UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE BIBLIOTECONOMIA E COMUNICAÇÃO
DEPARTAMENTO DE CIÊNCIAS DA INFORMAÇÃO
CURSO DE BIBLIOTECONOMIA

PEDRO LUIZ DE MARICHAL

Phishing **na era da informação:** relevância da proteção de dados pessoais

Porto Alegre
2022

PEDRO LUIZ DE MARICHAL

Phishing **na era da informação:** relevância da proteção de dados pessoais

Trabalho de Conclusão de Curso apresentado como requisito à obtenção do título de Bacharel em Biblioteconomia da Faculdade de Biblioteconomia e Comunicação da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Rene Faustino Gabriel Junior

Porto Alegre

2022

CIP - Catalogação na Publicação

Marichal, Pedro Luiz de
Phishing na era da informação: relevância da proteção de dados pessoais / Pedro Luiz de Marichal. -- 2022.
63 f.
Orientador: Rene Faustino Gabriel Junior.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Biblioteconomia e Comunicação, Curso de Biblioteconomia, Porto Alegre, BR-RS, 2022.

1. phishing. 2. engenharia social. 3. segurança da informação. 4. proteção de dados pessoais. 5. sociedade da informação. I. Junior, Rene Faustino Gabriel, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

Faculdade de Biblioteconomia e Comunicação
Departamento de Ciências da Informação
Rua Ramiro Barcelos, 2705, Bairro Santana
Porto Alegre/RS - CEP 90035-007
Telefone: 51 3308 5067
E-mail: fabico@ufrgs.br

PEDRO LUIZ DE MARICHAL

Phishing **na era da informação:** relevância da proteção de dados pessoais

Trabalho de Conclusão de Curso apresentado como requisito à obtenção do título de Bacharel em Biblioteconomia da Faculdade de Biblioteconomia e Comunicação da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Rene Faustino Gabriel Junior

Aprovado em: __/__/__

COMISSÃO EXAMINADORA:

_____

Prof. Dr. Rene Faustino Gabriel Junior (Orientador)
UFRGS/FABICO/DCI

_____

Prof. Dr. Rafael Port da Rocha
UFRGS/FABICO/DCI

_____

Mestranda Lucia Helena Cunha Vidal (PPGCIN-UFRGS)

AGRADECIMENTOS

Agradeço aos meus pais e minha irmã por todo o apoio, carinho, incentivo e compreensão nos momentos difíceis, não somente durante a trajetória acadêmica, mas desde sempre.

Agradeço ao meu orientador, prof. Rene Faustino Gabriel Junior, por toda a dedicação, conselhos, apontamentos, críticas e ideias ao longo deste trabalho.

Agradeço a toda a equipe da Biblioteca Central da UFRGS, onde enquanto bolsista de informática, pude aprender muito, inclusive sobre a profissão de bibliotecário. Agradecimento especial à Luísia, que sempre se mostrou disposta a ajudar quando tinha alguma dificuldade.

Agradeço a toda a equipe da Biblioteca do Direito da UFRGS, local onde realizei o estágio curricular obrigatório e que sempre manteve as portas abertas para que eu pudesse retornar. Agradecimento especial ao Emerson, um exemplo de profissional a ser seguido, que demonstrou muito conhecimento e habilidade como bibliotecário e que foi muito solícito e paciente quando precisei sanar dúvidas.

Enfim, para todos que contribuíram de alguma forma na conclusão desta etapa, ficam aqui os meus agradecimentos.

RESUMO

O presente trabalho analisa a ameaça de *phishing* na era informação e discute sobre a proteção de dados pessoais. Aborda a transformação ocorrida na sociedade a partir da era da informação e contextualiza temas, como a segurança da informação, dados pessoais, proteção de dados pessoais e legislação de dados pessoais. Disserta sobre o direito ao esquecimento e o superinformacionismo. Apresenta a definição de crimes cibernéticos e seus variados tipos. Quanto a metodologia, trata-se de um estudo de natureza básica, com abordagem qualitativa e do tipo exploratório. Como resultado da pesquisa, sistematiza os conceitos mais importantes sobre proteção de dados pessoais, analisa o conceito de engenharia social e suas técnicas, caracteriza os tipos de *phishing* e discorre sobre a sua ameaça à proteção de dados pessoais. Conclui que a melhor forma de proteção de dados pessoais contra o *phishing* são medidas preventivas tomadas pelo usuário.

Palavras-chave: phishing; engenharia social; segurança da informação; proteção de dados pessoais; sociedade da informação.

ABSTRACT

The present work analyzes the threat of phishing in the knowledge society and discusses the protection of personal data. It addresses the transformation that has occurred in society since the knowledge society and contextualizes topics such as information security, personal data, personal data protection and personal data legislation. Lectures on the right to be forgotten and overinformationism. It presents the definition of cybercrime and its various types. As for methodology, this is a basic study, with a qualitative and exploratory approach. As a result of the research, it systematizes the most important concepts about personal data protection, analyzes the concept of social engineering and its techniques, characterizes the types of phishing and discusses its threat to the protection of personal data. It concludes that the best way to protect personal data against phishing are preventive measures taken by the user.

Keywords: phishing; social engineering; information security; personal data protection; knowledge society.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANPD - Autoridade Nacional de Proteção de Dados

AOL - America Online

Brapci - Base de dados de Periódicos em Ciência da Informação

DDoS - *Distributed Denial of Service*

DoS – *Denial of Service*

DNS - *Domain Name Server*

INPI - Instituto Nacional da Propriedade Industrial

IP – Internet *Protocol*

LGPD - Lei Geral de Proteção de Dados Pessoais

PARC - Palo Alto Research Center

SENACON - Secretaria Nacional do Consumidor

TI – Tecnologia da Informação

VoIP - *Voice over IP*

SUMÁRIO

1 INTRODUÇÃO

Na era da informação, considerando especificamente o contexto digital, onde a cada dia se torna mais fácil a troca e o consumo de informações, pessoas mal intencionadas utilizam-se de técnicas de engenharia social para tirar vantagem sobre outras. Entre as diversas técnicas de engenharia social existentes, há o *phishing*, termo derivado do verbo em inglês "*fishing*", o qual significa pescaria. A pescaria de dados tem como objetivo obter informações sensíveis, tais como, dados bancários, senhas de contas de *e-mail*, serviços, entre outros. Esse método de obtenção de dados, pode parecer simples, uma vez que a vítima acaba por fornecer seus dados ao golpista. Entretanto, buscando cada vez mais parecerem fidedignos, *sites*, mensagens, aplicativos falsos, entre outros estão em constante evolução, tornando pessoas menos familiarizadas com as novas tecnologias, ou com menor compreensão acerca do funcionamento destes golpes, potenciais vítimas desses cibercrimes.

Dentre os variados tipos de cibercrimes, pode-se citar: ataques de *ransomware*, invasão de dispositivos para disseminação de vírus e *malware*, golpes e fraudes perpetuados por meio de redes sociais, além da interrupção ou perturbação de sites. Os tipos de crimes cibernéticos baseados em engenharia social, apesar das diferenças que têm entre si, possuem uma característica em comum: todos dependem da falha humana para o seu êxito, ou seja, a vítima precisa ser ludibriada a fazer o que o cibercriminoso está buscando. Assim, uma interação bem-sucedida entre o criminoso e a vítima, se estabelece como um papel-chave.

Dessa forma, é destacada a importância da proteção de dados pessoais, sendo alguns dos principais cuidados: desconfiar de *links* recebidos, criar backups dos dados armazenados, principalmente em nuvem, criar senhas fortes combinando caracteres especiais, letras maiúsculas, minúsculas e números, evitando o uso de palavras comuns ou dados pessoais e habilitar a verificação de senhas em duas etapas sempre que possível, especialmente em sistemas de armazenamento em nuvem e aplicativos de mensagens.

Existem leis que protegem os cidadãos contra crimes cibernéticos, como a Lei nº 12.737/2012, conhecida por "Lei Carolina Dieckmann", que dispõe sobre a

tipificação criminal de delitos informáticos, a Lei nº 12.965/2014 ou “Marco Civil da Internet”, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e a Lei nº 14.155/2021, que torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela Internet. Em um âmbito mais geral, existe a Lei Geral de Proteção de Dados, responsável por regular a coleta, o tratamento e o uso de dados, buscando garantir a privacidade das pessoas físicas e jurídicas.

Sendo a segurança da informação responsável pela gestão de diversos ativos, como a própria informação e os agentes que manipulam ou processam informações, tendo como destaque os agentes humanos, é necessário compreender e identificar os riscos, bem como as medidas relacionadas à segurança da informação que podem ser tomadas visando a proteção de dados.

1.1 PROBLEMA DE PESQUISA

Diante do que foi apresentado, surge o seguinte problema de pesquisa: Como as pessoas protegem seus dados da ameaça de *phishing* na era da informação?

1.2 OBJETIVOS

Nas próximas subseções serão apresentados os objetivos geral e específicos.

1.2.1 Objetivo geral

O objetivo geral deste trabalho é contextualizas formas de proteção de dados pessoais contra a ameaça de técnicas de engenharia social (*phishing*).

1.2.2 Objetivos específicos

Abaixo estão descritos os objetivos específicos desse trabalho:

a) identificar e definir os conceitos relacionados a proteção de dados pessoais;
b) analisar o conceito de engenharia social e as técnicas usadas para enganar usuários na Internet;
c) caracterizar os tipos de *phishing* e apresentar a sua ameaça à proteção de dados pessoais.

1.3 JUSTIFICATIVA

A escolha do tema é justificada por tratar de um problema que, embora exista há mais de duas décadas, está cada vez mais presente, sendo noticiado com frequência em portais de notícias na Internet, programas de televisão, rádio, entre outros meios de comunicação.

Na era da informação, período atual da sociedade, o volume de informação criado e acessível por meio de dispositivos, móveis ou não, é gigantesco, sendo assim necessário saber se comportar diante deste cenário, ou seja, ter um comportamento infocomunicacional adequado. Como aponta Neves e Borges (2020, p. 2), o: “Comportamento infocomunicacional refere-se às formas como as pessoas se informam e comunicam, ou seja, aos modos como consomem informação, mas também a produzem, comunicam e se relacionam”.

Nesse sentido, o pesquisador por ter afinidade com a área da Tecnologia da Informação (TI) e como um futuro profissional da informação, considera necessário tratar desse tema. Pela formação em Biblioteconomia, que tem como insumo a informação, é primordial conhecer as ameaças que põem em risco a segurança da informação, em especial a proteção de dados, e saber como evitar tais riscos ao adotar medidas que impeçam os vazamentos de dados.

Outra justificativa refere-se ao aumento de casos de crimes cibernéticos decorrente da captura de informações pessoais e institucionais. Delitos estes, motivados principalmente no período da pandemia do novo coronavírus (2020-2022), o que levou inclusive a criação da Lei nº 14.155/2021 que aumenta a gravidade de crimes como o estelionato ocorrido em meios digitais. Dessa forma, percebe-se que estes tipos de crimes vêm recebendo cada vez mais atenção por parte do Poder Legislativo.

Segundo Araujo, Mota e Oliveira (2020), os profissionais da informação precisam sempre estar atentos à qualidade e veracidade das informações, colaborando pelo bem comum, uma vez que qualquer ser humano com acesso à rede mundial de computadores é um potencial produtor e replicador de conteúdo.

2 METODOLOGIA

O método científico é composto de um conjunto de regras básicas dos procedimentos que produzem o conhecimento científico. Conforme salienta Gil (2008), o que torna o conhecimento científico diferente dos demais é a verificabilidade, sua característica principal. Dessa forma, para que o conhecimento possa ser considerado científico, é preciso determinar o método que possibilitou chegar a esse conhecimento. Apesar dos diversos métodos existentes, cada um mais adequado para determinada área do conhecimento, todos têm um mesmo objetivo. Como discorre Gil (2008, p. 8): “Pode-se definir método como caminho para se chegar a determinado fim. E método científico como o conjunto de procedimentos intelectuais e técnicos adotados para se atingir o conhecimento.”.

A pesquisa é o conjunto de atividades com a finalidade de descobrir novos conhecimentos. Silva e Menezes (2005, p. 20) definem pesquisa como “[...] um conjunto de ações, propostas para encontrar a solução para um problema, que têm por base procedimentos racionais e sistemáticos. A pesquisa é realizada quando se tem um problema e não se têm informações para solucioná-lo.”. Em outras palavras, para Gil (2008 p. 26), a pesquisa é “[...] o processo formal e sistemático de desenvolvimento do método científico. O objetivo fundamental da pesquisa é descobrir respostas para problemas mediante o emprego de procedimentos científicos.”.

Assim sendo, o presente estudo, quanto a sua natureza, é uma pesquisa básica, uma vez que tem a finalidade de gerar novos conhecimentos úteis para o avanço da ciência, envolvendo verdades e interesses universais sem precisar ter a previsão de uma aplicação prática (SILVA; MENEZES, 2005).

Sobre a forma de abordagem do estudo, caracteriza-se como uma pesquisa qualitativa, pois este tipo de pesquisa considera que:

> [...] há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa. Não requer o uso de métodos e técnicas estatísticas. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento-chave. É descritiva. Os pesquisadores tendem a analisar seus dados indutivamente. O processo e seu significado são os focos principais de abordagem. (SILVA; MENEZES, 2005, p. 20).

Dentro da abordagem qualitativa, o método indutivo pode ser definido como a generalização constatada a partir da observação de casos concretos suficientemente confirmadores dessa realidade (GIL, 2008). Assim, Gil (2008, p. 10) complementa:

> Nesse método, parte-se da observação de fatos ou fenômenos cujas causas se deseja conhecer. A seguir, procura-se compará-los com a finalidade de descobrir as relações existentes entre eles. Por fim, procede-se à generalização, com base na relação verificada entre os fatos ou fenômenos.

Em relação aos fins, o estudo trata-se de uma pesquisa exploratória. Este nível de pesquisa tem “[...] como principal finalidade desenvolver, esclarecer e modificar conceitos e ideias, tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores.” (GIL, 2008, p. 27). Ainda segundo Gil (2008), a pesquisa exploratória é, dentre todos os tipos de pesquisa, a que apresenta menor rigidez no planejamento. Frequentemente inclui levantamento bibliográfico e documental, entrevistas não padronizadas e estudos de caso, além disso, não costuma utilizar técnicas quantitativas de coleta de dados e procedimentos de amostragem, pois são desenvolvidas com o objetivo de proporcionar visão geral, de tipo aproximativo, sobre determinado fato e também são realizadas principalmente em temas pouco explorados, o que torna difícil formular hipóteses precisas e operacionalizáveis.

Pesquisas exploratórias comumente compõem a primeira fase de uma pesquisa mais extensa. Caso o tema escolhido seja muito genérico, o seu esclarecimento e delimitação se tornam necessários, onde, nesse caso, a partir da revisão de literatura, discussão com especialistas e outros procedimentos, o resultado do processo acaba sendo um problema mais compreensível e passível de investigação mediante procedimentos mais sistematizados (GIL, 2008).

Para atender os objetivos, o estudo realiza o levantamento bibliográfico do tema de pesquisa. O levantamento bibliográfico é descrito como o procedimento onde o autor tem contato direto com as obras que abordam o tema escolhido com o intuito de elucidar os objetivos de pesquisa (SOUSA; OLIVEIRA; ALVES, 2021).

Segundo Cervo e Bervian (2002, p. 65), “A pesquisa bibliográfica procura explicar um problema a partir de referências teóricas publicadas em documentos”. Sobre a abordagem, será realizada a análise e síntese, onde a análise é responsável pela “[...] decomposição de um todo em suas partes.” (CERVO; BERVIAN, 2002, p. 38), enquanto: “A síntese é a reconstituição do todo decomposto pela análise.” (CERVO; BERVIAN, 2002, p. 38).

Para tal, são realizadas buscas em diversas bases de dados utilizando palavras-chave a fim de localizar as obras que serão usadas. O pesquisador deve realizar uma leitura exploratória para a delimitação do tema (SOUSA; OLIVEIRA; ALVES, 2021).

Dentre as bases de dados utilizadas estão a Base de dados de Periódicos em Ciência da Informação (Brapci), Google acadêmico e SciELO. As palavras-chave utilizadas foram: *phishing*, dados pessoais, proteção de dados, segurança da informação, LGPD, cibercrimes, engenharia social e sociedade da informação.

Os resultados das buscas foram agrupados em um *corpus* de pesquisa, onde posteriormente foi feita a análise das informações obtidas. Assim, a análise foi dividida nas seguintes etapas:

a) identificar o contexto histórico e atual dos assuntos que compõem o trabalho no material recuperado;
b) identificar os conceitos presentes no *corpus* de pesquisa destacando as partes principais para citação no trabalho;
c) relacionar os temas de modo a atingir os objetivos específicos.

3 RESULTADOS DA PESQUISA

O trabalho está organizado de forma a apresentar os resultados conforme apresentação dos objetivos específicos, o primeiro objetivo de identificação dos conceitos relacionados à proteção de dados pessoais está dividido nas seguintes seções: a sociedade da informação, segurança da informação, proteção de dados pessoais, dados pessoais – definição, proteção de dados pessoais, legislação sobre proteção de dados pessoais, direito ao esquecimento e o superinformacionismo, crimes cibernéticos (cibercrimes), tipos de cibercrimes e *malware*.

3.1 A SOCIEDADE DA INFORMAÇÃO

A sociedade da informação, também conhecida como era da informação, teve seu começo no final do século XX, por volta dos anos 1970 (MARTINI, 2017). Segundo Martini (2017), um dos exemplos que marcam o início desta era foi a criação do Palo Alto Research Center (PARC) pela Xerox. O laboratório de pesquisa, localizado em Palo Alto, Califórnia era composto por pesquisadores de várias áreas.

Corroborando com isso, é possível ver que:

> Ele fora pensado e desenvolvido pela poderosa Corporação Xerox em 1970, em Palo Alto, Califórnia, e de forma interdisciplinar reunia pesquisadores em diversas áreas (físicos, engenheiros, programadores etc.), com a missão de criar o que a Corporação chamava de forma fantasticamente visionária: arquitetura da informação. Ao longo dos anos 1970, é impressionante o legado do Centro de Pesquisa PARC. (MARTINI, 2017, p. 27).

Os anos 1970 se destacam no que se refere ao início do período entendido como sociedade da informação, Castells (1999) destaca que devido à importância de contextos históricos específicos das trajetórias tecnológicas e do modo característico de interação entre a tecnologia e a sociedade, considera que houve um divisor tecnológico nos anos 1970 e recorda alguns exemplos e datas associadas a descobertas básicas nas tecnologias da informação. Assim, sobre as tecnologias da informação, Castells (1999, p. 91) afirma que:

> Todas têm algo de essencial em comum: embora baseadas principalmente nos conhecimentos já existentes e desenvolvidas como uma extensão das tecnologias mais importantes, essas tecnologias representaram um salto qualitativo na difusão maciça da tecnologia em aplicações comerciais e civis, devido a sua acessibilidade e custo cada vez menor, com qualidade cada vez maior.

Entre as tecnologias destacadas por Castells (1999) estão o microprocessador, o principal dispositivo de difusão da microeletrônica, inventado em 1971 e que começou a ser difundido em meados dos anos 1970. Mais tarde, em 1975 foi inventado o microcomputador e, em seguida, em abril de 1977, o Apple II surgiu e se tornou o primeiro produto comercial de sucesso. Nessa mesma época, a Microsoft já começa a produzir sistemas operacionais para computadores. A matriz de variadas tecnologias de *software* para computadores pessoais dos anos 1990, Xerox Alto, foi desenvolvida nos laboratórios PARC em Palo Alto, em 1973. O primeiro comutador eletrônico industrial, apareceu em 1969, e o comutador digital foi desenvolvido entre os anos de 1970 e passou a ser comercializado em 1977. A empresa Corning Glass, no início da década de 1970, iniciou a produção, em escala industrial, da fibra ótica. Ainda nos anos 1970, a Sony começou a produzir videocassetes comercialmente a partir das descobertas ocorridas nos EUA e na Inglaterra, que não haviam conseguido alcançar a produção em massa desses aparelhos na década anterior.

Por fim, Castells (1999) cita a instalação da nova e revolucionária rede eletrônica de comunicação feita em 1969 pela ARPA (Agência de Projetos de Pesquisa Avançada do Departamento de Defesa Norte-Americano) que se desenvolveu ao longo dos anos de 1970 e, algum tempo depois, se tornou a Internet. A rede foi profundamente beneficiada pela invenção de Vinton Cerf e Robert Kahn, em 1973, quando foi desenvolvido o protocolo TCP/IP, introduzindo uma tecnologia capaz de conectar diferentes tipos de rede. Castells (1999) ainda salienta o surgimento e a difusão paralela da engenharia genética ocorrida nesse mesmo período e faz a seguinte afirmação: “[...] podemos dizer, sem exagero, que a revolução da tecnologia da informação propriamente dita nasceu na década de 1970 [...]” (CASTELLS, 1999, p. 91).

Com o advento da infraestrutura da informação, a circulação e o fluxo de informações se intensificam e isso é possível observar na rede, mais precisamente, na sociedade em rede (MARTINI, 2017).

Apesar do começo da sociedade da informação ter acontecido nos anos 1970, o seu conceito foi utilizado anteriormente pelo economista Fritz Machlup, em seu livro *The Production and Distribution of Knowledge in the United States*[1] publicado em 1962 (COUTINHO; LISBÔA, 2011). Como aponta Werthein (2000), a expressão “sociedade da informação” começou a ser utilizada no final do século XX para substituir o termo “sociedade pós-industrial”, muito utilizado na época.

No início dessa nova sociedade que estava surgindo, os serviços substituiriam os produtos como impulso decorrente da atividade econômica. Depois, o trabalho se basearia no conhecimento e na criatividade mais do que na burocracia, característica bastante marcante desde o século XIX (MARTINI, 2017). Dessa forma, a informatização da vida teria um aspecto predominante, obrigando as corporações que buscavam estar uma situação confortável, por meio da estabilidade a descobrirem novas formas de se sentir à vontade em uma nova vida focada na mudança e na inovação. A respeito da união entre a sociedade pós-industrial e a sociedade da informação, Martini (2017, p. 35) observa que “[...] é uma remissão histórica importante, já que essa fusão, por assim dizer, entre, por um lado, a sociedade da informação, e, por outro, a sociedade pós-industrial, seja hoje talvez consensual.”.

Werthein (2000) apresenta a ideia de que o conceito de sociedade pós-industrial era bastante complexo por englobar aspectos sociais, políticos e econômicos. As transformações técnicas organizacionais e administrativas fizeram a sociedade não mais se basear em insumos de energia, mas em insumos de informação propiciados a partir de avanços tecnológicos em microeletrônica e telecomunicações. Sendo agora a informação a matéria-prima, o homem passa a agir diretamente sobre a informação, ao contrário da sociedade industrial, onde a informação já existente era usada sobre as tecnologias, seja com o objetivo de implementar ou adaptar para novos usos. A respeito dessa transformação na sociedade, cabe a seguinte afirmação de Martini (2017, p. 27): “Está no coração da

[1] A produção e distribuição do conhecimento nos Estados Unidos

sociedade da informação e de sua economia a capacidade de inovar com a finalidade de investigar algo, ainda que sem capacidade de mercado ou sem demanda imediata.”.

Para Demo (2000), lidar com informação exige inteligência. Por envolver subjetividade, fator que propicia a capacidade de criar, mudar e refazer, o processo de criação do conhecimento não é linear e compreende diversas dificuldades, sendo a manipulação uma delas. Apesar do volume gigantesco de informação que é produzido, a sociedade da informação falha em informar. Tratando-se sobre a economia da informação, onde esta é considerada primariamente como uma mercadoria, é apontado que a manipulação juntamente com a desinformação das pessoas e a relação delas com a mídia, uma fonte manipuladora, contribui contra a formação da inteligência necessária para lidar com a informação.

3.2 SEGURANÇA DA INFORMAÇÃO

A presença da informação pode ser observada em diversas fases da história, como aponta Sêmola (2003, p. 1), “[...] todas as empresas, independentemente de seu segmento de mercado, de seu *core business* e porte, em todas essas fases de existência, sempre usufruíram da informação [...]”, ou seja, nas diversas fases históricas, a informação sempre foi utilizada para a tomada de decisão.

Dessa forma, as empresas têm sido influenciadas por mudanças e novidades decorrentes de novas descobertas, experimentos, conceitos, métodos e modelos derivados de uma movimentação frequente, como se fosse um ciclo, de estudiosos, pesquisadores e executivos inconformados e que buscam a inovação e a quebra de paradigmas (SÊMOLA, 2003).

Ao longo dos anos, a informação tem se apresentado quase que em sua totalidade no formato digital. A presença de sistemas digitais se expandiu tanto que as organizações, atualmente, têm a sua base de funcionamento dependente de tecnologias. A partir disso, os riscos como furto, perda ou alterações de informações que ameaçam esses sistemas, colocaram em evidência o tema de segurança da informação (SOUZA, 2020).

A dependência da tecnologia da informação, segundo Sêmola (2003) começou a ocorrer devido à redução dos custos existentes para investimentos em *mainframes*, o que possibilitou que essas máquinas passassem a exercer a função de central de processamento e armazenamento de dados. Se décadas antes, estes grandes computadores eram vistos apenas como uma nova e promissora ferramenta, dada as limitações de armazenamento e os preços proibitivos desta tecnologia, logo depois, os *mainframes* se tornaram mais acessíveis enquanto coexistiam com os tradicionais arquivos deslizantes, onde eram armazenados documentos manuscritos. Mais adiante, terminais começaram a se espalhar pelos ambientes da empresa, onde inicialmente, existiam um único por departamento de modo a permitir consultas remotas. Nesse sentido, Sêmola (2003, p. 3) sugere que:

> Compartilhar informação passou a ser considerada uma prática moderna de gestão e necessária a empresas que buscam maior velocidade nas ações. Diante disso, surgiram em seguida as primeiras redes de computadores e, paralelamente, as informações passaram a ser mais digitalizadas e os processo mais automatizados.

De acordo com Castells (2003), a partir da difusão da Internet no mundo dos negócios na década de 1990, momento marcado pela transformação organizacional das empresas de tecnologia que buscavam ser mais produtivas e competitivas por meio da cooperação, o modelo de empresa de rede foi popularizado, deixando de estar restrito à indústria tecnológica e se tornando cada vez mais presente em diversos setores de atividade. Desde então, as empresas de rede vêm tornando suas formas de administração, produção e distribuição semelhantes umas com as outras, sendo comum a existência de companhias essencialmente *on-line*, uma vez que a essência do negócio eletrônico está na conexão em rede, a qual é baseada na Internet.

Beal (2004) aponta que administrar os recursos informacionais e seus fluxos na organização é uma necessidade cada vez mais presente em qualquer tipo de negócio. Por estarem inseridas em um contexto que compreende um ambiente repleto de inter-relações que permanecem em constante estado de mutação, a informação e o conhecimento representam patrimônios que vão aumentando progressivamente de valor. Informação e conhecimento são necessários para

prever, compreender e responder às mudanças ambientais, bem como alcançar ou manter uma posição favorável no mercado. A respeito disso, Sêmola (2003, p. 39) define o valor da informação da seguinte forma: “A Informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa.”.

Nesse sentido, como complementam Mascarenhas Neto e Araújo (2019), a gestão da informação se tornou um mecanismo estratégico para os administradores, os gestores e os executivos no processo decisório, uma vez que a informação exerce um papel fundamental na busca pela competitividade e sobrevivência das organizações. Assim, a gestão da segurança da informação pode ser definida como uma atividade básica de proteção contra ameaças com o objetivo de garantir a integridade, disponibilidade e confidencialidade, controlando e assegurando o ambiente informacional na organização. Os ambientes informacionais estão expostos a fortes mudanças que aceleram as suas transformações. Tais mudanças podem constituir-se em diversas ordens, sejam elas econômicas, sociais, culturais, políticas, ideológicas e tecnológicas.

Sêmola (2003) apresenta a informação como um ativo, pois esse termo derivado da área financeira, é atribuído a elementos que possuem valor a um indivíduo ou organização e, portanto, necessitam de proteção adequada. Assim, considerando a segurança da informação, um ativo é: “Todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.” (SÊMOLA, 2003, p. 45).

Para Souza (2020), reconhecer o valor que as informações representam para as organizações é universalmente aceito e considerado um dos recursos mais importantes para o seu sucesso. Dessa forma, “[...] a informação é um fator estruturante e um instrumento de gestão para as organizações, a qual necessita ser devidamente protegida.” (SOUZA, 2020 p. 21).

Mascarenhas Neto e Araújo (2019) identificam uma transição de paradigmas nas organizações referente a interação humana com a informação. Os elementos ativos, conhecidos como “usuários”, que interagem com os processos, procedimentos organizacionais e com os sistemas de informação, tomaram o lugar

dos antigos “colaboradores”, que recebiam as informações de forma passiva. Assim, os usuários da informação passam por constantes mudanças ao estarem diretamente ligados aos avanços da tecnologia. A partir dessa transição de paradigmas, observada nas organizações, se faz necessário adotar um comportamento dinâmico a respeito da segurança das informações. Essa interação contínua e sem barreiras pertencente ao referido contexto cria diversos desafios para as organizações, em especial à segurança da informação que tem como função proteger os ambientes informacionais dos múltiplos e variados métodos de ataque (MASCARENHAS NETO; ARAÚJO, 2019).

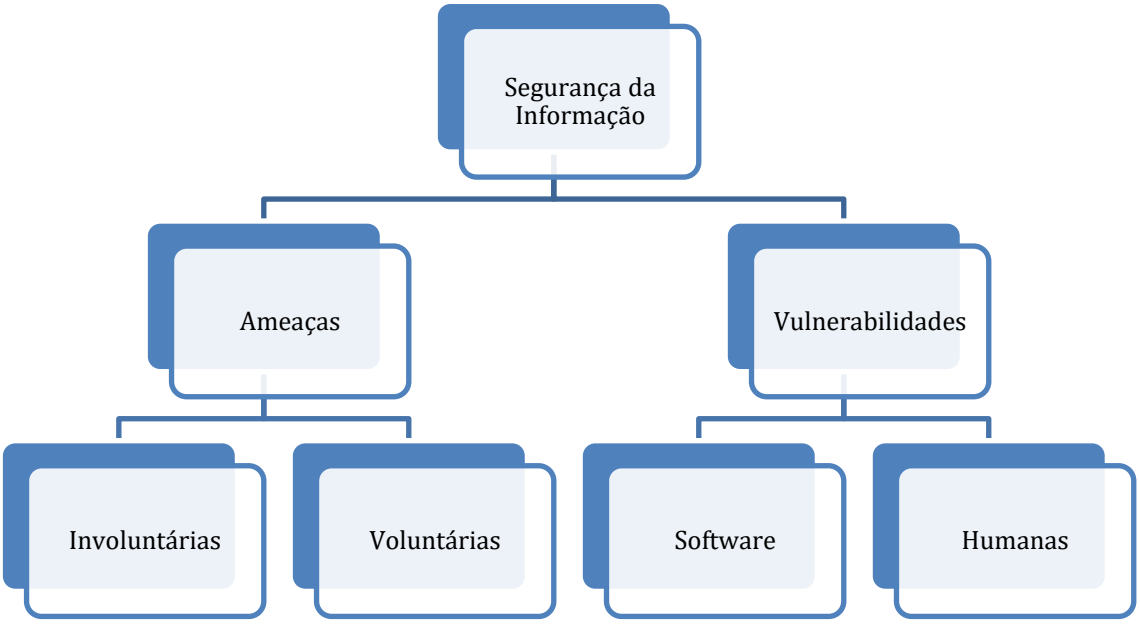
Para Sêmola (2003), a segurança total não existe e a empresa é a encarregada de decidir o nível de segurança que será implementado na organização. Dessa forma, a segurança da informação é definida como uma área do conhecimento que visa proteger os ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Também é possível “[...] considerá-la como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação.” (SÊMOLA, 2003, p. 43).

Sêmola (2003) destaca que as ameaças e vulnerabilidades da segurança da informação estão ligadas ao fator humano. As ameaças são agentes ou condições que comprometem os três conceitos da segurança da informação. Entre elas, cita-se as ameaças involuntárias, que costumam ser causadas por erros, acidentes e desconhecimento das pessoas na codificação e configurações de *softwares*, e as ameaças voluntárias frequentemente derivadas da ação de *hackers*, invasores de sistemas, disseminadores de vírus de computador, entre outros.

As vulnerabilidades, elementos passivos que dependem de um agente ou condição favorável para provocar incidentes, são fragilidades associadas a ativos que podem ser exploradas por ameaças. Como exemplo de vulnerabilidades podem ser citadas as de *software* e as humanas. As vulnerabilidades de *software* podem acarretar acessos indevidos, vazamentos de dados, perdas de dados ou indisponibilidade oriundos de erros na instalação ou configuração de programas. Dentre as vulnerabilidades humanas, alguns elementos merecem destaque. São eles, a falta de treinamento, o compartilhamento de dados confidenciais e a não

execução de rotinas de segurança. A Figura 1 a seguir representa os conceitos abordados em uma visão hierárquica:

Figura 1 - Ameaças e Vulnerabilidades da Segurança da Informação



Fonte: adaptado de Sêmola (2003)

Ainda na questão de segurança da informação, Souza (2020) define três categorias fundamentais que conduzem os seus procedimentos: Pessoas, Processos e Tecnologia. Sendo assim, a tecnologia é fundamental, porém incapaz de evitar todos os problemas se não estiver acompanhada de processos definidos, estudos de vulnerabilidade e pessoal capacitado para manter o ambiente seguro.

Considerando que empresas e organizações trabalham com diversos tipos de dados, sobretudo dados pessoais, e a interferência humana nos processos é considerada uma vulnerabilidade no contexto da segurança da informação, é importante estar atento e conhecer as formas de proteção desses tipos de dados pessoais.

3.3 PROTEÇÃO DE DADOS PESSOAIS

Esta seção abordará o tema proteção de dados pessoais. As definições de dados pessoais serão apresentadas, contendo discussões sobre conceitos e abordagens diferentes encontradas na literatura.

Após, em posse das definições, será feita discussão específica sobre a proteção de dados pessoais.

3.3.1 Dados Pessoais – definição

O entendimento de dados pessoais pode variar conforme a aplicação, seu uso e formas de disseminação, neste contexto, resgata-se algumas definições de dados pessoais conforme a Lei Geral de Proteção de Dados Pessoais (LGPD). Segundo a LGPD, existem três tipos de dados (Quadro 1):

Quadro 1 – Tipos de dados segundo a LGPD

Tipo de dado	Definição
Pessoal	Informação relacionada a pessoa natural identificada ou identificável
Pessoal sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
Anonimizado	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

Fonte: adaptado de Brasil (2018a).

É possível citar como exemplo de dados pessoais aqueles que normalmente fornecemos em um cadastro como: nome, RG, CPF, gênero, data e local de nascimento, filiação, telefone, endereço residencial, cartão ou dados bancários. Além disso, os dados pessoais podem ser algumas informações que nem sempre fornecemos de forma consciente, como localização via GPS, retrato em fotografia, prontuário de saúde, hábitos de consumo, endereço de IP (Protocolo da Internet) e *cookies*. (PARANÁ, [202?a]).

Em uma abordagem diferente, Vainzof (2020) divide dados pessoais em indiretos e diretos, exemplificando-os conforme o Quadro 2:

Quadro 2 - Tipos de dados segundo Vainzof

Tipo de dado	Definição
Pessoal direto	Identifica diretamente uma pessoa natural, sem a necessidade de outras informações, como CPF, título eleitoral, nome (se não houver homônimos)
Pessoal indireto	Torna a pessoa natural identificável, mas necessita de informações adicionais para identificá-la, como gostos, interesses, hábitos de consumo, profissão, sexo, idade e geolocalização

Fonte: adaptado de Vainzof (2020).

Dentre os tipos de dados citados, a LGPD atribuiu uma importância maior aos dados pessoais caracterizados como sensíveis. Essas informações tratadas anteriormente, são as que costumam ser compartilhadas sem a ciência ou, até mesmo, o consentimento do titular. O consentimento é definido pela LGPD, no art. 5º, inc. XII da seguinte forma: “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.” (BRASIL, 2018a). A LGPD não tem como objetivo impedir o tratamento de dados, mas criar mecanismos de proteção garantindo que os dados sejam tratados de maneira adequada e sejam utilizados para fins lícitos e com a ciência e consentimento do cidadão.

Sobre a relevância dos dados pessoais indiretos, Vainzof (2020) faz alguns apontamentos. Tendo em vista o serviço de geolocalização, presente em diversos dispositivos como *smartphones* e em *chips* instalados em automóveis, a partir da análise dos dados de geolocalização, é possível traçar o comportamento do titular destes dispositivos através do número de vezes, do tempo despendido e dos dias da semana em que determinado lugar foi frequentado.

Sendo assim, os dados pessoais indiretos, os quais não são capazes de identificar o titular por si só, tem o potencial de se tornarem dados sensíveis quando as inferências, mesmo incorretas, a respeito da origem racial ou étnica do indivíduo, convicção religiosa, opinião política, dados referentes a saúde, entre outros são realizadas. Com o objetivo de reduzir o número de inferências incorretas, decorrentes do processamento de dados em larga escala por meio de sistemas automatizados, cabe o uso do princípio da qualidade dos dados que rege “[...] a garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.” (BRASIL, 2018a).

Complementando as definições vistas, a Lei Geral de Proteção de Dados (LGPD) entende que existem dados pessoais que exigem maior atenção no tratamento, aqueles relacionados a crianças e adolescentes (BRASIL, 2022c). Assim, quanto ao consentimento dos responsáveis sobre as crianças e adolescentes, a LGPD estabelece que:

> Quando o dado corresponder a menores de idade, é imprescindível obter o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal e se limitar a pedir apenas o conteúdo estritamente necessário, sem repasse a terceiros. (BRASIL, 2022c).

A coleta de dados pessoais de menores sem o consentimento pode apenas ocorrer quando os dados forem necessários para contatar os pais ou responsável legal, podendo ser utilizados uma única vez e sem armazenamento, ou para a sua proteção. Em nenhum caso poderão ser repassados para terceiros sem o consentimento dado por pelo menos um dos pais ou responsável legal (BRASIL, 2022c).

Já em relação ao tratamento dos dados sensíveis, o processo depende do consentimento explícito do titular dos dados e de um fim definido. O tratamento desses dados sem consentimento será possível exclusivamente quando a informação for indispensável para situações relacionadas a uma obrigação legal, a políticas públicas, a estudos via órgão de pesquisa, ao exercício regular de direitos, à preservação da vida e da integridade física de uma pessoa, à tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária e à prevenção de fraudes contra o titular (BRASIL, 2022c).

A respeito dos dados anonimizados, entende-se que eles não são dados pessoais, uma vez que o titular não pode ser identificado. Ou seja, a partir do uso de meios técnicos disponíveis na ocasião do seu tratamento, "[...] o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo [...]" (VAINZOF, 2020). Considerando isso, Vainzof (2020) aponta que: “É uma contradição utilizar o termo “dado anonimizado pessoal”, pois, se anonimizado, ele perde a característica de ser pessoal.”.

3.3.2 Proteção de dados pessoais

A proteção de dados pessoais teve sua origem na transformação do direito à privacidade que passou a ocorrer a partir do final do século XIX, onde a discussão desse assunto se tornou recorrente, pois, na época, a fotografia, os jornais e aparatos tecnológicos começaram a invadir os sagrados domínios da vida privada e doméstica e passaram a possibilitar o acesso e a divulgação de fatos pertencentes à vida privada do indivíduo de uma forma nunca antes vista. (MENDES, 2011).

Assim, Mendes (2011, p. 3) mostra que:

> A transformação desse conceito pode ser percebida de forma mais clara a partir da década de 70, com a edição de legislações específicas e de decisões judiciais de diversos países, bem como a partir da aprovação de acordos internacionais e transnacionais em diferentes níveis. Todos esses instrumentos compartilham o conceito segundo o qual os dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela forte.

Compreender a diferença entre vida privada, privacidade e intimidade é necessário, pois trata-se de um assunto que merece atenção em decorrência das diferentes interpretações que esses conceitos podem ter. Para Martins (2020), esses três termos não devem ser usados como sinônimos, pois vida privada é entendida "[...] como a esfera que as pessoas possuem mais acesso à informação, acontecimentos de vida, vontades e afazeres do indivíduo, que opta por dividir com seus conhecidos e familiares distantes." (MARTINS, 2020, p. 20).

Por outro lado, a privacidade é definida como algo confidencial e íntimo, se constituindo de assuntos que o indivíduo compartilha apenas com amigos e familiares próximos. Já a intimidade, é tudo aquilo que não é dividido com ninguém, pois representa os valores mais secretos e intrínsecos do indivíduo. (MARTINS, 2020). Complementando, Martins (2020) traz um outro ponto de vista, baseado na Constituição Federal, que atribui um mesmo significado para os termos apresentados. Dessa forma, a Constituição Federal, no art. 5º, inc. X, determina que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação." (BRASIL, 1988).

Quando a proteção de dados pessoais é discutida, o foco se volta às soluções tecnológicas existentes enquanto o fator humano não recebe a atenção necessária. Como golpes de engenharia social visam se aproveitar da falha da vítima para a obtenção de dados sensíveis, é essencial que os usuários da *web* saibam agir diante destas ameaças. Como afirmam Freire, Silva e Queiroz (2017, p. 155), "Soluções definitivas são praticamente impossíveis. O comportamento humano é constantemente mutável e imprevisível.".

De posse dessas informações, cabe ao usuário da *web* tomar certos cuidados que podem ajudá-lo a se prevenir de golpes ou ter seus dados vazados na rede mundial de computadores. Segundo o Guia criado pelo Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a Autoridade Nacional de Proteção de Dados (ANPD) e a Secretaria Nacional do Consumidor (SENACON), as seguintes estratégias são fundamentais para a proteção de dados pessoais (BRASIL, 2022?a):

a) criar *backups* dos dados armazenados, principalmente em nuvem;
b) ativar a criptografia nos discos e mídias externas, como *pen drives*;
c) criar senhas fortes combinando caracteres especiais, letras maiúsculas e minúsculas e números evitando o uso de palavras comuns ou dados pessoais;
d) habilitar a verificação de senhas em duas etapas sempre que possível, principalmente em sistemas de armazenamento em nuvem e aplicativos de mensagens;
e) instalar aplicativos somente de fontes e lojas oficiais;
f) sempre manter o sistema operacional e aplicativos atualizados;
g) desconfiar de *links* recebidos por aplicativos de mensagens;
h) limitar a divulgação ou fornecimento de dados pessoais na Internet, inclusive em redes sociais, ou para empresas, aos casos estritamente necessários.

Algumas outras medidas complementares são relevantes e podem ser implementadas, como evitar redes Wi-Fi públicas, pois *hackers* podem utilizar ferramentas para captura dos dados que trafegam entre o dispositivo da vítima (celulares, *notebooks*, entre outros) e o roteador de uma rede que não exija autenticação para acessá-la (10 FORMAS, 2019).

Outra questão a se considerar é no uso de computadores públicos. Após usar contas de *e-mail* ou redes sociais nesses computadores, é de fundamental importância efetuar o *logout*, ou seja, encerrar a sessão desses serviços para evitar que dados fiquem armazenados nestes dispositivos.

Outras situações também merecem a atenção do usuário, como os riscos que as lojas *on-line* podem oferecer. Com a popularização de *sites* de compra, é necessário tomar alguns cuidados, por exemplo: buscar avaliações de outros compradores, preferir lojas bem conhecidas e se atentar se o endereço da loja *online* é um ambiente seguro, geralmente iniciado por “https://” ou quando há a presença do ícone de um cadeado, indicando que o site possui um certificado válido de segurança. *Sites* que solicitam muitas informações sem deixar claro qual será o uso

desses dados podem não ser confiáveis. Nesse caso, a atenção deve ser redobrada quando informações financeiras, como o número de cartão de crédito, são pedidas.

Figura 2 - HTTPS e cadeado na barra de endereço de um website

Fonte: Mozilla (2022).

Com o grande volume de dados ao qual a sociedade tem acesso e a facilidade em criar e compartilhar informação nos dias atuais, é importante saber que a Internet está repleta de boatos e notícias falsas, ou seja, compartilhar tudo o que é recebido via *e-mail*, redes sociais ou aplicativos de mensagem não é uma boa ideia. Mesmo que o remetente seja conhecido, estes tipos de conteúdo podem conter *links* para *sites* falsos ou *malwares*, que tem por objetivo capturar dados, enquanto se disfarçam de um serviço novo ou uma petição *on-line*, por exemplo.

De acordo com Demartini (2022), é de grande importância desconfiar de contatos por ligações, *e-mails* e mensagens em aplicativos ou redes sociais, prestando atenção para verificar se os remetentes, *sites*, domínios, perfis e telefones são oficiais. Caso a verificação não possa ser feita, não é recomendável responder ao contato. Além disso, é essencial manter o telefone e serviços protegidos com autenticação biométrica. As credenciais devem ter um alto nível de complexidade e ser diferentes umas das outras visando que, caso uma credencial seja vazada, isso não comprometa as demais. Por fim, é fundamental controlar as publicações em redes sociais de modo a evitar que os bandidos obtenham informações pessoais sobre vítimas potenciais, as quais podem ser familiares e amigos.

De acordo com 10 Formas (2019), ainda em relação à proteção de dados pessoais, porém considerando casos específicos, é recomendado evitar responder provocações e ameaças na Internet, visto que, é muito comum entrevistadores de empresas realizarem pesquisas nas redes sociais para conhecerem os perfis dos candidatos.

Além das formas de proteção de dados pessoais citadas acima, ressalta-se que o cidadão pode e deve incorporar em sua rotina cuidados com seus dados, e conhecer a legislação vigente no Brasil. Questão essa tratada a seguir.

3.4 LEGISLAÇÃO SOBRE PROTEÇÃO DE DADOS PESSOAIS

De acordo com Paraná ([202?b]), a Lei Geral de Proteção de Dados (LGPD), Lei n° 13.709/2018 rege fundamentalmente o tratamento de dados, atividade que utiliza dados pessoais na execução da sua operação. As atividades caracterizam-se em coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Como é explicado no Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor: “A LGPD concretiza direitos previstos na Constituição Federal de 1988 e complementa a proteção conferida pelo Código de Defesa do Consumidor e pelo Marco Civil da Internet.” (BRASIL, 2022a).

O tratamento de dados pode ser feito por dois agentes, o Controlador e o Operador. Ao Controlador, cabe a função de tomar as decisões referentes ao tratamento de dados pessoais. Tanto o controlador quanto o operador podem ser pessoa natural física ou jurídica, de direito público ou privado. O Controlador também indica a pessoa denominada como Encarregado, a qual atua como canal de comunicação entre o Controlador, o Operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Ao Operador é designada a função de realizar o tratamento de dados pessoais em nome do controlador (BRASIL, 2022b).

A LGPD criou obrigações e padrões para quem trata dados pessoais e instituiu a Autoridade Nacional de Proteção de Dados (ANPD), responsável por

regular a coleta, o uso, o processamento e o compartilhamento de dados no país. As obrigações e padrões a serem seguidos estão disponíveis no Guia de Boas Práticas para Implementação na Administração Pública Federal da Lei Geral de Proteção de Dados, documento elaborado pelos órgãos que compõem o Comitê Central de Governança de Dados e orienta as atribuições e atuação do Controlador, do Operador, do Encarregado e da Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2022b).

Sendo assim, a qualidade do tratamento de dados é essencial. Caso a má conduta do operador cause algum prejuízo ao titular dos dados, a LGPD diz que:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (BRASIL, 2018a).

Como já visto, a Lei Geral de Proteção de Dados (LGPD), expõe as diretrizes sob as quais a coleta, o tratamento de dados e o uso das informações devem ser realizados, de modo a proteger a privacidade das pessoas físicas e jurídicas de direito público ou privado. Sendo assim, empresas ou instituições que têm as suas informações armazenadas vazadas a partir de falhas de segurança no tratamento de dados por parte do Controlador e/ou do Operador, podem sofrer consequências como ações judiciais individuais ou coletivas, sanções administrativas, perdas financeiras e danos de reputação e imagem. A organização também deverá responder caso as informações vazadas sejam utilizadas para fins ilícitos que causem prejuízo aos titulares dos dados (BARROS; CORT, 2021). Para melhor compreensão, Brasil (2020) caracteriza Controlador como o órgão contratante e o Operador como a empresa contratada para o tratamento de dados pessoais.

Sobre isso, o artigo 44 da LGPD diz o seguinte: “Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.” (BRASIL, 2018a).

É possível observar, portanto, que a LGPD cobre a questão de vazamento de dados, quando a proteção dos dados é violada, porém as técnicas de *phishing* não

estão cobertas pela Lei, já que nesse tipo de situação, a vítima acaba entregando voluntariamente os seus dados para o criminoso, o que não se caracteriza como um vazamento de informações. Dessa forma, mesmo que o cibercriminoso esteja se passando por uma empresa, por exemplo, a instituição não pode ser responsabilizada legalmente pelo crime, pois esta situação não é interpretada como uma falha de segurança (BARROS; CORT, 2021).

No Brasil ainda não há legislação específica sobre crimes cibernéticos, mesmo assim, vale ressaltar que já existem algumas leis que visam coibir esses tipos de crimes. Nesse sentido, em 2012, entrou em vigor a Lei 12.737, conhecida por “Lei Carolina Dieckmann” que criminaliza a invasão de dispositivos informáticos, conectados ou não à rede a fim de obter, adulterar ou destruir dados ou informações sem o consentimento do titular do dispositivo.

Em 2014, O “Marco Civil da Internet”, Lei nº 12.965, passou a vigorar. A Lei estabelece princípios, como o da proteção da privacidade e dos dados pessoais, garantias, direitos e deveres para o uso da Internet no Brasil, introduzindo, por exemplo, o conceito de neutralidade da rede, o qual garante o tratamento isonômico dos pacotes de dados que trafegam pela rede de computadores. Também estabelece a guarda, em sigilo, dos registros de conexão pelos provedores de Internet durante o período de um ano, os quais só poderão ser disponibilizados mediante autorização judicial.

Em dezembro de 2021, o diretor da ANPD, Arthur Sabbat, em um Seminário transmitido virtualmente pelo *site* e-Democracia[2], que discutia o papel do Parlamento no combate aos crimes cibernéticos, afirmou que durante a pandemia, no período de 2020 a 2021, houve um aumento de 300% na incidência de crimes cibernéticos. No início, esses crimes estavam voltados a diversos órgãos públicos e instituições privadas e possuíam uma característica letal, sem alvos preferenciais. Já da metade para o final de 2020, os ataques começaram a se voltar contra os cidadãos, aqueles tratados como titulares de dados pessoais pela LGPD (BRASIL, 2021).

[2] https://edemocracia.camara.leg.br/

> De acordo com pesquisa da Federação Brasileira de Bancos - Febraban, os registros de tentativas de golpes pela internet aumentaram cerca de 70% nesse período. Os criminosos usam links de bancos para fisgar os consumidores e roubar dados. (BRASIL, 2021).

Sendo assim, visando coibir o aumento do número de crimes cibernéticos impulsionado pela pandemia do novo coronavírus, foi publicada a Lei nº 14.155/2021, que alterou o Código Penal e o Código de Processo Penal para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela Internet e definir a competência em modalidades de estelionato.

A proteção de dados pessoais passou a ser considerada um direito fundamental a partir da Emenda Constitucional 115/2022, promulgada em 10 de fevereiro de 2022, tendo em vista que o direito à privacidade e à proteção de dados pessoais garante a dignidade da vida humana, primordialmente no contexto de inserção total na vida digital (BRASIL, 2022a).

Nesse sentido, é relevante discutir outros direitos relacionados à privacidade e aos dados pessoais e que também vêm à tona quando se considera os ambientes digitais, a facilidade de criação e compartilhamento de informação, bem como o volume excessivo de informação ao qual a sociedade em rede está exposta. Assim, um dos direitos que vem sendo alvo de discussão em diversos países nos últimos anos, é o direito ao esquecimento, que será abordado a seguir.

3.5 DIREITO AO ESQUECIMENTO E O SUPERINFORMACIONISMO

O direito ao esquecimento é um recurso que visa conter a divulgação de dados indesejados, tratando da possibilidade de desconsideração e abstração de fatos vexatórios ocorridos no passado. O tema vem sendo discutido há vários anos nos países europeus, bem como nos Estados Unidos em decorrência da era da informação, onde a facilidade na divulgação de conteúdos pessoais é predominante. Assim, informações referentes à intimidade, vida privada, imagem, nome ou memória das pessoas podem facilmente ferir ou causar situações prejudiciais. Em casos como esse, o direito ao esquecimento passa a ser cogitado como recurso para conter a divulgação de dados indesejados (SABBATINI; GOBATO, 2021).

Nesse sentido, Barros (2022) aponta a importância do direito ao esquecimento como o “[...] direito de ser deixado em paz [...]” (BARROS, 2022, p. 10) na era da superinformação, uma vez que a Internet eterniza notícias e informações, este direito mostra ao indivíduo que é possível controlar o que deve ou não ser exibido sobre as suas vidas no ambiente virtual, visando não permitir que algum fato possa prejudicá-lo durante sua vida.

De acordo com Sabbatini e Gobato (2021), a Internet se mostra como um grande desafio em relação ao direito ao esquecimento, já que a rede mundial de computadores cria um ambiente propício para a divulgação de informações ao ponto de se tornar inviável a identificação do número exato de compartilhamentos principalmente quando se considera a quantidade de usuários e visualizações que as plataformas de mídias sociais, como *Instagram*, *Facebook*, *YouTube*, *Whatsapp*, entre outros, possuem. Esse fenômeno ocorrido a partir existência desses diversos canais de comunicação, que além de serem usados para a criação, distribuição, manipulação e integração, possibilitam que os inúmeros usuários propaguem a informação, é denominado superinfomacionismo. Dessa forma, as pessoas, mesmo sem querer, acabam sendo bombardeadas por informação e se tornam sujeitas à exposição, uma vez que a sociedade é incessantemente alimentada por enormes quantidades de fatos e dados.

Assim sendo, Barros (2022) afirma que há lacunas legislativas no que se refere a proteção efetiva de quem usa a Internet. O cenário digital resultante do avanço tecnológico vem tornando a violação da vida privada cada vez mais comum. A Internet possibilita que, em poucos segundos, o acesso a fotos, notícias, documentos e qualquer outra informação sobre uma pessoa seja feito com quase nenhuma dificuldade.

Sabbatini e Gobato (2021) mencionam que, embora o Brasil seja considerado um país atrasado em relação a discussão desse direito, a aplicabilidade do estudo do direito ao esquecimento já foi pauta de julgamentos. No entanto, o tema abordado pelo Supremo Tribunal Federal foi julgado como incompatível à Constituição por decisão majoritária, pois ficou entendido que não haveria a possibilidade de extrair uma interpretação do texto normativo capaz de não restringir

o exercício de outros direitos fundamentais, como o direito de liberdade de manifestação e de liberdade de imprensa.

A exposição excessiva causada, em grande parte, pelas plataformas de mídias sociais pode canalizar a ocorrência de delitos nos ambientes virtuais. Como será abordado na próxima seção, alguns crimes que não dependem necessariamente do espaço virtual para ocorrer, utilizam-se das tecnologias da informação e o acesso facilitado a fatos e dados para atentar contra a honra, a vida ou a integridade física.

3.6 CRIMES CIBERNÉTICOS (CIBERCRIMES)

Crimes cibernéticos ou cibercrimes são atividades criminosas praticadas no ambiente virtual. Geralmente têm como motivação o dinheiro, porém menos frequentemente, podem ocorrer tendo em vista a destruição da reputação de uma pessoa, empresa ou ser usado para fins políticos, por exemplo. Os crimes cibernéticos podem ser cometidos por indivíduos ou organizações. Alguns cibercriminosos possuem vasta experiência, muito conhecimento técnico, alto nível de organização e utilizam-se de técnicas avançadas enquanto outros são hackers iniciantes. (KASPERSKY, 2022?).

Nesse sentido, Zambonato (2022) entende como crime cibernético toda ação ilegal que se utiliza de recursos tecnológicos como meio para a prática delituosa afetando pessoas, computadores ou seus sistemas (ZAMBONATO, 2022). Assim, é destacada a necessidade de classificar estas atividades criminosas dada realidade tecnológica emergente onde “[...] novas ações lesivas surgem em um ritmo acelerado [...]” (ZAMBONATO, 2022 p. 12). De acordo com Zambonato (2022), os crimes cibernéticos são classificados de duas formas: crime cibernético próprio e crime cibernético impróprio.

Os crimes cibernéticos próprios são aqueles que dependem do espaço virtual para serem praticados e consumados. Em outras palavras, estão necessariamente relacionados com a utilização de sistemas informáticos. Desse modo, o criminoso visa atingir principalmente sistemas informatizados ou de telecomunicações de dados, usando-os como objeto e meio para atingir o seu objetivo. É possível

observar, portanto, que para este tipo de crime cibernético ocorrer, é esperado que o criminoso possua conhecimentos técnicos especiais e avançados em computação. Dentre os crimes que podem ser citados, estão os crimes de invasão de dispositivo informático, obtenção e transferência ilegal de dados e interceptação de sistemas eletrônicos (ZAMBONATO, 2022).

Por sua vez, os crimes cibernéticos impróprios são aqueles que já se encontram tipificados no código penal, porém são praticados com o auxílio da tecnologia. Alguns exemplos de crime desse grupo incluem, os crimes de calúnia, injúria, difamação, ameaça, falsidade ideológica, estelionato, pornografia infantil e todos os demais delitos passíveis de serem praticados com a utilização da tecnologia de informação. Dessa forma, nos crimes impróprios, a ameaça deixa de estar voltada contra a integridade da rede internacional de computadores, seus sistemas ou equipamentos de informática e volta-se contra a honra, a vida ou a integridade física.

Em síntese, o que diferencia as classificações de crimes cibernéticos vistas são os meios necessários para a realização do crime e o que está sendo lesado ou posto em perigo (ZAMBONATO, 2022).

3.6.1 Tipos de cibercrimes

Segundo Paz Mendes Sociedade de Advogados (2021), os tipos mais comuns de cibercrimes são:

a) invasão de dispositivos para disseminação de vírus e *malware*;
b) distribuição de material pornográfico e pedofilia.
c) violação de propriedade intelectual;
d) falsificação de dados financeiros, documentos particulares ou cartões de crédito;
e) extorsão cibernética;
f) ataques de *ransomware*;
g) cryptojacking;
h) interrupção ou perturbação em *sites*;
i) golpes e fraudes perpetuados por meio de redes sociais;

São consideradas invasões de dispositivos de informática quando dispositivos são infectados por *malware* para danificá-los ou fazê-los parar de funcionar. Os *malwares* também podem ser usados para excluir ou roubar dados. Os *hackers*, também conhecidos como cibercriminosos, frequentemente infectam computadores com vírus e os fazem espalhar a infecção para outras máquinas da rede. Assim, as máquinas infectadas podem ser utilizadas para cometer uma infinidade de crimes, tais como a própria disseminação de *malware*, a distribuição de conteúdo ilegal ou o armazenamento de dados roubados. (KASPERSKY, 2022).

Sobre a distribuição de material pornográfico e pedofilia, é previsto crime quando o material pornográfico é gerado e compartilhado sem o consentimento da vítima, em casos de estupro (BRASIL, 2018b). Em relação a pedofilia, também constitui crime o armazenamento de material envolvendo criança ou adolescente (BRASIL, 1990).

Os cibercrimes de violação de propriedade intelectual acontecem na utilização de elementos visuais distintivos ou até mesmo sonoros de empresas ou organizações que possuem patentes expedidas pelo Instituto Nacional da Propriedade Industrial (INPI) ou similares internacionais. Uma das estratégias utilizadas nos golpes de *phishing* é clonar ou criar *sites* muito semelhantes aos reais para enganar as suas vítimas. Destaca-se que somente os detentores possuem direito sobre suas criações e invenções e que para utilizá-las é necessário contratos de licenciamento. O uso não autorizado de características de uma marca de modo

que possa gerar confusão na sua identificação se caracteriza como crime (REZENDE, 2022).

A falsificação de dados financeiros, documentos particulares ou cartões de crédito, é enquadrado no Art. 298 do Código Penal, Lei 2848, o qual considera crime: “Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro.” (BRASIL, 1940). Segundo a Lei nº 12.737/2012, cartões de crédito ou débito passaram a ser considerados documentos particulares (BRASIL, 2012).

A extorsão cibernética é um tipo chantagem onde é exigido dinheiro para evitar que um ataque se inicie. O *ransomware* é um tipo de *malware* usado para extorquir dinheiro, mantendo os dados de máquinas pessoais ou de empresas como reféns em troca de resgate. A infecção por este vírus, criptografa os dados e exige uma quantia, geralmente em criptomoedas, para que o resgate possa ser efetuado. Um caso famoso desse tipo de ataque por *malware*, ocorreu em 2017 com o *ransomware* “*WannaCry*”, que afetou computadores que executavam o sistema operacional Microsoft Windows, por meio de uma vulnerabilidade identificada pelos cibercriminosos. O ataque afetou 230.000 computadores em 150 países e foi estimada uma perda financeira, no mundo todo, de 4 bilhões de dólares americanos (KASPERSKY, 2022?).

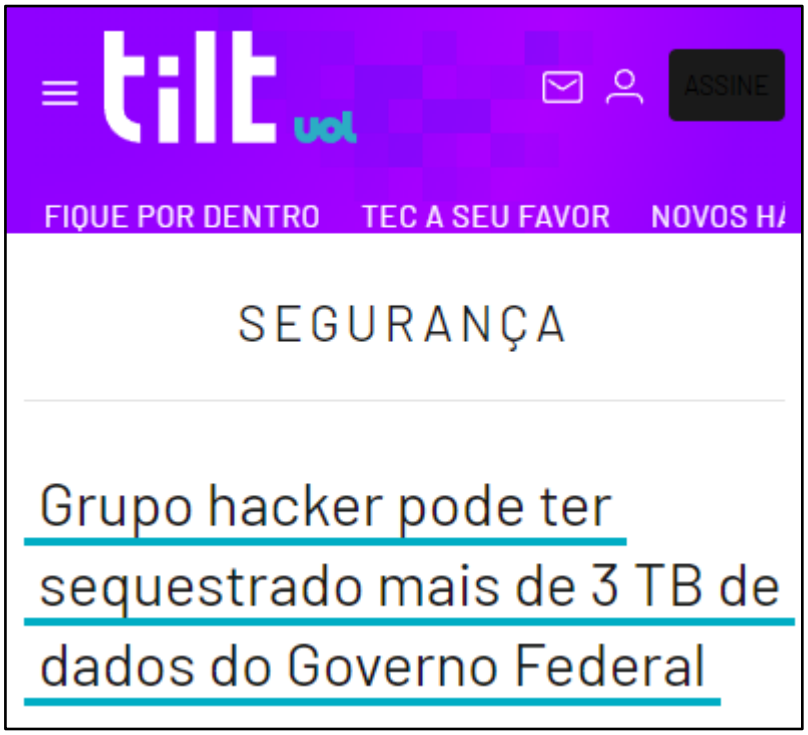
No Brasil, algumas notícias de ataques por *ransomware* em sistemas do governo, voltaram a atenção a esse tipo de crime. No final de 2021, um ataque *hacker* afetou diversos sistemas do ministério da saúde, incluindo o ConecteSUS que o deixou inacessível por quase duas semanas. A apuração do caso pela Polícia Federal, a partir da operação *Dark Cloud*, entretanto, começou em agosto de 2022 e o grupo suspeito do ataque, porém não mencionado pelas autoridades policiais, foi o Lapsus$ Group. Esse grupo *hacker* já era conhecido por atacar diversas organizações ao redor do mundo, inclusive a Microsoft (ALECRIM, 2022).

Figura 3 - Notícia sobre ataque *hacker* ao ConecteSUS

Fonte: Alecrim (2022).

Também em agosto de 2022, um grupo *hacker* intitulado como “Everest” disponibilizou, na *deepweb*, uma rede que torna mais difícil o rastreamento dos seus usuários, a compra de 3TB de dados do Governo Federal aos interessados. Nesse caso específico, os cibercriminosos optaram pela venda dos dados interceptados em vez de pedir o resgate para a vítima do ataque. Apesar isso, o Serviço Federal de Processamento de Dados (SERPRO) informou que os sistemas continuaram em plena operação e que não houve indícios de crime cibernético nas bases de dados (MANNARA, 2022).

Figura 4 - Notícia sobre ataque *hacker* ao Governo Federal



Fonte: Mannara (2022).

Em relação às criptomoedas, existe o *cryptojacking*, crime onde um dispositivo após ser infectado, passa a minerar criptomoedas de forma não autorizada, ou seja, o cibercriminoso utiliza o poder de processamento do dispositivo invadido para gerar lucros a si mesmo (MALWAREBYTES, 2022?).

Outra atividade comum é a interrupção ou perturbação em sites. De acordo com Kaspersky (2022?), nesse tipo de crime, os criminosos podem fazer os usuários dos dispositivos ficarem impedidos de utilizar um *site* ou rede e impossibilitar que uma empresa forneça serviços aos seus clientes, o que é chamado de ataque de negação de serviço ou *Denial of Service* (DoS). Uma variação desse tipo de ataque de negação de serviço, o DDoS, *Distributed Denial of Service* ou ataque de negação de serviço distribuído, segundo Brasil (2023) “[...] acontece de forma similar ao DoS, porém, ele ganha algumas camadas extras, onde um computador mestre pode gerenciar uma série de outros computadores zumbis, fazendo com que todas as máquinas envolvidas direcionem o ataque para um único alvo, sobrecarregando-o.”. Dessa forma, “Dependendo da proporção do ataque, um servidor alvo pode ser inundado por um tráfego muito maior do que o enviado pelo atacante ao serviço

vulnerável, tendo como consequência o esgotamento de seus recursos de processamento e/ou indisponibilidade.” (BRASIL, 2023).

De acordo com Ataques (2022), o número de ataques DDoS dobrou no Brasil em consequência do período eleitoral de 2022. Entre 1º de julho e 31 de agosto, cerca de 225 mil *sites* foram atacados, atingindo agências governamentais, de notícias, instituições educacionais e operadoras de comunicação. Os alvos principais foram instalações críticas e áreas governamentais, sendo as operadoras de fibra ótica o setor mais afetado.

Golpes e fraudes perpetuados por meio de redes sociais são bastante recorrentes. Os golpistas têm como objetivo enganar as vítimas nestes meios digitais através de diversas técnicas como o uso de dados públicos para criar contas falsas ou *phishing*, utilizado para obter informações sigilosas como dados bancários, ou de cartões de crédito (MANZZI, 2022).

Complementam a lista de crimes cibernéticos o crime de roubo de identidade, que segundo Demartini (2022), ocorre quando os golpistas, utilizando-se de técnicas de engenharia social, se passam por instituições, órgãos governamentais ou colaboradores de empresas, induzindo as vítimas a compartilharem seus dados. Pessoas com maior dificuldade, principalmente idosos, costumam ser o alvo principal desses cibercriminosos. Dessa forma, esse tipo de crime pode trazer às vítimas os seguintes problemas:

> De posse de informações pessoais, por exemplo, eles podem pedir empréstimos ou realizar cadastros. Caso o volume vazado tenha dados de cartão de crédito, as compras fraudulentas são o principal reflexo. E na soma de tudo isso, golpes podem ser realizados na tentativa de invadir sistemas bancários, redes sociais e e-mails em busca de mais ganhos furtados e golpes (DEMARTINI, 2022).

3.6.2 *Malware*

Conforme Garrett (2021), *malware* é um termo derivado da fusão de “*malicious*” – “malicioso”, em inglês – com “*software*” e é definido como qualquer tipo de programa indesejado. Nesse grupo estão inclusos: vírus, *ransomware*, *worms*, *trojans*, *rootkits*, *adwares* e vários outros. Embora todo o vírus de computador seja um *malware*, o contrário não é verdadeiro. Vírus é um termo mais antigo, datado da

década de 1990 que define as ameaças virtuais com alta capacidade de reprodução. Por não conseguir mais classificar os *softwares* maliciosos, que tem comportamentos específicos e causam problemas diversos, o termo vírus tem caído em desuso optando-se, dessa forma, por classificar cada ameaça conforme o seu modo de operação e aplicação.

Os crimes cibernéticos ocorridos a partir da disseminação e infecção por *malware* merecem destaque, pois são bastante recorrentes, afetando desde dispositivos domésticos de usuários comuns até servidores e outros equipamentos de organizações governamentais e empresas multinacionais, que regularmente armazenam e processam dados sensíveis próprios da organização, de clientes ou de cidadãos.

De modo a identificar e definir conceitos sobre a proteção de dados pessoais, foram realizadas pesquisas nas seguintes bases de dados: Base de dados de Periódicos em Ciência da Informação (Brapci), Google Acadêmico e SciELO, identificando 15 documentos, os quais foram extraídos os principais conceitos da temática.

Serão apresentados os resultados da pesquisa em um quadro contendo os termos obtidos no levantamento bibliográfico, bem como as definições da literatura para esses termos.

No Quadro 3 abaixo estão destacados os termos e definições para o tema proteção de dados pessoais.

Quadro 3 - Conceitos e definições da proteção de dados pessoais

Conceito	Definição
Dados Pessoais	“Informação relacionada a pessoa natural identificada ou identificável.” (BRASIL, 2018a). “São considerados dados pessoais aqueles que comumente fornecemos em um cadastro, como nome, RG, CPF, gênero, data e local de nascimento, filiação, telefone, endereço residencial, cartão ou dados bancários.” (PARANÁ, [202?a]).
Consentimento	“Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.” (BRASIL, 2018a).
Direito ao esquecimento	“O direito ao esquecimento, considerado por muitos um desdobramento do princípio da dignidade da pessoa humana, trata da possibilidade de desconsideração e abstração de fatos vexatórios ocorridos no passado, entendidos como danosos à índole e à privacidade do indivíduo.” (SABBATINI; GOBATO, 2021).
Dado anonimizado	“Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.” (BRASIL, 2018a). "[...] o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo [...]" (VAINZOF, 2020).
Tratamento de dados	“Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (BRASIL, 2018a).
Controlador de dados	“Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.” (BRASIL, 2018a).
Operador de dados	“Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.” (BRASIL, 2018a).

Fonte: elaborado pelo autor.

Na próxima seção será discutida a engenharia social, responsável por colocar em risco a proteção de dados pessoais, a partir da utilização de técnicas de manipulação.

3.7 ENGENHARIA SOCIAL

Nesta seção será abordado o seguinte objetivo do trabalho: b) analisar o conceito de engenharia social e as técnicas usadas para enganar usuários na Internet.

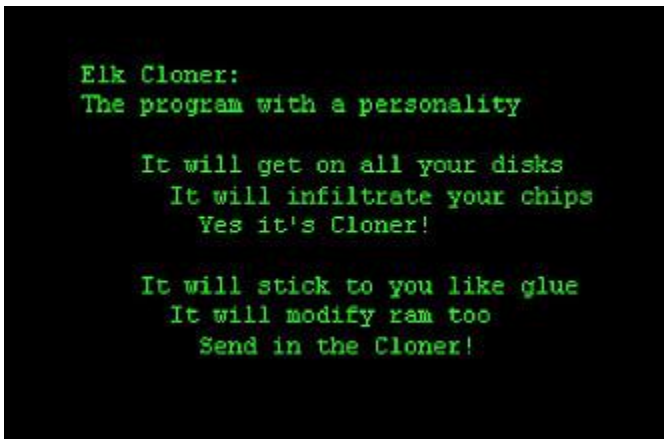
A engenharia social, técnica utilizada para induzir e enganar a vítima a fazer o que o criminoso deseja, dentre suas diversas aplicações, pode ser empregada para a obtenção de dados pessoais de maneira ilícita.

Um dos primeiros casos de engenharia social no ramo da computação e, provavelmente o mais famoso, aconteceu no ano de 1982, quando um estudante de 15 anos do ensino médio, nos Estados Unidos, criou o que passou a ser conhecido como o primeiro vírus de computador.

Rich Skrenta, criador do vírus “Elk Cloner” era integrante de um clube de computação, onde fazia cópias de *softwares* e compartilhava com seus amigos. Naquela época, era comum a troca de jogos e *software* por meio de discos. Pensando nisso, o jovem querendo fazer uma brincadeira, criou um programa feito para se propagar de disco para disco que rodava em segundo plano, verificando a presença de novos discos que, caso fossem encontrados, tinham seus arquivos modificados pelo programa (LEYDEN, 2012).

O resultado da infecção pelo vírus criado por Rich era um poema, conforme mostrado na Figura 5 abaixo:

Figura 5 - Mensagem exibida por "Elk Cloner"



Fonte: Meyer (2016).

Em português, o poema poderia ser lido de uma forma semelhante a essa:

Quadro 4 - Tradução da mensagem exibida por “Elk Cloner”:

Elk Cloner: O programa com personalidade Ele vai ficar em todos os seus discos Ele vai infiltrar seus chips Sim, é Cloner! Ele vai ficar grudar em você como cola Ele vai modificar sua RAM também Envie o Cloner!

Fonte: Leyden (2012, tradução nossa).

O código do programa não era exatamente malicioso porque embora causasse transtornos para quem tivesse seu disquete infectado, bastava reiniciar o sistema operacional para impedir que discos posteriormente inseridos no computador se mantivessem livres da ação do *software*.

A partir dessa breve história, verifica-se que a engenharia social é uma técnica que se baseia na manipulação de pessoas para obter acesso não autorizado a sistemas ou informações. Ao contrário do exemplo anterior, que tratava-se apenas de uma brincadeira, o principal objetivo da engenharia social é o de induzir o indivíduo a repassar os seus dados sensíveis ao golpista.

Alguns exemplos de dados visados por tais criminosos são senhas e *logins* pessoais e empresariais que podem ser utilizados em *sites* e banco de dados de empresas. A respeito disso, Conceição (2017) afirma que:

> A Engenharia Social usa a persuasão e o mérito de ser um bom comunicador, para enganar as pessoas. Há quem já tenha ouvido falar do termo no ambiente fora da rede, porém, além dos ataques por intermédio do discurso e exposição oral, o engenheiro social pode utilizar de suas artimanhas para induzir o indivíduo a disponibilizar senhas e *logins*, dentro de uma empresa, por exemplo, e repassar a um hacker, ou pode ser que o próprio atue nas duas funções. (CONCEIÇÃO, 2017, p. 2).

Retomando o caso “Elk Cloner”, é importante ressaltar que a engenharia social não ocorre somente nos meios digitais, tendo em vista que o criador do vírus

convenceu presencialmente suas “vítimas” a utilizarem o disco infectado. Uma vez que essa técnica depende apenas da capacidade de convencimento do golpista e da falta de atenção da vítima, a engenharia social pode ocorrer independentemente da forma de interação, seja ela presencial ou virtual. Assim, segundo Agência Brasileira de Inteligência (2021, p. 8): “Qualquer forma de interação pode ser um canal para o engenheiro social realizar sua ação: pessoalmente, por telefone, por e-mail ou até por meio de redes sociais.”.

Qualquer técnica de engenharia social depende de falha humana e devido ao grande volume de informações atualmente na *web*, ao qual as pessoas estão expostas, crimes digitais baseados em engenharia social podem ocorrer com qualquer indivíduo que tenha acesso a um terminal inteligente, como computadores e celulares (CONCEIÇÃO, 2017). Conceição (2017) ainda atribui a incidência de casos de engenharia social ao fácil acesso à tecnologia sem a devida instrução para o seu uso.

Agência Brasileira de Inteligência (2021) estabelece que a engenharia social ocorre quando há o convencimento da vítima, ou seja, as instruções dadas pelo criminoso precisam ser seguidas voluntariamente. Assim, a técnica de engenharia social não faz o uso de violência para atingir o seu objetivo e, além disso, pode ser aplicada tanto no contexto pessoal quanto no profissional. Engenheiros sociais podem explorar certas fragilidades sem que a vítima desconfie. Essas fragilidades são: a pressão de tempo, a pressão de autoridade e a empatia.

A pressão de tempo ocorre quando são criadas situações de prazo curto, causando uma sensação de urgência com o objetivo de incentivar uma ação rápida por parte da vítima. Um exemplo disso, são as mensagens que solicitam a atualização de dados bancários. Já a pressão de autoridade é muito eficiente em organizações hierarquizadas, pois o engenheiro social se identifica como alguém que trabalha para um funcionário de alto cargo dentro da organização enganando a vítima que pensa estar fornecendo informações a um superior. Por último, a empatia é a fragilidade explorada visando a disposição da pessoa em ajudar. O engenheiro social irá manipular a situação “de forma que ajudar seja a resposta natural e que recusar nos cause um sentimento de culpa.” (AGÊNCIA BRASILEIRA DE INTELIGÊNCIA, 2021, p. 10).

Dentre as várias formas de engenharia social, destaca-se o *phishing*, que será abordado na seção seguinte por ser uma das formas de engenharia social mais frequentes.

3.8 *PHISHING*

Nessa seção será abordado o seguinte objetivo do trabalho: c) caracterizar os tipos de *phishing* e apresentar a sua ameaça à proteção de dados pessoais.

O termo *phishing* é um neologismo da palavra "*fishing*" em inglês, que significa "pescaria", referindo-se aos golpes que tentam "fisgar" informações e dados pessoais. Teve sua origem por volta do ano de 1996, época da Internet discada, quando foi criada uma prática comum entre alguns usuários, a de utilizar geradores de cartão de crédito na criação de contas falsas na America Online (AOL) para se ter acesso ao serviço era realizada. Quando a empresa tomou ciência dessa estratégia, passou a implementar um sistema no qual, no momento da criação de uma conta, o cartão de crédito inserido era verificado na mesma hora no sistema bancário, a fim de verificar se este era válido. Com essa mudança, surgem em fóruns da época, discussões acerca de novos métodos para conseguir acessar a Internet sem precisar pagar por isso. A nova estratégia agora baseava-se em enganar os clientes da AOL que pagavam pelo serviço, fazendo com que eles fornecessem seus dados de acesso para os golpistas que se passavam por funcionários da empresa. Esse método para obter os dados das faturas dos clientes a partir de *links* e mensagens falsas, os quais funcionavam exatamente como iscas, ficou conhecido por *phishing* (EMAILVERITAS, 2022?).

O *phishing* consiste na criação de páginas ou endereços falsos com o intuito de roubar dados pessoais, como senhas bancárias. Para tal, a técnica de *phishing* utiliza-se de artimanhas que geram sensação de veracidade nas informações. Tratamento formal, assuntos relacionados a dinheiro, mensagens que instiguem a necessidade de uma resposta, preenchimento de formulários e urgência caracterizam as estratégias adotadas no *phishing* que podem induzir a vítima a abrir arquivos ou acessar conteúdos que contenham *malwares* (FREIRE; SILVA; QUEIROZ, 2017).

Em outras palavras, conforme descrito por Santos-d'Amorim e Miranda (2021, p. 14, tradução nossa): "Como um dispositivo de desinformação, o *phishing* é um tipo de uso indevido de informações pessoais e/ou confidenciais. O roubo de informações pessoais copiando um site popular e inserindo dados pessoais tornou-se uma ferramenta comum." [3].

Os tipos mais comuns de *phishing*, de acordo com Pereira (2012), são:

a) *pharming*
b) *spear phishing*
c) *iPhishing*
d) *vishing scam*
e) mensageiros instantâneos
f) *sites* de relacionamento

A técnica de *pharming* ou DNS *cache poisoning*, consiste em explorar uma vulnerabilidade do sistema DNS (*Domain Name Server*) ou Servidor de Nomes de Domínios, que é responsável traduzir o endereço de sites da Internet, por exemplo, para um endereço IP. Se o servidor DNS estiver vulnerável, o endereço digitado poderá redirecionar para uma página falsa, criada pelos cibercriminosos para simular um *site* legítimo.

O *spear phishing* trata-se de um golpe altamente focalizado, utilizado geralmente para ataques a grandes organizações. A palavra do inglês, "*spear*", significa "arpão", fazendo referência à pesca de arpão, atividade que demanda uma alta precisão.

O *iPhishing* é uma técnica impulsionada pelos mais diversos dispositivos que dispõem de acesso à Internet, como os *smartphones*, *tablets* e aparelhos de televisão. Fatores como os distintos tamanhos de tela podem dificultar a visualização dos endereços eletrônicos de *sites* que esses aparelhos acessam, tornando a identificação de endereços falsos uma tarefa árdua. Além disso, algumas questões

[3] "As a malinformation device, phishing is a type of misuse of personal and/or confidential information. Theft of personal information by copying a popular website and inserting personal data has become a common tool.".

técnicas como a falta de atualização do sistema operacional desses dispositivos os tornam mais propensos a sofrerem ataques.

A combinação de uma técnica antiga de golpes apoiada nas tecnologias recentes é o *Vishing Scam*. Os *hackers* aproveitam-se dos baixos custos de ligação propiciados pela tecnologia VoIP (*Voice over IP*) juntamente com a dificuldade para rastrear o telefone de origem para tentar obter dados das suas vítimas. O golpe funciona da seguinte forma: em posse do número de telefone da vítima, o atacante começa a disparar mensagens de texto (SMS), *e-mails* e até mesmo mensagens de voz com o objetivo de convencer a vítima a ligar para um número informado pelos golpistas. Ao ligar para o número fornecido, que simula uma central de atendimento e possui uma tecnologia capaz de detectar a inserção de dados através das teclas do dispositivo, os criminosos convencem a vítima a fornecer seus dados pessoais, que posteriormente serão usados para atividades ilícitas.

Os mensageiros instantâneos são mais uma oportunidade para o uso das técnicas de *phishing*. Nesse tipo de abordagem, anexos e endereços eletrônicos suspeitos, também conhecidos por URL's, são enviados pelos criminosos às vítimas que ao interagirem com esses recursos, os baixando ou acessando, acabam tendo seus dispositivos infectados. Normalmente pessoas com menos afinidade com a tecnologia acabam sendo vítimas dessa estratégia por acreditarem que o conteúdo malicioso foi enviado por algum amigo ou familiar.

Por fim, os sites de relacionamento, assim como o exemplo anterior, são mais uma possibilidade para os criminosos obterem vantagem sobre a fragilidade e curiosidade das pessoas. Ao inventarem uma história convincente o bastante para induzir a vítima a clicar em um *link* malicioso que redireciona para um *site* muito semelhante com o padrão desse tipo de plataforma, o usuário é induzido a fornecer seus dados ao criminoso.

Como foi possível observar, o fator humano é fundamental para o êxito dos golpes baseados em *phishing*. Com a tecnologia cada vez mais presente e acessível, é comum que esses tipos de ataque estejam em alta e, por conta disso, é de suma importância conhecer as formas de atuação e as estratégias usadas pelos criminosos.

Por serem conceitos bastante próximos, muitas das vezes é difícil identificar a diferença entre engenharia social e o *phishing*. De maneira resumida, enquanto a engenharia social pode ser aplicada em qualquer contexto, seja ele presencial ou virtual, as técnicas de *phishing* são aquelas criadas para a utilização na Internet. Segundo Agência Brasileira de Inteligência (2021), o *phishing* tem como objetivo atingir o maior número de pessoas, uma vez que a sua taxa de sucesso é muito baixa.

A evolução da tecnologia tem favorecido o aparecimento de novos tipos de golpes e o aperfeiçoamento das estratégias já conhecidas, porém tais técnicas sempre têm a mesma base de funcionamento: ludibriar as pessoas. Da mesma forma, a proteção dos dados também tem uma base que deve ser seguida. Sendo assim, cuidados básicos como desconfiar de *links* recebidos por mensagem, criar senhas fortes e instalar aplicativos somente de fontes oficiais são jeitos fáceis e efetivos de diminuir os riscos das ameaças existentes.

A LGPD trata das implicações relacionadas ao vazamento de dados, ou seja, a violação da proteção de dados ocasionada por alguma falha de segurança, como a invasão de sistemas informacionais decorrente da não observação das diretrizes, as quais o Controlador e/ou o Operador de dados devem seguir. O *phishing*, por sua vez, caracteriza-se como um vazamento de dados ocasionado por falha humana, onde o criminoso obtém dados que foram voluntariamente entregues pela vítima, não havendo a invasão de um sistema de informações, por exemplo. Dessa forma, ataques de *phishing* não estão cobertos pela Lei Geral de Proteção de Dados, entretanto, o cidadão dispõe de algumas outras leis que visam coibir a ação de criminosos e estabelecer penas mais graves para esses tipos de delitos. A Leis nº 12.737/2012 e nº 14.155/2021 são exemplos que visam atender essa finalidade.

Observando isso, cabe ao próprio usuário cuidar de seus dados pessoais, adotando medidas de segurança na sua rotina. Entre as principais medidas de segurança, retomando as já recomendadas pela Autoridade Nacional de Proteção de Dados (BRASIL, 2022?a), estão incluídas:

a) criar *backups* dos dados armazenados, principalmente em nuvem;
b) ativar a criptografia nos discos e mídias externas, como *pen drives*;
c) criar senhas fortes combinando caracteres especiais, letras maiúsculas e minúsculas e números evitando o uso de palavras comuns ou dados pessoais;
d) habilitar a verificação de senhas em duas etapas sempre que possível, principalmente em sistemas de armazenamento em nuvem e aplicativos de mensagens;
e) instalar aplicativos somente de fontes e lojas oficiais;
f) sempre manter o sistema operacional e aplicativos atualizados;
g) desconfiar de links recebidos por aplicativos de mensagens;
h) limitar a divulgação ou fornecimento de dados pessoais na Internet, inclusive em redes sociais, ou para empresas, aos casos estritamente necessários.

Como é possível constatar, as medidas de segurança contra o *phishing* são todas relacionadas ao contexto digital, uma vez que os golpes de *phishing* somente existem nesse meio, ao contrário da engenharia social que engloba todos os tipos de manipulação, em ambientes físicos ou virtuais visando a obtenção de dados. A era da informação, a partir da popularização de tecnologias, possibilitou o acesso, geração e compartilhamento facilitado de informações, fatores que atraíram a atenção dos cibercriminosos para os ambientes virtuais, colocando ainda mais em risco a proteção de dados pessoais dos cidadãos.

4 CONSIDERAÇÕES FINAIS

A era da informação vem, desde a década de 1970, marcando a sociedade no que se refere à interação com a informação, principalmente após o advento da Internet. O acesso rápido a diversos tipos de conteúdo e a possibilidade de criar e compartilhar informações em poucos cliques, muitas das vezes na palma da mão, revolucionou as formas de comunicação e os fluxos de informação.

Com o enorme volume de informações existente, são necessárias formas de proteção eficientes. Assim, a segurança da informação é responsável pela gestão de diversos ativos, como a própria informação e os agentes que manipulam ou processam informações, destacando-se o agente humano.

Algumas ameaças, conhecidas como crimes cibernéticos ou cibercrimes, põem em risco a segurança da informação. Os tipos de cibercrimes mais comuns são os ataques de *ransomware*, invasões de dispositivos para disseminação de vírus e *malware*, golpes e fraudes perpetuados por meio de redes sociais, além da interrupção ou perturbação de sites.

Embora não exista uma legislação específica contra crimes cibernéticos, algumas leis foram criadas visando coibir esses tipos de delitos, tais como a Lei nº 12.737/2012, também conhecida como “Lei Carolina Dieckmann”, que dispõe sobre a invasão de dispositivos informáticos e a Lei nº 14.155/2021, que torna mais grave crimes de violação de dispositivo informático e os crimes já tipificados no Código Penal, porém praticados no meio eletrônico.

De modo a proteger os dados pessoais, destacam-se os cuidados que devem ser tomados e também a Lei Geral de Proteção de Dados, que rege fundamentalmente qualquer atividade que utiliza dados pessoais na execução da sua operação. Ainda sobre legislação, vale ressaltar a discussão a respeito do direito ao esquecimento, que embora tenha sido considerado inconstitucional no Brasil, visa conter a divulgação de dados indesejados com a finalidade de proteger a intimidade, vida privada, imagem e nome para que se estabeleça o direito de não ser perturbado.

A partir da identificação dos conceitos relacionados a proteção de dados pessoais, é possível observar que a LGPD protege os cidadãos no tocante aos

dados comumente utilizados em cadastros, como RG, CPF, data e local de nascimento, dados de cartão de crédito, dados bancários, entre outros, determinando que tais informações sejam tratadas e armazenadas de forma correta, ou seja, a legislação aborda a responsabilidade das organizações no armazenamento de dados pessoais. Entretanto, como ataques de *phishing* utilizam-se técnicas de engenharia social para explorar a falha humana, com o objetivo de convencer ou enganar a vítima a entregar os seus dados, a LGPD não é capaz de amparar o cidadão nesses casos.

Sobre a engenharia social, foi possível observar que seus métodos são utilizados há várias décadas, como foi citado o caso do primeiro vírus de computador, “Elk Cloner”, que felizmente, tratava-se apenas de uma brincadeira, mas obteve sua fama a partir dos métodos de engenharia social aplicados pelo seu criador para disseminar tal ameaça. Sendo assim, é importante ressaltar que a engenharia social pode ocorrer tanto fisicamente quanto virtualmente, existindo na atualidade um maior destaque às estratégias de engenharia social voltadas aos meios eletrônicos, como o *phishing*.

Como já dito, a era da informação vem gerando um volume cada vez maior de informações, principalmente em decorrência da Internet, o que determinou uma revolução na forma como as pessoas interagem nesse contexto de superinformação. Os criminosos, portanto, vêm buscando se adaptar a essa nova realidade, utilizando-se de técnicas de engenharia social, constituindo, dessa forma, uma ameaça à segurança de dados pessoais, conhecida por *phishing*.

Assim, para se defender da ameaça de *phishing* na era da informação, cabe às pessoas adotarem medidas básicas de segurança nos ambientes digitais, como criar senhas fortes, instalar aplicativos somente de fontes e lojas confiáveis, desconfiar de *links* recebidos por aplicativos de mensagens e limitar o compartilhamento de informações pessoais para casos estritamente necessários.

Este trabalho não encerra o assunto, outras pesquisas devem ser feitas para aprofundar a análise do *phishing* e de como as pessoas podem proteger seus dados de ataques cibernéticos, principalmente no contexto da era da informação.

REFERÊNCIAS

10 FORMAS de proteger seus dados pessoais na internet. **ConectaJá**. Rio de Janeiro, 2019. Disponível em: https://conectaja.proteste.org.br/proteger-seus-dados-pessoais. Acesso em: 12 set. de 2022.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Engenharia social**: guia para proteção de conhecimentos sensíveis. Abin: [S.l.]. 2021. Disponível em: https://www.gov.br/abin/pt-br/acesso-a-informacao/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis. Acesso em: 14 mar. 2023.

ALECRIM, E. PF realiza operação para investigar ataque hacker que derrubou ConecteSUS. **Tecnoblog**. [S.l.]. 2022. Disponível em: https://tecnoblog.net/noticias/2022/08/16/pf-realiza-operacao-para-investigar-ataque-hacker-que-derrubou-conectesus. Acesso em: 14 mar. 2023.

ARAUJO, N. C.; MOTA, F. R. L.; OLIVEIRA, C. M. B. S. de. Desafios da informação frente a fake news em tempos de coronavírus. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, João Pessoa, PB, v. 15, n. 2, p. 35-50, jun. 2020. Disponível em: https://www.pbcib.com/index.php/pbcib/article/view/53012/30716. Acesso em: 12 set. 2022.

ATAQUES DDoS dobram no Brasil por conta das eleições. **Security Report**. [S.l.]. 2022. Disponível em: https://www.securityreport.com.br/overview/ataques-ddos-dobram-no-brasil-por-conta-das-eleicoes. Acesso em: 14 mar. 2023.

BARROS, C.; CORT, N. D. **Roubo de dados**: o que é phishing e como se prevenir? [S.l], 2021. Disponível em: https://investnews.com.br/geral/roubo-de-dados-o-que-e-phishing-e-como-se-prevenir. Acesso em: 12 set. 2022.

BARROS, L. M. **O direito ao esquecimento como instrumento de efetivação da dignidade da pessoa humana**. 2022. 37 f. Trabalho de Conclusão de Curso (Graduação) - Curso de Direito, Universidade São Judas Tadeu, São Paulo, 2022. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/29137/1/Laura%20Mendieta%20Barros%20-%20VERS%c3%83O%20FINAL%20-%20TCC%20II.pdf. Acesso em: 15 mar. 2023.

BEAL, A. **Gestão estratégica da informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2004.

BRASIL. Autoridade Nacional de Proteção de Dados. **ANPD participa de Seminário que discute o combate aos crimes cibernéticos**. [S.l.], 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-seminario-que-discute-o-combate-aos-crimes-ciberneticos. Acesso em: 14 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Proteção de dados pessoais agora é um direito fundamental**. [S.l.], 2022a. Disponível em: https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental. Acesso em: 21 mar. 2023.

BRASIL. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. **Recomendação 03/2023**. [S.l.], 2023. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2023/recomendacao-03-2023. Acesso em: 21 mar. 2023.

BRASIL. Comitê Central de Governança de Dados. **Guia de boas práticas para implementação na administração pública federal**. [S.l], 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 15 abr. 2023.

BRASIL. [Constituição (1988)]. **Constituição da república federativa do Brasil.** Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em 15 mar. 2023.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília: Presidência da República, [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 set. 2022.

BRASIL. Ministério da Cidadania. **Lei geral de proteção de dados pessoais (LGPD)**. [S.l], 2022b. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd. Acesso em: 27 set. 2022.

BRASIL. Ministério da Justiça. **Como proteger seus dados pessoais**: guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON. [S.l], 2022?a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. Acesso em: 11 set. 2022.

BRASIL. Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome. **Classificação dos dados**. [S.l], 2022c. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados. Acesso em: 06 mar. 2023.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília: Presidência da República, [1990]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 12 set. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília: Presidência da República, [2012]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 set. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, [2018a]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 set. 2022.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) [...]. Brasília: Presidência da República, [2018b]. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm. Acesso em: 12 set. 2022.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) [...]. Brasília: Presidência da República, [2021b]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 12 set. 2022.

CASTELLS, M. **A galáxia da internet**. Rio de Janeiro: Zahar, 2003.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

CERVO, A. L.; BERVIAN, P. A. **Metodologia científica**. 5. ed. São Paulo: Prentice Hall, 2002.

CONCEIÇÃO, J. P. da. A arte da fraude no campo da informação: engenharia social, big data e a manipulação do usuário na rede. **Bibliotecas Universitárias**: pesquisas, experiências e perspectivas, Belo Horizonte, v. 4, n. 1, p. 36-45, jan./jun. 2017. Disponível em: https://periodicos.ufmg.br/index.php/revistarbu/article/view/3110. Acesso em: 5 set. 2022.

COUTINHO, C. P.; LISBÔA, E. S. Sociedade da informação, do conhecimento e da aprendizagem: desafios para educação no século XXI. **Revista de Educação**, Minho, v. 18, n. 1, p. 5-22, 2011. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/14854/1/Revista_Educa%c3%a7%c3%a3o%2cVolXVIII%2cn%c2%ba1_5-22.pdf. Acesso em: 11 set. 2022.

DEMARTINI, F. **Como se proteger contra o roubo de identidade na internet**. Canaltech. 2022. Disponível em: https://canaltech.com.br/seguranca/como-se-proteger-contra-o-roubo-de-identidade-na-internet-223449/. Acesso em: 06 mar. 2023.

DEMO, P. Ambivalências da sociedade da informação. **Ciência da Informação**, [S. l.], v. 29, n. 2, 2000. Disponível em: https://revista.ibict.br/ciinf/article/view/885. Acesso em: 5 set. 2022.

EMAILVERITAS. **História do phishing**. Victoria: Canadá, 2022? Disponível em: https://www.emailveritas.com/pt/blog/historia-do-phishing. Acesso em: 30 set. 2022.

FREIRE, R. F. P.; SILVA, H. C. C.; QUEIROZ, R. G.; BATISTA, A. A. M. O fator humano como uma vulnerabilidade em segurança da informação. **Revista Brasileira de Administração Científica**, Aracaju, v. 8, n. 3, p. 146-157, jun./dez. 2017. Disponível em: https://www.sustenere.co/index.php/rbadm/article/view/SPC2179-684X.2017.003.0012/1259. Acesso em: 05 set. 2022.

GARRETT, F. **O que é malware? Veja significado, tipos e saiba remover**. Techtudo. [S.l.]. 2021. Disponível em: https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml. Acesso em: 14 mar. 2023.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2008.

KASPERSKY. **O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos**. [S.l], c2022. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 20 set. 2022.

LEYDEN, J. **The 30-year-old prank that became the first computer virus**. **The** Register. [S.l.]. 2012. Disponível em: https://www.theregister.com/2012/12/14/first_virus_elk_cloner_creator_interviewed/?page=1. Acesso em: 14 mar. 2023.

MALWAREBYTES. **Cryptojacking**. [S.l], 2022? Disponível em: https://br.malwarebytes.com/cryptojacking. Acesso em: 20 set. 2022.

MANNARA, B. **Grupo hacker pode ter sequestrado mais de 3 TB de dados do Governo Federal**. Tilt. [S.l.]. 2022. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/08/31/grupo-hacker-pode-ter-sequestrado-mais-de-3-tb-de-dados-do-governo-federal.htm. Acesso em: 14 mar. 2023.

MANZZI, A. C. **Conheça os principais golpes na Internet e saiba como proteger os seus dados**. NIC.br: São Paulo, 05 de set. de 2022. Disponível em: https://www.nic.br/noticia/na-midia/conheca-os-principais-golpes-na-internet-e-saiba-como-proteger-os-seus-dados/. Acesso em: 25 set. 2022.

MARRA, F. B. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. **Journal of Law and Sustainable Development**, São Paulo, v. 7, n. 2, p. 145–167, 2019. Disponível em: https://journalsdg.org/jlss/article/view/289. Acesso em: 10 set. 2022.

MARTINI, R. **Sociedade da informação**: para onde vamos. 1. ed. São Paulo: Trevisan, 2017. *E-book*.

MARTINS, I. T. **Tratamento de dados pessoais**: por que precisamos saber como os nossos dados pessoais são tratados?. 2020. 50 f. Trabalho de Conclusão de Curso (Graduação) - Curso de Direito, Pontifícia Universidade Católica de Goiás, GOIÂNIA, 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/563/1/Isabella%20Teixeira%20Martins_monografia%20%282%29.pdf. Acesso em: 15 mar. 2023.

MASCARENHAS NETO, P. T.; ARAÚJO, W. J. **Segurança da informação**: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019. *E-book*.

MENDES, L. S. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**. São Paulo, vol. 20, n. 3, p. 45- 81, jul/set, 2011.

MEYER, M. **O que é malware? Veja significado, tipos e saiba remover**. Oficina da net. [S.l.]. 2016. Disponível em: https://www.oficinadanet.com.br/post/13962-os-primeiros-virus-de-computador-da-historia. Acesso em: 14 mar. 2023.

MOZILLA CORPORATION. **HTTPS and padlock in website address bar**. [S.l], 2022. Disponível em: https://blog.mozilla.org/netpolicy/2022/05/31/enhancing-trust-and-security-on-the-internet-browsers-are-the-first-line-of-defence/https-and-padlock-in-website-address-bar/. Acesso em: 12 mar. 2023.

NEVES, B. C.; BORGES, J. Por que as Fake News têm espaço nas mídias sociais?: uma discussão a luz do comportamento infocomunicacional. **Informação & Sociedade**: Estudos, João Pessoa, v. 30, n. 2, p. 1-22, abr./jun. 2020. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/50410. Acesso em: 17 out. 2022.

PARANÁ. Tribunal Regional Eleitoral – PR. **Lei geral de proteção de dados**. Curitiba: TRE-PR, [202?a]. Disponível em: https://www.tre-pr.jus.br/transparencia-e-prestacao-de-contas/lei-geral-de-protecao-de-dados/o-que-sao-dados-pessoais. Acesso em: 11 set. 2022.

PARANÁ. Tribunal Regional Eleitoral – PR. **O tratamento de dados e seus requisitos**. Curitiba: TRE-PR, [202?b]. Disponível em: https://www.tre-pr.jus.br/transparencia-e-prestacao-de-contas/lei-geral-de-protecao-de-dados/o-tratamento-de-dados-e-seus-requisitos. Acesso em: 11 set. 2022.

PAZ MENDES SOCIEDADE DE ADVOGADOS. **Crimes cibernéticos no Brasil**: conheça os tipos, suas penas e agravantes. São Paulo, 2021. Disponível em: https://www.pazmendes.com.br/crimes-ciberneticos-no-brasil/. Acesso em: 28 set. 2022.

PEREIRA, C. G. **Phishing**: conceitos e ações preventivas aplicadas à empresa. 2012. 56 f. Trabalho de Conclusão de Curso (Pós-Graduação) - Curso de Pós-graduação em Redes de Computadores, Centro Universitário de Brasília, Brasília, 2012. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/235/8136/1/50910909.pdf. Acesso em: 10 fev. 2023.

REZENDE, G. G. **O phishing e a responsabilidade empresarial**: aspectos sobre as medidas protetivas do empresário face ao prejuízo de seus usuários. 2022. 22 f. Trabalho de Conclusão de Curso (Graduação) - Curso de Direito, Universidade Federal de Uberlândia, Uberlândia, 2022. Disponível em: https://repositorio.ufu.br/bitstream/123456789/34807/4/PhishingResponsabilidadeEmpresarial.pdf. Acesso em: 07 out. 2022.

SABBATINI, G.; GOBATO C. Direito ao esquecimento na 'era da superinformação'. **Consultor Jurídico**. São Paulo: SP, 8 de mar. 2021. Disponível em: https://www.conjur.com.br/2021-mar-08/opiniao-direito-esquecimento-superinformacao. Acesso em: 15 mar. 2023.

SANTOS-D'AMORIM, K.; MIRANDA, M. Informação incorreta, desinformação e má informação: Esclarecendo definições e exemplos em tempos de desinfodemia. **Encontros Bibli:** revista eletrônica de biblioteconomia e ciência da informação, Florianópolis, v. 26, p. 1-23, 2021. DOI: 10.5007/1518-2924.2021.e76900. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/76900. Acesso em: 6 set. 2022.

SCHAUN, G. **Uma lista com 24 crimes virtuais**. Jusbrasil. [S.l.], 2019. Disponível em: https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais. Acesso em: 02 mar. 2023.

SÊMOLA, M. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Elsevier, 2003.

SILVA, E. L. da; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. Florianópolis: UFSC, 2005, 138p. Disponível em: https://tccbiblio.paginas.ufsc.br/files/2010/09/024_Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes1.pdf. Acesso em: 22 fev. 2023.

SOUSA, A. S. de; OLIVEIRA, G. S. de; ALVES, L. H. A. Pesquisa Bibliográfica: princípios e fundamentos. **Cadernos da Fucamp**, Monte Carmelo, MG, v. 20, n. 43, p. 64-83, mar. 2021. Disponível em: https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2336/1441. Acesso em: 11 set. 2022.

SOUZA, D. C. R. de. **Segurança da Informação**: uma metodologia para implantação de um sistema de gestão de segurança da informação. 2020. 107 f. Dissertação (Mestrado) - Curso de Políticas Públicas,

Gestão e Avaliação da Educação Superior, Universidade Federal da Paraíba, João Pessoa, 2020. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/20370/1/DiegoChavesReinaldoDeSouza_Dissert.pdf. Acesso em: 3 mar. 2023.

VAINZOF, R. Disposições preliminares. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD – Lei Geral de Proteção de Dados Comentada.** 2. ed. São Paulo: Revista dos Tribunais, 2020. *E-book*.

WERTHEIN, J. A sociedade da informação e seus desafios. **Ciência da Informação**. v. 29, n. 2, p. 71-77, maio/jun. 2000. Disponível em: https://doi.org/10.1590/S0100-19652000000200009. Acesso em: 10 set. 2022.

ZAMBONATO, M. S. **Avanços da legislação brasileira no combate aos crimes cibernéticos**. 2022. 50 f. Trabalho de Conclusão de Curso (Graduação) - Curso de Ciências Jurídicas e Sociais, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2022. Disponível em: http://www.bibliotecadigital.ufrgs.br/da.php?nrb=001154043&loc=2022&l=7ed32eaa89420ddd. Acesso em: 3 mar. 2023.