Kaspersky Blog, 2023. Disponível em: https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/. Acesso em: 05 out. 2024.

[22] Ou conforme nossa tradução: “Corporação Internacional de Máquinas de Negócios”.

[23] DITORARONCARATI. Relatório da IBM: as crescentes interrupções nos negócios pelas violações de dados aumentam os custos de cibersegurança no Brasil. *Editora Roncarati*, 2022. Disponível em: https://www.editoraroncarati.com.br/v2/Artigos-e-Noticias/Artigos-e-Noticias/Relatorio-da-IBM-as-crescentes-interrupcoes-nos-negocios-pelas-violacoes-de-dados-aumentam-os-custos-de-ciberseguranca-no-Brasil.html. Acesso em: 23 set. 2024.

[24] KASPERSKY LAB. Kaspersky Lab revela que Brasil é o décimo país que mais envia *spam* no mundo. *Kaspersky Lab*, 28 jul. 2017. Disponível em: https://www.kaspersky.com.br/about/press-releases/kaspersky-lab-revela-que-brasil-e-o-decimo-pais-que-mais-envia-spam-no-mundo. Acesso em: 23 set. 2024.

que a vítima colabora involuntariamente para o acesso do agente ao dispositivo, não há invasão propriamente dita (JESUS; MILAGRE, 2024, p. 52).

Essa linha de entendimento sugere que o crime de invasão exige a superação de um obstáculo ou mecanismo de segurança, o que não ocorre nas situações em que o agente obtém acesso por meio de engenharia social ou fraude. Nesses casos, a vítima permite, mesmo que de forma induzida, a entrada do infrator.

Por essa perspectiva, o *phishing* com engenharia social poderia ser classificado como tentativa ou consumação do crime de estelionato, previsto no artigo 171 do Código Penal, se a fraude for utilizada para induzir a vítima a fornecer dados sensíveis. Da mesma forma, caso o objetivo do agente seja distrair a vítima para obter uma vantagem indevida, pode-se cogitar o enquadramento na figura do furto mediante fraude (JESUS; MILAGRE, 2024, p. 52).

Uma segunda corrente, no entanto, defende que o *phishing*, em qualquer de suas modalidades, poderia ser abrangido pelo artigo 154-A do Código Penal, pois a fraude utilizada pelo agente seria considerada uma forma de ultrapassar o mecanismo de segurança. Nessa interpretação, ainda que a vítima tenha colaborado, involuntariamente, com o acesso, o ato seria equivalente a uma invasão, uma vez que a fraude teria o papel de instrumentalizar a entrada indevida no sistema (JESUS; MILAGRE, 2024, p. 53).

Ainda mais intricado é o cenário envolvendo o uso de *malwares* no *phishing*, visto que nesses casos, a vítima pode ser induzida a executar um programa que libera as barreiras de segurança, permitindo que o agente acesse o sistema.

Essa situação é vista por alguns doutrinadores como uma forma de invasão, ainda que indireta, justificando a aplicação do artigo 154-A. Em contrapartida, quando o *malware* apenas captura dados sem permitir acesso direto ao dispositivo, surge a possibilidade de enquadramento em outras figuras penais, como espionagem ou concorrência desleal – tipificado no artigo 195 da Lei n. 9.279/96 - ou interceptação telemática – do artigo 10 da Lei n. 9.296/96 (JESUS; MILAGRE, 2024, p. 53).

Portanto, a classificação do *phishing* no ordenamento jurídico brasileiro é permeada por debates e divergências, visto que a multiplicidade de formas com que essa prática pode ocorrer, exige uma análise contextual e detalhada de cada caso concreto.

A depender dos meios empregados e do resultado obtido, o *phishing* pode ser enquadrado como estelionato, furto qualificado ou, em alguns casos, como invasão de dispositivo informático.

Contudo, ainda há lacunas legislativas, o que reforça a necessidade da atualização do arcabouço jurídico para acompanhar a evolução das práticas criminosas no ambiente digital, e inclusive da prática de *phishing*, que atualmente não encontra um respaldo seguro devido à lacuna legislativa existente.

Capítulo 2: Vitimologia

2.1 Estudo da Vitimologia: Conceito e Contextualização

Agora que já estudamos o *phishing* propriamente dito, vamos adentrar no estudo da vítima e o processo vitimizatório no contexto do *phishing*. Para isso, iniciemos com a conceituação e estudo da vitimologia.

A vitimologia é uma ciência que têm como objeto de estudo a vítima[25] e seu processo de vitimização, ou seja, é uma ciência que se preocupa em estudar o papel da vítima antes, durante e após a prática criminosa, analisando as complexas interações entre vítima e agressor, as influências das ações da vítima no crime e os impactos e consequências da prática criminosa na vida da vítima. Nas palavras de Viana (2018, p. 156), "compete à Vitimologia o estudo científico das vítimas do delito."

Insta salientar aqui o conceito de vítima, que conforme o professor a Declaração dos Princípios Fundamentais de Justiça Relativos às Vítimas da Criminalidade e de Abuso de Poder da ONU, são vítimas:

> as pessoas que, individual ou coletivamente tenham sofrido um prejuízo, nomeadamente um atentado à sua integridade física e um sofrimento de ordem moral, uma perda material, ou um grave atentado aos seus direitos fundamentais, como conseqüência de atos ou de omissões violadores das leis vigor num Estado membro, incluindo as que proíbem o abuso de poder. (ONU, 1985)

Não obstante, a vitimologia é um campo do conhecimento que busca estudar a origem da vitimização e analisar os fatores que a influenciam, como contextos sociais, psicológicos e individuais, além de explorar as consequências psicológicas, sociais e jurídicas enfrentadas pelas vítimas após a prática criminosa.

Salienta-se que o fenômeno da vitimização é o processo pelo qual uma pessoa ou grupo de pessoas se torna vítima de uma ação criminosa ou de qualquer forma de violência ou abuso, consequentes ou não do crime. Esse conceito vai além do ato criminoso em si, abrangendo também as consequências físicas, emocionais, psicológicas e sociais sofridas pela vítima. Nesse sentido,

[25] Vítima é “Aquela pessoa que sofre danos de ordem física, mental e econômica, bem como a que perde direitos fundamentais” (OLIVEIRA, 1999, p. 78). Assim sendo, vítima é pessoa que sofre direta ou indiretamente os efeitos de uma ação prejudicial, seja ela física, psicológica, financeira ou moral. No âmbito do direito penal, a vítima é o sujeito passivo da infração penal, aquele que sofre o dano ou a lesão decorrente da prática de um crime (OLIVEIRA, 1999, p. 81).

elencamos o comentário da professora Shirley Lizak Zulfa, a fim de melhor conceituar a vitimização:

> [...] vitimização refere-se ao efeito que um delito ou conduta criminosa tem sobre a vítima. Isto inclui efeitos psicológicos, físicos e financeiros que a vítima enfrenta após se tornar alvo de atividade criminosa. É notável que a vitimização pode acontecer mesmo quando uma pessoa não sofre lesões físicas diretas. O estresse, o medo e a ansiedade causada pelo crime são outras formas de vitimização. (ZULFAN, 2024, p. 159)

Assim, a vitimologia é uma ciência fundamental dentro do campo penal, que concentra seus esforços em analisar a vítima sob todas as suas esferas e perspectivas.

Embora seja de extrema relevância, o estudo da vítima e de sua experiência no contexto criminal foi, por muito tempo, negligenciado e marginalizado. Historicamente, especialmente no período que vai da Antiguidade até a Idade Média, houve o que é chamado de "idade de ouro da vítima", em que a vítima desempenhava um papel central na justiça primitiva (VIANA, 2018, p. 156-158).

O sistema de justiça, naquela época, funcionava com base em práticas como a "vingança de sangue" e o princípio do "olho por olho, dente por dente", ou seja, a justiça se fundava na vingança privada, em que a vítima ou seus familiares eram responsáveis por exigir reparação pelo dano sofrido, sem qualquer participação ou intermediação de uma autoridade estatal.

As sociedades antigas, como a babilônica, representada pelo Código de Hamurabi, o direito Hebreu, representado pela Lei de Talião, a índia antiga com o Código de Manu, o direito germânico e até o direito romano, com a lei das XII Tábuas, exemplificam essa abordagem de justiça (OLIVEIRA, 1999, p. 22-30)**.** Nessas culturas, não existia uma figura estatal forte ou sistemas centralizados de justiça como os que conhecemos hoje; a vítima era o ponto central na determinação da resposta ao crime.

Contudo, esse cenário começou a mudar com o surgimento do Estado, que tomou para si a titularidade do *jus puniendi* (direito de punir) e monopolizou o processo de aplicação da justiça, passando a ser o único responsável pela persecução penal e pela punição dos infratores.

Assim, as práticas de “justiça com as próprias mãos” e da “vingança de sangue”, que antes eram comuns e contempladas pela justiça primitiva, foram

completamente substituídas pela proteção Estatal, fazendo com que a vítima, que antes desempenhava um papel central na busca por reparação e justiça, se tornasse cada vez mais uma figura secundária. Nesse sentido, temos os ensinamentos da professora Ana Sofia Schmidt de Oliveira:

> O declínio da vítima no sistema penal coincide com o nascimento do Estado e do direito penal como instituição pública: o direito penal estatal surge exatamente com a neutralização da vítima. O Estado assume o controle absoluto do *jus puniendi*, convertendo-se no exclusivo detentor do monopólio da reação penal. (OLIVEIRA, 1999, p. 33)

Dessa forma, à medida que as estruturas estatais evoluíram e os sistemas de justiça se formalizaram, o papel da vítima foi progressivamente sendo relegado a um segundo plano. Isso se intensificou ainda mais com a ascensão e desenvolvimento da Escola Penal Positivista, que deu enfoque ao estudo do crime e do criminoso, tratando este último como o principal sujeito do crime. Assim, a vítima foi praticamente excluída das discussões jurídicas e tratada apenas como uma testemunha ou uma figura passiva no processo penal (VIANA, 2018, p. 158).

Esse distanciamento da vítima continuou com a consolidação do Direito Penal moderno, que trouxe uma abordagem de prevenção e repressão do crime. O Estado assumiu o protagonismo, tornando-se o principal interessado na punição dos infratores, o que contribuiu para a crescente marginalização da vítima, enquanto o crime passou a ser considerado uma ofensa ao Estado, e não diretamente à vítima, aprofundando ainda mais essa exclusão (VIANA, 2018, p. 158-159).

Foi somente no século XX, após a Segunda Guerra Mundial, que as ciências penais “redescobriram a vítima”, dando maior enfoque e atenção à sua existência e ao seu papel no sistema de justiça criminal.

Os horrores do conflito mundial, particularmente as atrocidades cometidas durante o Holocausto e os demais crimes de guerra praticados durante a guerra, expuseram de forma brutal as profundas consequências psicológicas, sociais e físicas que essas práticas geram nas vítimas.

Esse cenário ensejou criação de uma série de proteções e direitos voltados às vítimas do conflito, culminando na Declaração Universal dos Direitos Humanos, que representou uma reavaliação fundamental do modo de abordagem e tratamento do ser humano no pós-guerra.

Esse movimento não apenas reconheceu a necessidade de proteção aos direitos humanos, mas também trouxe à tona, a necessidade de reavaliar o papel da vítima no contexto do crime e na justiça, o que, de certa forma, pavimentou o caminho para o surgimento da vitimologia como ciência penal.

A professora Ana Sofia Schmidt de Oliveira, aponta em sua obra, a intrínseca ligação da vitimologia com a criação dos direitos humanos. Vejamos:

> O enorme sofrimento e o grande número de mortos nas batalhas da II Guerra Mundial, geravam já uma consternação generalizada que veio a ser intensificada quando os horrores dos campos de extermínio e de concentração vieram ao conhecimento público. (...) Este ultraje, esta grave ofensa, gerou um movimento no sentido contrário e impulsionou a construção de um direito dos direitos humanos e a criação de mecanismos protetores na ordem internacional. “Formando organizações como as Nações Unidas, muitos sonharam com um mundo livre da guerra, da violência, da ignorância, da pobreza e da doença. A comunidade internacional começou a criar convênios que iriam amparar os direitos das pessoas e protegê-las da vitimização”. (...) Não é difícil, portanto, identificar na genealogia do movimento internacional de direitos humanos, sempre buscando a proteção dos mais fracos, dos excluídos, dos apátridas, das minorias, o mesmo germe do movimento vitimológico, que pode ser visto como uma manifestação daquele. (OLIVEIRA, 1999, p. 64-65)

Assim, a partir do pós-guerra, começaram a surgir estudiosos que hoje são considerados por muitos como pioneiros da vitimologia, como Hans von Hentig e Benjamin Mendelsohn, cujos trabalhos foram fundamentais para a consolidação da vitimologia moderna. Seus estudos trouxeram à tona a importância de examinar as circunstâncias que tornam certas pessoas mais vulneráveis à vitimização, destacando fatores sociais, individuais e psicológicos que contribuem para essa exposição. Nesse sentido:

> A partir de 1947 a vitimologia passou a ser estudada, tendo como expoentes dessa primeira geração Benjamin Mendelsohn (Romênia), Hans Von Heting (Estados Unidos), Herry Ellenberger (Canadá), Jean Graven (Suíça), Steven Schafer e Margery Fry (Inglaterra), partindo-se nesse momento de um método dedutivo- empírico similar ao utilizado pelo positivismo para o sujeito ativo do crime e ato infracional, aplicando-se agora ao sujeito passivo. (SANTOS, 2024, p. 100)

Após, por volta das décadas de 1970 e 1980, o movimento vitimológico se intensificou e fortaleceu, tornando-se um ramo de estudo do Direito Penal, conforme assevera Oliveira:

> O início do movimento vitimológico pode ser localizado no período do pós-guerra, mas é só anos mais tarde que ganha corpo e substância. Alguns autores apontam a década de 70, outros a década de 80, como o período de seu efetivo robustecimento. (OLIVEIRA, 1999, p. 66)

Com isso, a vitimologia passou a ser vista como um campo essencial para a compreensão da dinâmica do crime, não apenas a partir da perspectiva do criminoso, mas também focando nas consequências que o delito impõe sobre a vítima.

Nesse ínterim, a vitimologia emergiu como um ramo de estudo ou “braço” da criminologia, mas com o tempo, vem se consolidando e sendo cada vez mais reconhecida como uma ciência autônoma, com abordagens próprias e independentes, tornando-se uma disciplina essencial para a compreensão das dinâmicas de vitimização e das relações entre vítimas, agressores e o sistema de justiça penal.

2.2 Vitimologia em face do *Phishing*

Agora, vamos abordar o processo de vitimização no contexto do *phishing*. Como já analisamos anteriormente, para que a vítima caia na armadilha e se torne efetivamente o sujeito passivo desse crime, antes, é necessário que ela, de alguma forma, participe ativamente - ainda que de maneira não intencional ou inconsciente - para que a prática criminosa tenha efeito.

Geralmente, a vítima é vista como um mero agente passivo, mas no *phishing*, essa perspectiva é um pouco diferente. A vítima nesse contexto, é agente passivo do crime, na medida em que é induzida ao erro e manipulada pelas técnicas de engenharia social do criminoso, vindo a sofrer os efeitos do crime, seja pela perda de patrimônio, pela violação de seus dados pessoais e de sua vida privada, ou por outros motivos. No entanto, devido a essa manipulação sofrida, paradoxalmente, no *phishing*, a vítima também acaba atuando e contribuindo para a consumação do crime. Ao seguir as instruções fraudulentas recebidas – como clicar em *links* maliciosos, fornecer dados pessoais ou financeiros –, a vítima facilita e garante o êxito do ataque.

Como analisado no presente trabalho, sem essa “micro-participação” da vítima, a prática criminosa não se consumaria. Assim, podemos concluir que essa interação ativa, mesmo que não intencional, coloca a vítima em uma posição complexa, pois, apesar de ser o alvo do crime, sua própria ação é parte essencial para a concretização do delito.

Não obstante, como veremos a seguir, essa característica da vítima do *phishing*, de não ser tratada como um mero agente passivo, mas também como uma espécie de “provocadora” ou “facilitadora” da prática criminosa, se alinha a algumas das categorias e classificações de vítimas que foram delineadas ao longo dos anos pelos principais estudiosos da vitimologia.

Nesse diapasão, a vítima do *phishing* se encaixa quase que perfeitamente na classificação da “Vítima de culpabilidade menor ou por ignorância”, trazida por Benjamin Mendelsohn, um dos pais da vitimologia. Essa, seria a vítima que coopera de alguma forma para o resultado danoso, em que, haveria certo grau de culpa da vítima para a consumação do crime, incitado por um impulso não voluntário da vítima ou por ignorância desta (OLIVEIRA, 2005, p. 194).

Essa classificação se coaduna, de certa forma, à figura da "Vítima Facilitadora" descrita por Jean Pinatel, sendo aquela que "gera a ocasião para o ato criminoso" (OLIVEIRA, 2005, p. 199). Esse tipo de vítima é comumente associado aos crimes de estelionato e extorsão – delitos muitas vezes ao *phishing* –, pois, nesses contextos, o criminoso não consegue concluir a prática criminosa sem que a vítima tome alguma atitude.

Insta salientar que não utilizaremos aqui a classificação de Benjamin Mendelsohn referente à "Vítima voluntária ou tão culpada quanto o infrator" (OLIVEIRA, 2005, p. 194), devido à técnica de engenharia social aplicada no *phishing*. Embora essa possa parecer a classificação mais adequada, dado que a vítima de *phishing* tem uma participação ativa para a indispensável consumação do crime, não podemos falar em culpa por parte da vítima, pois ela é manipulada por meio de técnicas de engenharia social.

Podemos também classificar a vítima do *Phishing* Scam e do *phishing* tradicional, como uma “Vítima indiferente ou indefinida”, em razão da técnica desse tipo de *phishing* ser empregada de forma massificada, não objetivando um indivíduo específico, mas buscando atingir o maior número possível de pessoas dentro daquele contexto e espectro-alvo (OLIVEIRA, 2005, p. 196).

Por outro lado, é evidente que ao tratarmos de outras técnicas de *phishing*, como o Spear *Phishing* ou o Whaling, estaremos lidando com uma "Vítima determinada". Ambas as classificações de vítimas – definida e indefinida -, são de Luiz Jiménez de Asúa (OLIVEIRA, 2005, p. 200).

Necessário ainda pontuar que, como a prática de *phishing* é multifacetada e se manifesta de diferentes formas e por diversos meios, a vítima também pode ser classificada como uma "Vítima ocasional", classificação de Severin Versele (OLIVEIRA, 2005, p. 201).

Não obstante, como vimos anteriormente, o principal meio de propagação do *phishing*, é o ambiente virtual, o que torna pontual e necessário se utilizar da classificação de Vasile Stanciu da “Vítima do progresso tecnológico” (OLIVEIRA, 2005, p. 204). É evidente que esse tipo de vítima será vitimizada mormente no ambiente digital, tendo em vista que a técnica de “pescaria” é desenvolvida principalmente no cyberespaço.

Para a próxima classificação, nos utilizaremos dos conhecimentos expostos no primeiro capítulo deste trabalho. Assim, como supramencionado, a

expansão da internet ocorreu de forma extremamente rápida e descontrolada, e uma parcela significativa da população mundial ainda carece de educação digital suficiente para navegar com segurança na rede.

Essa lacuna é ainda mais acentuada no caso da população brasileira, que, em grande parte, não possui sequer a alfabetização básica[26], quanto mais o conhecimento necessário para se proteger em ambientes digitais. Ademais, uma pesquisa recente realizada pela Agência Nacional de Telecomunicações (Anatel), revelou que mais de metade dos brasileiros não possuem habilidades digitais básicas, como anexar documentos em e-mails ou baixar aplicativos.[27]

A desinformação e a falta de educação digital são fatores que corroboram de forma significativa para a vitimização por *phishing*, pois tornam os indivíduos mais suscetíveis às técnicas de engenharia social utilizadas pelos cybers criminosos.

Nesse ínterim, por haver a aplicação de técnicas de engenharia social que exploram as fraquezas psicológicas e manipulam as vítimas de *phishing*, bem como pela vulnerabilidade causada pela ignorância e analfabetismo digital dessas vítimas, caberá também a classificação de “Vítima latente ou predisposta” (Ezzat Fatah)[28] e/ou de “Vítima com ânimo de lucro” (Hans von Hentig)[29].

Isso ocorre pelo fato de que muitos anúncios, páginas da *web*, *links* maliciosos e e-mails fraudulentos utilizam mensagens apelativas que exploram vulnerabilidades psicológicas e socioeconômicas das vítimas.

Para exemplificar, um *Pop-up* ou propaganda de determinado *site* malicioso, com mensagens como “clique aqui e aprenda a ganhar dinheiro fácil”, exploram a vulnerabilidade econômico-financeira da vítima, bem como seu

---

[26] O GLOBO. IBGE: 9,3 milhões de brasileiros ainda são analfabetos; a grande maioria com mais de 40 anos. *O Globo*, 22 mar. 2024. Disponível em: https://oglobo.globo.com/brasil/educacao/noticia/2024/03/22/ibge-93-milhoes-de-brasileiros-ainda-sao-analfabetos-a-grande-maioria-com-mais-de-40-anos.ghtml. Acesso em: 13 out. 2024.

[27] OLHAR DIGITAL. Quase metade dos brasileiros não tem habilidades digitais básicas. *Olhar Digital*, 19 jun. 2024. Disponível em: https://olhardigital.com.br/2024/06/19/internet-e-redes-sociais/quase-metade-dos-brasileiros-nao-tem-habilidades-digitais-basicas/. Acesso em: 13 out. 2024.

[28] Para verificar a explicação da classificação, ver OLIVEIRA (2005, p. 203).

[29] Para verificar a explicação da classificação, ver OLIVEIRA (2005, p. 195).

analfabetismo digital, incitando-a a clicar no *link*, resultando no roubo de seus dados ou até na instalação de *malwares* em seu dispositivo.

Assim, a “vítima latente ou predisposta” é aquela que, por algum motivo, já possui características ou vulnerabilidades – seja psicológica, social, econômica, física ou qualquer outra – que facilitam sua vitimização. Já a “vítima com ânimo de lucro” é induzida ao erro pela expectativa de obter ganhos financeiros rápidos, tornando-se, assim, um alvo fácil para golpes que exploram sua ganância ou curiosidade (OLIVEIRA, 2005, p. 195 e 203).

Agora que já alinhamos as classificações de vítimas, com a prática do *phishing*, vamos delinear o perfil da vítima do *phishing*.

Com base em pesquisas e artigos já publicados, não existe um perfil específico para a vítima de *phishing*, pois todos estão, em certa medida, suscetíveis a esse tipo de ataque.

Estudos, como o encontrado no artigo de Dawn M. Sarno, indicam que indivíduos mais velhos, por vezes, apresentam maior vulnerabilidade devido ao declínio cognitivo associado ao envelhecimento, embora possam adotar uma postura mais cautelosa ao se depararem com mensagens suspeitas, o que reduz o risco de vitimização (SARNO, 2023, p. 791 e 796).

Por outro lado, jovens adultos, embora mais familiarizados com tecnologia, tendem a exibir comportamentos impulsivos e a assumir riscos, o que os torna particularmente suscetíveis ao *phishing*. A curiosidade também exerce um papel relevante, pois mensagens que despertam interesse ou sugerem informações urgentes e inéditas atraem facilmente sua atenção, induzindo-os a interagir com conteúdos maliciosos (SARNO, 2023, p. 791-794 e 796).

Os estudos também sugerem que homens são menos suscetíveis ao *phishing*, possivelmente por terem uma maior exposição à tecnologia desde cedo e, com isso, desenvolverem maior familiaridade com as práticas digitais (IUGA, 2016, p. 11). No entanto, essas diferenças não são determinantes, e ambos os sexos podem ser alvos eficazes, dependendo das técnicas aplicadas.

Ainda assim, a experiência e o conhecimento em segurança digital podem colaborar para que o usuário fique mais preparado e alerta, mas não garantem proteção absoluta. Embora indivíduos expostos a tentativas anteriores de *phishing* ou que tenham recebido treinamento específico demonstrem maior capacidade de reconhecer mensagens fraudulentas, a confiança excessiva pode

levá-los a erros de julgamento e comportamentos negligentes, colocando-os novamente em risco (SARNO, 2023, p. 790).

Destarte, o *phishing* é uma prática que pode vitimar quase qualquer pessoa, especialmente por se tratar de uma técnica de engenharia social sofisticada, que manipula as emoções e expectativas da vítima para induzi-la ao erro, não havendo um perfil específico, embora existam grupos de indivíduos que são mais suscetíveis à prática criminosa.

Outro ponto da vitimização que deve ser abordado, é o ramo da vitimo-dogmática, que consiste no estudo da participação e do envolvimento da vítima no crime, analisando em que medida, a vítima pode ter contribuído para a consumação do delito, verificando sua culpa ou responsabilidade parcial, muitas vezes levantando questionamentos sobre a relação causal entre as ações da vítima e o resultado criminoso, o que, em algumas circunstâncias, pode ser usado para afastar ou atenuar a responsabilidade do autor da infração.

Sobre a vitimo-dogmática, destacamos as colocações do professor Eduardo Viana:

> [...] a vítimo-dogmática sugere valorar e incorporar os conhecimentos e princípios vitimológicos na delimitação das categorias e figuras delitivas, além de recorrer à influência da vítima na resolução dos problemas dogmáticos, atenuando ou mesmo excluindo a responsabilidade plena, em particular no tocante aos crimes patrimoniais (...) Em miragem de aproximação, a **vitimo-dogmática** compreende o exame do comportamento da vítima como fator que pode ser levado em consideração para calibrar a graduação da responsabilidade do autor ou alcance do âmbito de proteção do tipo penal. Como em geral se tem posto em manifesto, trata-se de investigar as aportações realizadas tanto pelo autor como pela vítima e, a partir daí, atribuir âmbitos de responsabilidade a um e outro (VIANA, 2018, p. 160 e 168-169)

Tendo isso em vista, no contexto do *phishing*, o fato de que a vítima frequentemente precisa incorrer em erro, imperícia ou até mesmo agir com dolo para que o crime obtenha êxito, tendo, de certa forma, uma participação ativa na consumação do delito, faz com que seja comum a tendência social de redirecionar a culpa para a própria vítima, como se ela fosse a verdadeira responsável por sua vitimização.

Nessa senda, poderíamos dizer que pelo fato de a vítima não tomar as cautelas adequadas para evitar a prática criminosa que é comum e recorrente no ambiente digital, a vítima teria certa culpabilização em sua própria vitimização, como muitas vezes a sociedade preceitua. Nesse sentido:

> [...] desenvolve-se uma racionalização do processo de responsabilidade baseado no princípio da autorresponsabilidade da vítima, cuja ideia central é: se a vítima renuncia ao uso de medidas de autoproteção disponíveis para ela e, portanto, abandona o bem jurídico, há de se eximir ou atenuar a responsabilidade penal do autor. O portador do bem jurídico não é merecedor de proteção se ele mesmo abre mão dessa. (VIANA, 2018, p. 170)

Ocorre que esse redirecionamento da culpa é um grande erro que ignora a dinâmica criminosa do *phishing*, visto que, como extensamente exposto neste trabalho, o criminoso explora e manipulada a vítima por uma estratégia sofisticada de engenharia social, não podendo assim, falar em culpabilidade por parte da vítima.

Dessa forma, transferir a responsabilidade do crime para a vítima não apenas desconsidera o papel do criminoso, mas também contribui para a revitimização, ao culpar aquele que foi enganado.

Essa culpabilização da vítima pode ter sérias consequências, tanto para o sistema de justiça quanto para o registro e tratamento adequado dos crimes de *phishing*.

Muitas vítimas, ao serem confrontadas com esse estigma de culpa, acabam por não reportar o crime às autoridades, temendo serem julgadas ou ridicularizadas. Esse comportamento contribui para o aumento da chamada cifra negra, termo utilizado para descrever o número de crimes que ocorrem, mas não são registrados oficialmente.

Como preceitua VIANA “a cifra negra representa a diferença entre a criminalidade real (...) e a criminalidade aparente”. (2018, p. 168), e nas palavras de GIMENES e FILHO, a cifra negra consiste no “número de delitos que por alguma razão não são levados ao conhecimento das autoridades, contribuindo para uma estatística divorciada da realidade fenomênica” (2024, p. 53).

No caso de crimes cibernéticos como o *phishing*, a cifra negra é particularmente alta,[30] justamente porque as vítimas frequentemente optam por

[30] FONTES SEGURA. Estelionatos crescem, já superam os roubos e fortalecem o crime organizado no Brasil. *Fontes Segura*, 2023. Disponível em: https://fontesegura.forumseguranca.org.br/estelionatos-crescem-ja-superam-os-roubos-e-fortalecem-o-crime-organizado-no-brasil/. Acesso em: 15 out. 2024.
O DIA. Cerca de 150 milhões de brasileiros foram vítimas do golpe de *phishing* em 2021, estima PSafe. *O Dia*, 22 out. 2021. Disponível em: https://odia.ig.com.br/economia/2021/10/6254180-cerca-de-150-milhoes-de-brasileiros-foram-vitimas-do-golpe-de-*phishing*-em-2021-estima-psafe.html. Acesso em: 15 out. 2024.

não buscar reparação, seja por vergonha, por desconhecimento de seus direitos, ou por falta de confiança no sistema de justiça.

Não obstante, essa transferência de culpa à vítima no contexto do *phishing*, também contribui para a revitimização dela, fazendo com que a vítima sofra em diferentes “fases”, e não somente com as consequências do crime, podendo vir a sofrer também com a persecução penal e posteriormente com a validação da própria sociedade.

Nessa senda, acerca dessa possibilidade da “revitimização”, nos utilizaremos dos ensinamentos do professor Guilherme de Souza Nucci, a constar:

> Além disso, é preciso identificar outros aspectos, que seguem além da vitimização primária (sofrer o delito diretamente). Secundariamente, o ofendido é submetido à investigação e ao processo criminal, obrigando-se a relembrar e narrar muitas vezes a mesma cena. Uma terceira fase se atinge com o comportamento da vítima depois de tudo isso, lidando com o trauma e outras consequências. Menciona-se muito a estigmatização dos delinquentes, mas se esquece, por vezes, do mesmo estigma suportado pelas vítimas, bastando enfocar os delitos sexuais para se ter noção disso. A pessoa ofendida sofre repetidos vexames, seja na polícia, seja em juízo. Há, ainda, em alguns casos, a avaliação pericial.20 Num outro estágio, a vítima ganha fama nos meios de comunicação, para bem ou para mal, recebe aplausos e críticas de grupos de redes sociais, sofrendo uma nova etapa da vida, com a qual tem que aprender a lidar.21 Tudo isso deve ser considerado pelos estudos de vitimologia, uma decorrência natural da criminologia. (NUCCI, 2024, p. 273)

Assim, a vítima, além de sofrer com a vitimização primária, que nas palavras de FILHO e GIMENES é “aquela que corresponde aos danos à vítima decorrentes do crime” (2024, p. 106), ou seja, com o crime em si; também pode vir a sofrer com uma vitimização secundária, terciária e até mesmo quaternária.

Esses conceitos de "fases da vitimização" servem para identificar e analisar as diferentes instâncias e momentos em que a vítima pode experimentar sofrimentos e impactos decorrentes do crime. Cada fase reflete um período específico da experiência da vítima, abrangendo desde o momento inicial da infração até os efeitos prolongados e as consequências sociais e psicológicas que podem surgir posteriormente.

No contexto do *phishing*, a primeira fase da vitimização pode gerar danos de natureza patrimonial à vítima, como a perda de dinheiro, bens ou acesso a contas bancárias, mas também podem envolver danos relativos à violação de privacidade e intimidade da vítima. Isso, pois, como já visto, a vítima é

frequentemente levada a fornecer informações sensíveis que, ao serem expostas ou utilizadas indevidamente, podem comprometer sua vida pessoal e financeira.

Já a segunda fase da vitimização, ou vitimização secundária, ou até mesmo revitimização, ou ainda sobrevitimização, consiste no “sofrimento adicional causado pela dinâmica do sistema de justiça criminal (inquérito policial e processo penal) (FILHO; GIMENES, 2024, p. 106), portanto, o ofendido é submetido novamente aos efeitos danosos causados pela conduta delitiva por meio da persecução penal.

Para a vítima do *phishing*, a grande problemática nessa fase se encontra na busca pela reparação, que na maior parte das vezes, não acontece. Os crimes cibernéticos nem sempre são adequadamente abarcados pelo sistema jurídico, e a complexidade envolvida na investigação de crimes cibernéticos dificulta a identificação e a responsabilização dos autores. A natureza anônima e transnacional desses delitos torna o rastreamento das ações criminosas um desafio, deixando muitas vítimas desamparadas e sem a possibilidade de obter reparação ou justiça.

Em continuidade, a vitimização terciária, na ótica da vítima, consistirá na estimação e julgamento social no pós-crime; basicamente será a fase em que a vítima poderá sofrer por ataques advindos da própria sociedade. Nesse sentido, para explicitar, destacamos as palavras do professor Eduardo Viana:

> [...] compreende, (...) o conjunto de custos (adicionais) sofridos por aquele que foi penalizado pela prática do crime, (...) como, eventualmente, a penalização suportada pela própria vítima do crime, como, por exemplo, na hipótese em que a comunidade exalta o criminoso e ridiculariza a vítima (VIANA, 2018, p. 167).

Assim, a vitimização terciária envolve os impactos sociais e culturais que a vítima enfrenta, muitas vezes sendo culpabilizada pela sociedade pelo próprio crime sofrido.

No Brasil, há uma tendência cultural de atribuir à vítima a responsabilidade pelo crime, rotulando-a como "ingênua", "burra" ou "idiota" por ter caído em um golpe. Essa postura é influenciada por valores como a "Lei de Gérson", que enaltece a ideia de levar vantagem em tudo, e a separação entre "malandro e mané", reforçando a crença de que quem foi enganado é culpado por sua falta de astúcia.

Esse tipo de vitimização é especialmente cruel, pois gera isolamento social, vergonha e constrangimento, dificultando que a vítima busque ajuda ou reparação e perpetuando um ciclo de silêncio e impunidade, contribuindo ainda mais para a já explicitada “cifra negra”. Nesta senda, destaca-se:

> [...] nesse contexto, a própria sociedade não acolhe a vítima, e muitas vezes a incentiva a não denunciar o delito às autoridades, ocorrendo o que se chama de cifra negra (quantidade de crimes que não chegam ao conhecimento do Estado). (FILHO; GIMENES, 2024, p. 106)

Para finalizar as fases de vitimização, falemos da chamada vitimização quaternária. Essa fase vem sendo cada vez mais latente nas últimas décadas, especialmente devido à influência crescente dos veículos de imprensa e das redes sociais.

Essa forma de vitimização ocorre quando a vítima é exposta publicamente e sofre com julgamentos e críticas amplificados pela mídia ou por interações em plataformas digitais. Nesse contexto:

> Esse processo de vitimização é muito frequente na atualidade, decorrendo do medo internalizado de tornar-se vítima de um crime. Ela é acometida pela insegurança psicológica ocasionada pelas notícias divulgadas pela mídia em geral, considerando que na maioria das vezes a criminalidade é retratada de modo sensacionalista na divulgação de crimes causando impacto na sociedade através do medo e da insegurança psicológica ou quando for vítima na esfera individual ou alguém de seu relacionamento. (FILHO; GIMENES, 2024, p. 106)

Dessa forma, os meios de comunicação, em sua busca por audiência e engajamento, muitas vezes exploram a imagem da vítima, desrespeitando sua privacidade e aprofundando seu trauma. Nas redes sociais, a situação pode ser ainda mais problemática, uma vez que a exposição da vítima ocorre de maneira massiva e instantânea, gerando julgamentos precipitados e discursos de ódio.

No caso do *phishing* envolvendo dados íntimos, como o ocorrido com a atriz Carolina Dieckmann, essa vitimização pode se tornar extremamente grave, visto que a vítima, além de sofrer com a perda de controle sobre suas informações, é forçada a enfrentar uma exposição pública desmedida, sendo sujeita ao escrutínio e à opinião de milhares de pessoas.

A vitimização quaternária se agrava pela dinâmica das redes sociais, onde a empatia costuma ser escassa, e o fenômeno de "culpabilização da vítima" é amplificado. Comentários depreciativos e ataques virtuais tornam-se comuns,

reforçando a ideia de que a vítima é a responsável pelo próprio infortúnio (FILHO; GIMENES, 2024, p. 106-107).

Além disso, a exposição midiática pode prejudicar a reputação da vítima, afetando sua vida profissional e suas relações sociais, podendo até mesmo inibir outras vítimas de denunciarem crimes semelhantes, por temer sofrer a mesma exposição e julgamento público.

Assim, essa fase “final” da vitimização, por ter um maior alcance devido à publicidade gerada pelas redes sociais, pode ser considerada uma extensão ou "amplificação" da vitimização terciária, porém, pode ser muito mais grave e perigosa devido a seu alcance e exposição massificados.

Destarte, finalizando a análise da vitimização no *phishing*, tendo em vista todo o exposto, podemos concluir que o processo de vitimização por *phishing* é um fenômeno complexo e multifacetado, e, portanto, o remédio e solução para a problemática do *phishing* – bem como de diversos outros crimes cibernéticos – não é simples e exige uma abordagem multidimensional que integre educação, legislação e o compromisso de diferentes setores da sociedade. Nesse contexto, destacamos:

> A resposta a essas condutas deve unir forças, tendo, de um lado, uma política educacional de conscientização da população acerca dos riscos associados ao meio e das práticas de segurança e prevenção, e, de outro lado, a própria legislação – tanto penal quanto cível. Assumem, aqui, importante papel, nessa união de forças, o setor privado – especialmente os provedores de serviços e os produtores de softwares – e a capacidade de autorregulação do setor. (...) Ainda, antes de utilizarmos a normatividade jurídico-penal como instrumento de solução da criminalidade relacionada às novas tecnologias, é importante adotarmos medidas educativas e informativas para a sociedade, pois o direito penal, nesse quesito, deve ser visto efetivamente como a *ultima ratio* para a solução do problema (SANTOS, 2022, p. 39)

Dessa maneira, a prevenção é a primeira linha de defesa contra os crimes de *phishing*. A conscientização da população acerca dos riscos associados ao ambiente digital e a disseminação de práticas de segurança cibernética são fundamentais para reduzir a vulnerabilidade das pessoas a esses ataques.

Nesse contexto, a alfabetização digital da população, bem como a promoção de campanhas educativas, desempenha um papel essencial, ao informar a sociedade sobre a importância de não compartilhar dados sensíveis, evitar clicar em *links* desconhecidos e verificar a autenticidade de comunicações digitais suspeitas.

Não obstante, além das campanhas de conscientização, vê-se também necessária a participação do setor privado, na medida em que a capacidade de autorregulação do setor tecnológico é essencial para antecipar ameaças e fornecer um ambiente digital mais seguro, complementando as políticas públicas e as iniciativas estatais.

Dessa forma, provedores de serviços de internet e produtores de *software* podem desenvolver ferramentas mais seguras, implementar tecnologias de autenticação multifatorial e melhorar os filtros de segurança que detectam e bloqueiam *links* fraudulentos.

Por fim, mesmo sendo o Direito Penal a *ultima ratio*, torna-se necessária a ampliação e modernização do arcabouço normativo, de modo que este seja capaz de acompanhar e enfrentar a complexidade crescente dos crimes cibernéticos.

Como já exposto, o Brasil carece de um acervo normativo robusto para tratar de crimes informáticos próprios. A grande problemática de continuar aplicando os tipos penais pré-existentes e tratar a grande maioria dos delitos informáticos como se impróprios fossem, está contida nos casos específicos, como da prática de *phishing*, em que há inadequação dos tipos penais já consagrados pelo Código Penal, pois não se ajustam plenamente a essa prática.

Esse cenário, por muitas vezes, faz com que o aplicador do Direito se utilize erroneamente da analogia in malam partem, para alinhar uma determinada conduta ilícita a um tipo penal pré-existente no ordenamento jurídico. Nesse sentido:

> Em que pese existirem tipos penais que possam criminalizar aquele que adultera ou destrói dados informatizados (art. 163 do Código Penal), ou mesmo aquele que copia ou move indevidamente informações (art. 155 do Código Penal) é inegável que tais “enquadramentos forçosos” sempre foram objeto de muitos e acalorados debates sob o prisma da “analogia in malan partem” e do princípio da reserva legal. (JESUS; MILAGRE, 2016, p. 35).

Ocorre que tal prática, em muitos dos casos, vai de encontro com os princípios da legalidade estrita e da reserva legal e pode gerar graves implicações para os direitos e garantias fundamentais.

Assim, a aplicação da analogia *in malam partem*, nesses casos, fere a segurança jurídica e a previsibilidade, alicerces fundamentais do Direito Penal, o que ao nosso ver, denota a evidente a necessidade de criação e

implementação de uma tipificação específica para ilícitos cometidos em meio digital, ainda não abarcados pela legislação brasileira.

Destarte, a criação de uma legislação específica para o *phishing* é de suma importância, mas não é a única medida, nem mesmo a principal para o combate dessa prática escusa e criminosa. A educação e a conscientização da população, somadas ao comprometimento do setor privado e ao fortalecimento do sistema de justiça, são medidas que devem ser integradas conjuntamente para o efetivo combate a essa prática.

Conclusão

O presente trabalho procurou abordar o processo de vitimização pela prática de *phishing*, demonstrando a complexidade e os desafios inerentes à caracterização da vítima e revelando que o combate à prática demanda mais do que a aplicação de ferramentas jurídicas tradicionais.

O *phishing*, enquanto prática criminosa, vai além de uma simples fraude eletrônica. Trata-se de uma sofisticada forma de manipulação psicológica, baseada em técnicas de engenharia social, que exploram tanto vulnerabilidades tecnológicas quanto falhas humanas. Essa característica torna indispensável uma abordagem integrada, que envolva educação digital, conscientização pública, e o aprimoramento do arcabouço legislativo para mitigar os danos causados por esse tipo de crime.

A expansão rápida e pouco regulada da internet no Brasil foi um dos fatores que ampliou significativamente a exposição dos cidadãos a crimes como o *phishing*. O ambiente digital, que deveria proporcionar um espaço seguro para a troca de informações, transformou-se em terreno fértil para ações ilícitas, em grande parte devido à limitada alfabetização digital da população. A falta de habilidades básicas para navegar com segurança facilita a atuação de cibercriminosos e expõe um número crescente de brasileiros a essas práticas.

Dessa forma, fica evidente a necessidade de promover uma educação digital acessível e contínua, visando capacitar os indivíduos para reconhecer e evitar golpes cibernéticos. Além da dimensão educacional, é essencial que o Brasil avance na criação de um arcabouço jurídico mais preciso para enfrentar crimes digitais. Embora a Lei Carolina Dieckmann e o Marco Civil da Internet representem progressos significativos, mas a ausência de uma tipificação penal específica para o *phishing* ainda dificulta a aplicação da lei.

Sem uma legislação própria, o sistema jurídico recorre a tipos penais inadequados, como o estelionato ou a invasão de dispositivos informáticos, para enquadrar as condutas relacionadas ao *phishing*. Esse enquadramento forçoso compromete a eficiência do sistema penal e gera insegurança jurídica, além de fomentar o uso da analogia in malam partem, violando o princípio da legalidade estrita e fragilizando o respeito às garantias fundamentais.

A criação de um tipo penal autônomo para o *phishing* traria maior clareza e precisão na imputação de responsabilidades, facilitando a persecução penal e

fortalecendo a segurança jurídica. Essa medida não apenas auxiliaria na punição efetiva dos cibercriminosos, mas também inibiria novas práticas por meio da dissuasão jurídica.

Portanto, a luta contra o *phishing* exige esforços coordenados entre o poder público, a sociedade e o setor privado, envolvendo educação contínua, modernização legislativa e conscientização coletiva. Apenas com uma abordagem integrada e atualizada será possível reduzir a incidência desse crime, oferecer proteção adequada às vítimas e garantir que o ambiente digital brasileiro seja um espaço seguro e confiável para todos os seus usuários.

Referências Bibliográficas

AFFINITY TECH PARTNERS. Scam alert: what you need to know about *Pop-up phishing*. *Affinity Tech Partners*, 3 maio 2018. Disponível em: https://www.affinitytechpartners.com/3n1blog/2018/5/3/scam-alert-what-you-need-to-know-about-pop-up-*phishing*#:~:text=What%20is%20Pop%2DUp%20*Phishing*,as%20the%20following%20example%20illustrates. Acesso em: 23 set. 2024.

ARAÚJO, Cláudio Rodrigues. Crimes Virtuais. Belo Horizonte: Expert, 2023. 66 p. ISBN 978-65-6006-018-0.

BISPO, Adrielle da Silva; BINTO, Emanuel Vieira. Crimes cibernéticos: da ineficácia da Lei Carolina Dieckmann na prática de crimes virtuais. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 11, p. 354-357, nov. 2023. DOI: 10.51891/rease.v9i11.12291.

BLOCKBIT. Fique alerta para os tipos comuns de *phishing*. *Blockbit Blog*, 2023. Disponível em: https://www.blockbit.com/pt/blog/fique-alerta-para-os-tipos-comuns-de-*phishing*/. Acesso em: 23 set. 2024.

BRASIL. Ministério Público Federal. Roteiro de atuação: crimes cibernéticos. 3. ed. rev. e ampl. Brasília: MPF, 2016. (Série Roteiros de Atuação, v. 5). Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes. Acesso em: 06 jun. 2024.

CGI.br. Combate ao spam na internet no Brasil: histórico e reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2015. 153 p. Disponível em: https://cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil-historico-e-reflexoes-sobre-o-combate-ao-spam-e-a-gerencia-da-porta-25-coordenados-pelo-comite-gestor-da-internet-no-brasil/. Acesso em: 06 jun. 2024.

CRESPO, Marcelo Xavier de F. Crimes digitais. Rio de Janeiro: Saraiva Jur, 2011. E-book. ISBN 9788502136663. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502136663/. Acesso em: 30 set. 2024.

DEMENTSHUK, Márcia; HENRIQUES, Percival. Pássaros voam em bando: a história da internet do século XVIII ao século XXI. João Pessoa: Editora da Associação Nacional para Inclusão Digital, 2019. 662 p. ISBN 978-65-80727-00-1.

DITORARONCARATI. Relatório da IBM: as crescentes interrupções nos negócios pelas violações de dados aumentam os custos de cibersegurança no Brasil. *Editora Roncarati*, 2022. Disponível em:

https://www.editoraroncarati.com.br/v2/Artigos-e-Noticias/Artigos-e-Noticias/Relatorio-da-IBM-as-crescentes-interrupcoes-nos-negocios-pelas-violacoes-de-dados-aumentam-os-custos-de-ciberseguranca-no-Brasil.html. Acesso em: 23 set. 2024.

EXTRA. Hackers atacam *sites* da Presidência, do governo brasileiro e da Petrobras. *Extra*, 23 jun. 2011. Disponível em: https://extra.globo.com/noticias/celular-e-tecnologia/hackers-atacam-*sites*-da-presidencia-do-governo-brasileiro-da-petrobras-2089754.html. Acesso em: 23 set. 2024.

FILHO, Nestor Sampaio P.; GIMENES, Eron V. Criminologia. 14th ed. Rio de Janeiro: Saraiva Jur, 2024. E-book. p.106. ISBN 9788553620326. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553620326/. Acesso em: 16 out. 2024.

FIORILLO, Celso Antônio P.; CONTE, Christiany P. Crimes no meio ambiente digital . Rio de Janeiro: Saraiva Jur, 2016. E-book. ISBN 9788547204198. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788547204198/. Acesso em: 30 set. 2024.

FIORILLO, Celso Antônio P. O Marco civil da internet e o meio ambiente digital na sociedade da informação - Comentários à Lei n. 12.965/2014, 1ª edição.. Rio de Janeiro: Saraiva Jur, 2015. E-book. ISBN 9788502627741. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627741/. Acesso em: 30 set. 2024.

FIORILLO, Celso Antonio Pacheco; FULLER, Greice Patricia. Sociedade da informação, crimes e direitos humanos sob o viés dos países centrais e periféricos. CONPEDI Law Review, Oñati, Espanha, v. 2, n. 1, p. 201-220, jan./jun. 2016. DOI: 10.21902/clr.v2i1.273.

FONTES SEGURA. Estelionatos crescem, já superam os roubos e fortalecem o crime organizado no Brasil. *Fontes Segura*, 2023. Disponível em: https://fontesegura.forumseguranca.org.br/estelionatos-crescem-ja-superam-os-roubos-e-fortalecem-o-crime-organizado-no-brasil/. Acesso em: 15 out. 2024.

GUEDES, Inês Sousa; GOMES, Marcus Alan de Melo (coord.). **CIBERCRIMINALIDADE**: NOVOS DESAFIOS, OFENSAS E SOLUÇÕES. [*S. l.*]: Pactor, 2021. 287 p. ISBN 978-989-693-122-3.

G1. Anatel diz que são golpe e-mails falsos notificando de multas por acesso ao X por VPN. *G1*, 4 set. 2024. Disponível em: https://g1.globo.com/politica/noticia/2024/09/04/anatel-diz-que-sao-golpe-e-

mails-falsos-notificando-de-multas-por-acesso-ao-x-por-vpn.ghtml. Acesso em: 05 out. 2024.

G1. Conheça o LulzSec, o grupo hacker que desafiou o governo dos EUA. *G1*, 27 jun. 2011. Disponível em: https://g1.globo.com/tecnologia/noticia/2011/06/conheca-o-lulzsec-o-grupo-hacker-que-desafiou-o-governo-dos-eua.html. Acesso em: 23 set. 2024.

G1. Suspeitos do roubo das fotos de Carolina Dieckmann são descobertos. G1, 7 maio 2012. Disponível em: https://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html. Acesso em: 23 set. 2024.

HAFNER, Katie; LYON, Matthew. Where wizards stay up late: the origins of the internet. New York: Simon & Schuster, 1998. 192 p. ISBN 0-684-87216-1.

INSTITUTO IBERO AMERICANO DE DERECHO PROCESAL (América Latina). La Víctima en el Proceso Penal: Su Régimen Legal en Argentina Bolivia Brasil Chile Paraguay Uruguay. Buenos Aires: Depalma, 1997. 229 p. ISBN 950-14-0946-5.

ISAACSON, Walter. The Innovators: how a group of hackers, geniuses, and geeks created the digital revolution. New York: Simon & Schuster, 2014. 544 p. ISBN 978-1-4767-0869-0.

IUGA, Cristian; NURSE, Jason R. C.; EROLA, Arnau. Baiting the hook: factors impacting susceptibility to *phishing* attacks. Human-centric computing and information sciences, v. 6, n. 8, p. 1-20, 2016. DOI https://doi.org/10.1186/s13673-016-0065-2. Disponível em: https://hcis-journal.springeropen.com/articles/10.1186/s13673-016-0065-2. Acesso em: Acesso em: 16 out. 2024.

JESUS, Damásio de; MILAGRE, José A. Manual de crimes informáticos . Rio de Janeiro: Saraiva Jur, 2016. E-book. ISBN 9788502627246. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/. Acesso em: 30 set. 2024.

KASPERSKY LAB. Kaspersky Lab revela que Brasil é o décimo país que mais envia *spam* no mundo. *Kaspersky Lab*, 28 jul. 2017. Disponível em: https://www.kaspersky.com.br/about/press-releases/kaspersky-lab-revela-que-brasil-e-o-decimo-pais-que-mais-envia-spam-no-mundo. Acesso em: 23 set. 2024.

KASPERSKY. Panorama de ciberameaças 2023: principais ameaças à cibersegurança no Brasil. Kaspersky Blog, 2023. Disponível em: https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/. Acesso em: 05 out. 2024.

LIMA, Cíntia Rosa Pereira de. ANPD e LGPD: Desafios e perspectivas. São Paulo: Almedina Brasil, 2021. E-book. ISBN 9786556272764. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556272764/. Acesso em: 30 set. 2024.

NOGUEIRA, Flavio Mirã de Souza; NOLASCO, Loreci Gottschalk. Crimes cibernéticos – desafios para o direito. Revista Jurídica Direito, Sociedade e Justiça, v. 9, n. 13, jan./jun. 2022. ISSN 2318-7034.

NORTON. Types of *phishing*. *Norton*, 2024. Disponível em: https://us.norton.com/blog/online-scams/types-of-*phishing*. Acesso em: 15 out. 2024.

NUCCI, Guilherme de Souza. Criminologia. Rio de Janeiro: Forense, 2021. E-book. p.262. ISBN 9786559641437. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559641437/. Acesso em: 16 out. 2024.

NUCCI, Guilherme de Souza. MANUAL DE DIREITO PENAL. 19. ed. rev. atual. e aum. Rio de Janeiro: Forense, 2023. 1182 p. v. ÚNICO. ISBN 978-65-5964-662-3.

O DIA. Cerca de 150 milhões de brasileiros foram vítimas do golpe de *phishing* em 2021, estima PSafe. *O Dia*, 22 out. 2021. Disponível em: https://odia.ig.com.br/economia/2021/10/6254180-cerca-de-150-milhoes-de-brasileiros-foram-vitimas-do-golpe-de-*phishing*-em-2021-estima-psafe.html. Acesso em: 15 out. 2024.

O GLOBO. Especialistas explicam como computador de Carolina Dieckmann foi hackeado. *O Globo*, 13 maio 2012. Disponível em: https://oglobo.globo.com/rio/especialistas-explicam-como-computador-de-carolina-dieckmann-foi-hackeado-4895771. Acesso em: 23 out. 2024.

O GLOBO. IBGE: 9,3 milhões de brasileiros ainda são analfabetos; a grande maioria com mais de 40 anos. *O Globo*, 22 mar. 2024. Disponível em: https://oglobo.globo.com/brasil/educacao/noticia/2024/03/22/ibge-93-milhoes-de-brasileiros-ainda-sao-analfabetos-a-grande-maioria-com-mais-de-40-anos.ghtml. Acesso em: 13 out. 2024.

OBSERVATÓRIO DA IMPRENSA. O AI-5 digital. *Observatório da Imprensa*, 19 nov. 2019. Disponível em: https://www.observatoriodaimprensa.com.br/e-noticias/o-ai-5-digital/. Acesso em: 23 set. 2024.

OLHAR DIGITAL. Quase metade dos brasileiros não tem habilidades digitais básicas. *Olhar Digital*, 19 jun. 2024. Disponível em: https://olhardigital.com.br/2024/06/19/internet-e-redes-sociais/quase-metade-dos-brasileiros-nao-tem-habilidades-digitais-basicas/. Acesso em: 13 out. 2024.

OLIVEIRA, Ana Sofia Schmidt de. A Vítima e o Direito Penal: Uma abordagem do movimento vitimológico e de seu impacto no direito penal. São Paulo: Revista os Tribunais, 1999. 190 p. ISBN 85-203-1811-8.

OLIVEIRA, Edmundo. Vitimologia e Direito Penal: O Crime Precipitado ou Programado pela Vítima. 4. ed. rev. e atual. Rio de Janeiro: Forense, 2005. 256 p. ISBN 85-309-2215-8.

ONU. Declaração dos Princípios Básicos de Justiça Relativos às Vítimas da Criminalidade e de Abuso de Poder. Nova York: Assembleia Geral das Nações Unidas, 1985.

PHOENIXNAP. Definição de rede mundial. PhoenixNAP Glossário, 2024. Disponível em: https://www.phoenixnap.pt/gloss%C3%A1rio/defini%C3%A7%C3%A3o-de-rede-mundial. Acesso em: 23 out. 2024.

PINHEIRO, Patricia P. Segurança Digital - Proteção de Dados nas Empresas. Rio de Janeiro: Atlas, 2020. E-book. ISBN 9788597026405. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 30 set. 2024.

SANTOS, Celeste Leite dos; INSTITUTO BRASILEIRO DE ATENÇÃO E APOIO ÀS VÍTIMAS; REVISTA INTERNACIONAL DE VITIMOLOGIA E JUSTIÇA RESTAURATIVA. Política judiciária de enfrentamento e apoio às vítimas de crimes e atos infracionais; os direitos no atendimento. Revista de Vitimologia e Justiça Restaurativa, São Paulo, v. 4, p. 93-118, 25 set. 2024. DOI https://doi.org/10.58725/rivjr.v2i2. Disponível em: https://revista.provitima.org/ojs/index.php/rpv/issue/view/4. Acesso em: 3 out. 2024.

SANTOS, Daniel Leonhardt dos. NOVOS ESPAÇOS DE PROTEÇÃO DO DIREITO PENAL NO MUNDO TECNOLÓGICO: a definição e caracterização dos crimes de informática. In: D'AVILA, Fabio Roberto; AMARAL, Maria Eduarda Azambuja (org.). DIREITO E TECNOLOGIA: ANAIS DO I COLÓQUIO NACIONAL DO IEDC. 1. ed. Porto Alegre: CItadel, 2022. cap. CIBERCRIME, p. 3-75. ISBN 978-65-5047-157-6.

SARNO, Dawn M.; HARRIS, Maggie W.; BLACK, Jeffrey. Which phish is captured in the net? Understanding *phishing* susceptibility and individual differences. Applied cognitive psychology, v. 37, n. 4, p. 789–803, 2023. DOI https://doi.org/10.1002/acp.4075. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1002/acp.4075. Acesso em: 16 out. 2024.

TI INSIDE. 35 milhões de brasileiros foram vítimas de *phishing* em 2023, estima Redbelt Security. *TI Inside*, 1 out. 2024. Disponível em:

https://tiinside.com.br/01/10/2024/35-milhoes-de-brasileiros-foram-vitimas-de-*phishing*-em-2023-estima-redbelt-security/. Acesso em: 23 out. 2024.

TREND MICRO. Tipos de *phishing*. *Trend Micro*, 2024. Disponível em: https://www.trendmicro.com/pt_br/what-is/*phishing*/types-of-*phishing*.html. Acesso em: 23 set. 2024.

TRIBUNAL DE JUSTIÇA DE SANTA CATARINA. Saiba identificar uma mensagem eletrônica indesejada. *TJSC*, 2024. Disponível em: https://www.tjsc.jus.br/*web*/servidor/dicas-de-ti/-/asset_publisher/0rjJEBzj2Oes/content/saiba-identificar-uma-mensagem-eletronica-indesejada#:~:text=Spam%20%C3%A9%20o%20termo%20usado,remetente%20na%20lista%20de%20destinat%C3%A1rios. Acesso em: 23 set. 2024.

VIANA, Eduardo. Criminologia. 6. ed. rev. atual. e aum. Salvador: JusPodivm, 2018. 448 p. ISBN 978-85-442-2073-3.

ZULFAN, Shirley Lizak; INSTITUTO BRASILEIRO DE ATENÇÃO E APOIO ÀS VÍTIMAS; REVISTA INTERNACIONAL DE VITIMOLOGIA E JUSTIÇA RESTAURATIVA. Vitimização e políticas públicas e reparação de danos à vítima de crimes e atos infracionais. Revista de Vitimologia e Justiça Restaurativa, São Paulo, v. 4, p. 159-179, 25 set. 2024. DOI https://doi.org/10.58725/rivjr.v2i2. Disponível em: https://revista.provitima.org/ojs/index.php/rpv/issue/view/4. Acesso em: 3 out. 2024.