UNIVERSIDADE FEDERAL DO PARANÁ

BRYAN FELIPE DE OLIVEIRA

# LGPD, PRIVACIDADE E SEUS IMPACTOS NOS PROCESSOS DE ENGENHARIA SOCIAL

CURITIBA

2022

BRYAN FELIPE DE OLIVEIRA

# LGPD, PRIVACIDADE E SEUS IMPACTOS NOS PROCESSOS DE ENGENHARIA SOCIAL

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Gestão da Informação, curso de Pós-graduação em Gestão da Informação, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

Orientador: Prof. Dr. José Simão de Paula Pinto

CURITIBA

2022

O48 Oliveira, Bryan Felipe de,

*LGPD, privacidade e seus impactos nos processos de engenharia social* [recurso eletrônico] / Bryan Felipe de Oliveira. – Curitiba, 2022.

Dissertação (Mestrado) – Programa de Pós-Graduação em Gestão da Informação. Setor de Ciências Sociais Aplicadas. Universidade Federal do Paraná.

Orientador: Prof. Dr. José Simão de Paula Pinto

1. Engenharia social. 2. Segurança da informação. 3. Gestão de Dados – Medidas de segurança. 4. Proteção de dados – Legislação – Brasil. I. Pinto, José Simão de Paula. II. Programa de Pós-Graduação em Gestão da Informação. Setor de Ciências Sociais Aplicadas. Universidade Federal do Paraná. III. Título.

CDD 320.6

FICHA CATALOGRÁFICA ELABORADA PELO SISTEMA DE BIBLIOTECAS / UFPR

BIBLIOTECÁRIA: MARILUCI ZANELA CRB 9/1233

MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIÊNCIAS SOCIAIS E APLICADAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO GESTÃO DA INFORMAÇÃO - 40001016058P1

# TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação GESTÃO DA INFORMAÇÃO da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **BRYAN FELIPE DE OLIVEIRA** intitulada: **LGPD, PRIVACIDADE E SEUS IMPACTOS NOS PROCESSOS DE ENGENHARIA SOCIAL**, sob orientação do Prof. Dr. JOSÉ SIMÃO DE PAULA PINTO, que após terem inquirido o aluno e realizada a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 09 de Maio de 2022.

JOSÉ SIMÃO DE PAULA PINTO
Presidente da Banca Examinadora

RODRIGO EDUARDO BOTELHO FRANCISCO
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

CLEVERTON JULIANO ALVES VICENTINI
Avaliador Externo (INSTITUTO FEDERAL DE EDUC., CIÊNCIA E TECNOLOGIA DO PARANÁ)

Dedico esta dissertação à minha mãe Neide, que com toda simplicidade me ensinou a importância da educação e onde ela pode nos levar.

## AGRADECIMENTOS

A Deus, por todas as oportunidades concedidas e pela força que nos move em direção ao progresso.

Ao Professor José Simão de Paula Pinto, que me conduziu e orientou, desde o primeiro momento, que me possibilitou a realização deste trabalho, assim como de todos os ensinamentos no âmbito acadêmico e científico.

Aos Docentes Rodrigo Eduardo Botelho Francisco e Cleverton Juliano Alves Vicentini pela participação das bancas de qualificação e defesa, podendo assim contribuir positivamente com o desenvolvimento deste trabalho.

A UFPR e ao PPGGI, por ter possibilitado toda essa experiência e o desenvolvimento dessa pesquisa, com apoio e incentivo por parte da Coordenação, Secretaria e os membros do corpo docente e discente.

Aos colegas Marcos Maia, Amanda Carvalho de Garcia, Irene Tomoko Nakano e Sílvio Tacara, por me conduzirem até o Mestrado, com palavras de incentivo e direcionamentos didáticos, técnicos e práticos, os quais foram essenciais para ingressar nessa jornada, bem como à servidora Edneia Oliveira Cavalcanti e ao doutorando do PPGMICS Rogério da Luz, pela parceria e colaboração, em todos os momentos que se fizeram presentes, dando o apoio profissional necessário e os melhores conselhos de amigos.

Aos colegas José Leandro Seguro e Larissa Lourenço Nunes Benck, mestrandos do PPGGI, pelas dicas, orientações e por compartilhar os momentos bons e de dificuldade dessa etapa.

Aos discentes dos grupos das disciplinas transversais de Métodos Estatísticos e Filosofias da Ciência e Tecnologia, por compartilharem seu conhecimento e pela união, na busca de auxiliar aos demais pós-graduandos, nos momentos de dificuldade, com sabedoria e muito bom humor.

Aos amigos e familiares que incentivaram e apoiaram essa e outras etapas tão importantes da minha caminhada, se fazendo presentes em todos os momentos.

Ao meu companheiro Luiz, por toda compreensão e apoio, nessa jornada de conhecimento, que me fortaleceu com encorajamento em relação desafios e obstáculos a serem enfrentados.

“Cada dia que amanhece assemelha-se a uma página em branco, na qual gravamos os nossos pensamentos, ações e atitudes. Na essência, cada dia é a preparação de nosso próprio amanhã”

Chico Xavier

## RESUMO

No contexto social da humanidade, a informação pode ser tida como um bem de valor inestimável e sua vulnerabilidade pode representar uma série de riscos aos seus titulares. A exemplo desta fragilidade, com relação à privacidade do indivíduo, os agentes da Engenharia Social, no uso de seus mecanismos são capazes de burlar sistemas informacionais, dos simples aos mais complexos, na busca da obtenção de informações, que auxiliam na aproximação de suas vítimas, com objetivo de aplicação de golpes. A concepção das definições de segurança e privacidade, na sociedade contemporânea, através de marcos regulatórios, evidencia a preocupação com o resguardo das informações dos cidadãos. Esses marcos vêm se desenvolvendo ao longo do tempo, para englobar políticas mais rígidas e específicas, de acordo com o avanço tecnológico e seus impactos nas relações sociais e informacionais. A lei geral de proteção de dados no Brasil, oriunda da influência de regulamentações internacionais, principalmente da União Europeia (GDPR), traz em seu arcabouço uma série de normas e conceitos aos seres sociais e ações que permeiam este universo dos dados. Essas definições buscam reforçar princípios constitucionais, que preveem a inviolabilidade da privacidade dos cidadãos. De acordo com a revisão de literatura, estudo documental dos marcos regulatórios de proteção de dados, levantamento de casos de vazamento de dados, o presente estudo visa inferir que as políticas de proteção de dados podem ser capazes de mitigar ações dos agentes da ES.



**Palavras-chave**: Engenharia Social; LGPD; Gestão de dados; Segurança da Informação.

## ABSTRACT

In humanity’s social context, information can be seen as an invaluable asset and its vulnerability can pose a series of risks to its holders. An example of this, in relation to the individual's privacy, the agents of Social Engineering, using their mechanisms, are able to circumvent informational systems, from simple to more complex, in the search for security information that facilitates approaching their victims, with the aim of apply blows. The assembly of privacy and security, on a modern society, through regulatory frameworks, shows a concern regarding the protection of citizens' information. These milestones arise from its comprehensive policies over time, to all the more rigid and comprehensive principles, which manifest themselves according to technological advances and impacts on social and informational relationships. The general data protection law in Brazil, arising from the influence of international regulations, mainly the European Union (GDPR), brings in its framework a series of norms and concepts to social beings and actions that permeate this universe of data. These constitutionally founded institutions, which provide for the inviolability of citizens' privacy. According to the data review, documentary study of regulatory frameworks for data protection, data collection can be provided from data literature, the present study aims to infer that data protection policies are capable of mitigating actions of ES agents.



**Keywords**: Social Engineering; Data management; LGDP, Information Security.

## LISTA DE FIGURAS E ILUSTRAÇÕES

FIGURA 1 – CICLO DA ENGENHARIA SOCIAL ..... 38
FIGURA 2 – FLUXO DE PROCEDIMENTOS METODOLÓGICOS ..... 56
GRÁFICO 1 – NÚMERO DE MULTAS MENSAIS APLICADAS ATRAVÉS DA GDPR (NÃO CUMULATIVO) ..... 64
GRÁFICO 2 – NÚMERO DE MULTAS MENSAIS APLICADAS ATRAVÉS DA LGPD (NÃO CUMULATIVO) ..... 66

## LISTA DE TABELAS E QUADROS

QUADRO 1 – TIPOS DE ENGENHARIA SOCIAL ..... 34
QUADRO 2 – EPISÓDIOS DE VAZAMENTO DE DADOS ..... 60

## LISTA DE ABREVIATURAS E SIGLAS

ANPD – ASSOCIAÇÃO NACIONAL DE PROTEÇÃO DE DADOS
ANPPD – ASSOCIAÇÃO NACIONAL DOS PROFISSIONAIS DE PRIVACIDADE DE DADOS
APPI – *ACT ON THE PROTECTION OF PERSONAL INFORMATION*
APPS – APLICATIVOS
BR – BRASIL
CCPA – CALIFORNIA *CONSUMER PRIVACY ACT*
CF – CONSTITUIÇÃO FEDERAL
ES – ENGENHARIA SOCIAL
EUA – ESTADOS UNIDOS DA AMÉRICA
FBI - FEDERAL *BUREAU OF INVESTIGATION*
GDPR – *GENERAL DATA PROTECTION REGULATION*
GET – *GDPR ENFORCEMENT TRACKER*
GI – GESTÃO DA INFORMAÇÃO
LGPD – LEI GERAL DE PROTEÇÃO DE DADOS
LGPDP – *LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES*
LPDP – *LEY DE PROTECIÓN DE LOS DATOS PERSONALES*
PA – *PROTECTION ACT*
PSI – POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO
PIPL – PERSONAL INFORMATION PROTECTION LAW
POPIA – *PROTECTION OF PERSONAL INFORMATION ACT*
PPGGI – PROGRAMA D EPÓS-GRADUAÇÃO EM GESTÃO DA INFORMAÇÃO
SI – SISTEMAS DE INFORMAÇÃO
TI – TECNOLOGIA DA INFORMAÇÃO
TOGAF – *THE OPEN GROUP ARCHITETURE FRAMEWORK*
UFPR – UNIVERSIDADE FEDERAL DO PARANÁ
UK – *UNITED KINGDOM*

**SUMÁRIO**

**1 INTRODUÇÃO ..... 13**
1.1 PROBLEMA DA PESQUISA ..... 15
1.2 OBJETIVOS ..... 16
1.2.1 Objetivo Geral ..... 16
1.2.2 Objetivos Específicos ..... 16
1.3 JUSTIFICATIVA ..... 17
**2 REFERENCIAL TEÓRICO ..... 18**
2.1 GESTÃO DA INFORMAÇÃO ..... 18
2.1.1 Informação Digital ..... 21
2.1.2 Arquitetura Informacional ..... 24
2.1.3 Segurança da Informação e Privacidade ..... 26
2.2 ENGENHARIA SOCIAL ..... 29
2.2.1 Agentes da Engenharia Social ..... 32
2.2.2 Tipos de Engenharia Social ..... 34
2.2.3 Natureza da Engenharia Social ..... 37
2.3 LEI GERAL DE PROTEÇÃO DE DADOS ..... 39
2.3.1 Marcos Legais ..... 41
2.3.2 Cenário Global ..... 44
2.3.3 LGPD ..... 51
**3 PROCEDIMENTOS METODOLÓGICOS ..... 55**
**4 ANÁLISE DE DADOS E DISCUSSÃO ..... 58**
**5 CONCLUSÃO E CONSIDERAÇÕES FINAIS ..... 70**
**6 REFERÊNCIAS BIBLIOGRÁFICAS ..... 74**

## 1 INTRODUÇÃO

No que diz respeito ao valor da informação, em toda a história da humanidade, se destaca a ideia de que a sua proteção é essencial para o triunfo. Quando uma tribo ou povoado permitia que seus segredos, comportamentos e crenças, ou ainda mais relevantes, como locais de caça e armazenagem dos alimentos, a forma com que mantinham o domínio e poder sobre seus escravizados era exposto ou descoberto, por algum grupo inimigo que os observava, era iminente que o ataque seria então direcionado, com base no conhecimento das suas fragilidades.

Mesmo com o passar do tempo, ainda é perceptível que através da posse de informações pessoais de um indivíduo é mais fácil aproximar-se dele, para triunfar sobre suas fraquezas, relacionadas a seus interesses e comportamentos. Não são necessários grandes esforços, nas redes sociais digitais, para que os usuários tenham um perfil traçado, com diversos possíveis apontamentos, sobre aquilo que os conecta com outros usuários ou mesmo sobre suas preferências de consumo. Essas informações podem ser de extrema relevância para grandes empresas que movimentam o mercado, em busca da expansão do seu lucro, que então trabalham fortemente em iniciativas de marketing, com objetivo de traçar o perfil detalhado de cada um dos seus consumidores, para ofertar exatamente aquilo que estes procuram ou algum objeto que lhe impulsione a satisfazer seu desejo. Além dessas empresas, a formação organizações criminosas anônimas, movidas pela ação de *crackers* e invasores, vêm explorando ferramentas tecnológicas digitais, na aplicação de golpes online, mapeando perfis de usuários e os atacando de maneira singela, através de suas redes, para crimes de extorsão.

Esses golpes e ações, através do uso do mal uso das informações dos indivíduos estão atrelados ao conceito da Engenharia Social, que pode ser definida como um coletivo de ferramentas, não somente através de meios eletrônicos, que visam a manipulação dos interesses de um usuário, a fim de influenciá-lo a optar por algo, com base na exposição de conteúdos provocativos, como também levá-lo ao fornecimento de seus dados pessoais, sem que se perceba o possível golpe envolvido.

Conforme previsto pela Constituição Federal (1988) em seu artigo 5º - Dos Direitos e Garantias Fundamentais: “X - 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". Entretanto, quando os dados dos usuários são utilizados para manipulação de suas opiniões e desejos, a Lei precisa ser mais específica, tendo em vista que mesmo utilizados de maneira irregular, os próprios detentores cedem o acesso de seus dados às empresas, em contrapartida ao acesso de uma rede, site de compras, conexão wifi, etc.

A lei 13.709, intitulada popularmente como LGPD, foi homologada no Brasil em 2018, concebida com base nos princípios norteadores dos marcos regulatórios de proteção de dados já instituídos pelo mundo, principalmente no da União Europeia, tem por objetivo trazer essa proposta mais específica, sobre proteção de dados pessoais, para a legislação brasileira. Em seus termos, estão definidos de maneira objetiva os personagens, ações e contextos do universo informacional da gestão de dados, na busca de instituir direitos e deveres nesse cenário. De acordo com sua proposta, tem como foco central o resguardo do direito à privacidade dos cidadãos, tendo então efeitos em possíveis inibições, para as ações dos mecanismos da Engenharia Social.

## 1.1 PROBLEMA DE PESQUISA

O surgimento das leis, no contexto social, remete à necessidade de estruturação das relações sociais, visando sua organização. A Ética tem definição científica aplicada ao campo social, trazendo conceitos morais às ações dos indivíduos (Sour, 2017). Ela pode ser tida como peça chave da otimização da estrutura social, num conjunto de melhorias, tendo em vista que tende a servir de métrica para comportamentos e ações dos seres sociais em seus ambientes de interação coletiva e mesmo singulares.

O avanço tecnológico viabiliza maior interação entre os indivíduos do conjunto social, através da concepção de novas ferramentas, capazes de conectar pessoas do mundo todo em uma mesma esfera, por plataformas organizadas de dados virtuais. O funcionamento desses sistemas, tal como o armazenamento dos dados que transitam por ele são de responsabilidade direta de quem estabelece a conexão entre os indivíduos. O mau uso dos dados de usuários, por parte das empresas que os detém, que até mesmo realizam sua comercialização de maneira informal, pode trazer prejuízos aos usuários. Essa exposição pode ser a fonte para aplicação de diversos golpes de Engenharia Social.

Os dados pessoais têm sido utilizados como moeda de troca para acesso às comodidades tecnológicas. Essa troca muitas vezes é nociva ao próprio usuário, que está entregando dados relevantes a respeito dos seus desejos e comportamentos, que servem de base para mecanismos de inteligência artificial, que lhes podem gerar impactos negativos, através do seu uso indevido por pessoas mal-intencionadas. Tendo em vista essa silenciosa violação das informações dos usuários, tornou-se necessária a instituição legal de normativa capaz de restringir o armazenamento, uso e acesso de dados de caráter pessoal, para que se pudesse conservar sua segurança online. **A LGPD tem como objetivo o resguardo do direito à privacidade dos usuários, seria ela capaz de mitigar os efeitos, sobre os mecanismos da Engenharia Social?**

## 1.2 OBJETIVOS

### 1.2.1 Objetivo Geral

Analisar os mecanismos da LGPD que podem contribuir para mitigação das ações da Engenharia Social.

### 1.2.2 Objetivos Específicos

a) Definir a LGPD e um breve contexto histórico até a sua concepção.
b) Realizar estudo documental da LGPD e marcos legais internacionais de mesmo teor, quanto às suas similaridades.
c) Descrever a Engenharia Social de forma conceitual, com exposição de casos.
d) Explanar as ferramentas de Engenharia Social na atualidade e seus principais aspectos.
e) Apontar casos de incidentes aplicáveis à LGPD.

## 1.3 JUSTIFICATIVA:

O presente estudo se justifica com base em alguns pilares estruturados comuns dos projetos científicos, tais como:

I - Com relação ao ponto de vista econômico, por conta dos impactos financeiros sofridos por empresas públicas e privadas diariamente, vítimas de crackers e invasores que são capazes de burlar seus sistemas de proteção e capturar dados sensíveis de clientes, fornecedores e usuários, gerando assim novas demandas de investimentos, que garantam aplicação de melhorias nas políticas de segurança da informação. Esses impactos também afetam financeiramente às pessoas físicas, que sofrem golpes via redes sociais digitais, aplicativos de compras, etc.

II – Do ponto de vista social, pela análise do fenômeno da concepção de marcos legais para reforçar princípios constitucionais já existentes, na busca de ampliar seu efetivo cumprimento.

III - De acordo com o ponto de vista acadêmico, justifica-se a relevância desta pesquisa, estando a ciência em constante processo de construção, necessitando o estudo de caminhos capazes de nortear futuras pesquisas, mais estruturadas, a respeito dos temas abordados, estabelecendo assim um direcionamento.

IV – Para a Ciência e Gestão da Informação, bem como ao PPGGI/UFPR que se insere nesse campo de conhecimento em constante desenvolvimento, se justifica o estudo dessa normativa legal, seus impactos e ações para sua operacionalização, uma vez que é de responsabilidade desta desenvolver esses mecanismos e aprimorá-los.

V - Do ponto de vista pessoal, dos pesquisadores à frente deste estudo, se define como a busca pelo aprimoramento de suas capacidades diante do cenário acadêmico e científico, visando explorar habilidades prévias adquiridas em estudos anteriores, da mesma maneira que a contribuição para este legado de preenchimento das lacunas encontradas acerca dos tópicos expostos.

# 2 REFERENCIAL TEÓRICO

## 2.1 GESTÃO DA INFORMAÇÃO

O surgimento da escrita representa um ponto muito relevante do registro das informações históricas da humanidade, que desde então servem como ferramenta de base às demais gerações. Para Queiroz (2005) a escrita pode ser tida como a forma primária de armazenamento de informações, da qual se pode estabelecer comunicação através do tempo e do espaço. As imagens de pinturas rupestres, encontradas no interior de antigas cavernas, datadas de períodos pré-históricos, sinalizam que a humanidade possa ter dado seus primeiros passos do registro de sua própria história. Os sumérios, na região da Mesopotâmia, foram os responsáveis pelos escritos mais antigos que se tem conhecimento, das civilizações. Desde então, as sociedades passaram a registrar, com cada vez mais frequência a sua história e seu desenvolvimento, de atividades simples como a contagem de seus pertences até dados de maior relevância histórica, como dados censitários.

Segundo Serra (2007) a informação é o resultante do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano, animal ou máquina) que a recebe. Essa informação pode ser organizada e descrita por setores de diferentes campos da sociedade, com o objetivo de analisar suas estruturas e principalmente aquilo que podem evidenciar sobre processos, pessoas, lugares, etc. O conjunto desses dados, descrito de forma lógica e ordenada compõe ciências que visam o estudo de tudo que é existente. Já o conjunto de dados individuais podem ser reconhecidos como a composição do sistema do ser social, suas emoções, anseios, planos, histórias, etc.

Barbosa (2008) descreve a Gestão da informação como a gerência de recursos informacionais, regressando às origens documentais e à preocupação com a armazenagem das informações, para o seu resguardo e para o repasse do conhecimento do conteúdo desses materiais. Tendo como principal atribuição gerir a forma como os dados são organizados, bem como onde isso ocorre. Para estabelecer a otimização das metodologias, previamente empregadas ou não, de armazenamento e controle de dados informacionais. Foi estabelecida então, como ciência

organizacional responsável por descrever e regular medidas para gerir as informações dentro do grupo social.

Ainda sobre a importância que é dada à informação pelo grupo social, a Gestão do seu controle de acesso e armazenamento dizem respeito a salvaguardar algo de extrema importância para o indivíduo, que são partículas de sua própria identidade, registradas em documentos, livros, fotos, afim de preservar essa identificação individual. Barreto (1994) entende que na sociedade atual, a relevância da informação eleva fatores como da sua natureza, seu conceito e principalmente dos benefícios atrelados ao ser social no seu relacionamento com o grupo social. O ciclo dessa atividade se inicia na aquisição do bem principal, a informação, oriunda de diversas fontes, com objetivo de direcioná-las àqueles que precisam dela, organizando-a em sua melhor disposição, com segurança, incluindo o seu processo de descarte.

Para Valentim (2004) a Gestão da Informação faz parte do processo evolutivo da sociedade e das organizações, e seu foco está direcionado em diagnosticar as necessidades informacionais, através da análise de seus fluxos em todas as esferas organizacionais, com objetivo de entregar o produto informacional àqueles que o requerem, através deste sistema. De forma sucinta, pode-se entender que o fluxo dos dados dentro da cadeia de informações, nos ambientes organizacionais, precisou ser otimizado e estabelecido de forma clara e objetiva aos usuários, para que então se pudesse, com segurança, realizar o uso desses dados para embasamento mais preciso das tomadas de decisão. Mais uma vez, se destaca a importância da informação como bem a ser preservado, tanto a nível institucional como social, pois a ela se atribui o valor estratégico, relacionado ao planejamento de metas e objetivos da organização.

Para Choo (2003) a informação é tida como insumo para os processos cotidianos dos indivíduos, que através dos seus sensores (sentidos) de interação com o ambiente, conseguem realizar sua captação. Essa atividade exploratória, e natural, da vida humana transcorre sua vida e lhe proporciona inúmeras experiências, das quais se obtém matéria-prima para suas relações e interações com o meio, num ciclo contínuo. Na correlação dessa percepção humana, com as organizações, é possível associar que o uso da informação como ferramenta para o planejamento estratégico certamente pode trazer diversos benefícios, pois no cenário empresarial é necessário atuar de forma analítica, com base nos dados já coletados no horizonte histórico, para

que se possa estabelecer o caminho a ser trilhado adiante, de acordo com as informações do passado. Esses dados analíticos serão facilmente acessados através de plataformas de SI integradas, que podem trazer aos usuários da Gestão os direcionamentos mais adequados. Se tratando de um banco de dados organizado e preciso, esses resultados serão otimizados. Através do processo de análise da informação, se obtém um o produto almejado pelas organizações, o conhecimento.

Assim como o surgimento da escrita pode ser tido como uma ameaça à existência da memória, por se entender que o mesmo inibiria o exercício dela, o desenvolvimento das condições tecnológicas digitais pode representar uma intimidação ao exercício da escrita, que perdura desde períodos tão primitivos da nossa existência e vem, aos poucos, sendo reduzida e transformada. A escrita digital hoje dá lugar aos inúmeros registros físicos realizados pela humanidade ao longo de sua história. Barreto (2012) expressa de forma minuciosa essa e demais ideias acerca do tema que abrange a ciência da informação, com o propósito de evidenciar que os processos de transição da informação, vividos pela sociedade.

### 2.1.1 Informação Digital:

Da pré-história aos dias atuais, a importância da informação tem se ampliado, juntamente com o seu volume. Lyman (2001) já estimava que a cada ciclo bienal, a quantidade de informações dobrava de volume. A revolução da informação ocorrida no final do século XX, impulsionada pelo desenvolvimento de tecnologias digitais de informação e comunicação passaram a trazer grandes influências para a economia global. A forma como a informação se organiza sistematicamente e os resultados que podem ser obtidos, através do seu uso, atribuem o seu valor principal.

Os sistemas de informação compreendem os métodos pelos quais são disponibilizadas as informações dentro das organizações. Para Audy (2007) o enfoque desses canais é o de articular as tecnologias disponíveis no momento de sua concepção com as necessidades informacionais das diversas esferas da organização. São mecanismos por onde percorrem os dados digitais, de uma ponta a outra, sendo coletados, armazenados e distribuídos de acordo com os protocolos pré-estabelecidos das empresas. Os fatores associados transcorrem pela integração da tecnologia com os indivíduos e a organização, a fim de estabelecer a otimização dos ciclos e fundamentar processos decisórios. Esses sistemas foram e ainda são idealizados pelos seres sociais como uma ferramenta, capaz de auxiliar no gerenciamento das informações nela contidas.

De acordo com Souza (2008) uma Rede Social pode ser definida por um coletivo finito de personagens, realizando suas interações. No contexto tecnológico, essas interações ocorrem através de interfaces online, acessadas através de dispositivos pessoais como tablets, smartphones e computadores, definidas como Redes Sociais Digitais. Para estabelecer relações sociais, em meio a este mundo tecnológico, o ser humano se vê na necessidade de lançar-se a este desconhecido mundo novo, onde precisa se conectar através da rede, para que possa realizar interações. Existem sites e *apps* onde os usuários se comunicam via chat, com diálogos via texto, áudio, vídeo. Muitos desses possuem campos específicos para o compartilhamento de informações a respeito do perfil pessoal e seus históricos, como relacionamentos afetivos, vínculos familiares, dados acadêmicos e profissionais, entre outros.

Vivemos numa realidade onde a grande maioria da população está conectada, de alguma forma; seja através de redes sociais digitais, aplicativos de smartphones, computadores, dispositivos de monitoramento, etc. Essa conexão, muitas vezes silenciosa, coleta e armazena diversos tipos de dados do usuário conectado Fernandes (2013).

Atrelado a ideia do cuidado da saúde e do auto monitoramento, há também uma variedade de itens, disponíveis nas lojas de aplicativos, que através do uso de dispositivos específicos conseguem captar batimento cardíacos, pressão arterial e até mesmo a quantidade de passos dados por um indivíduo. Nesses mesmos aplicativos ainda existem campos onde podem ser informadas a altura, o peso, as comorbidades que um indivíduo possui, etc. A função principal dessas plataformas seria entregar ao usuário ou seu responsável um relatório que contenha o histórico das suas atividades físicas, qualidade de sono, aceleração cardíaca, entre outros. Dieb (2020).

Agra *et al* (2018) entende que o advento da Internet das coisas, que se refere à conexão de objetos e dispositivos em meios digitais, capazes de realizar transmissão de dados, auxilia na otimização da vida cotidiana dos usuários, trazendo mais praticidade às suas atividades rotineiras. Embora haja praticidade, uma grande infinidade de *apps* guardam dados cadastrais básicos dos usuários e até mais detalhados, dependendo de suas finalidades, os quais são fornecidos pelos seus próprios detentores em troca de acesso. Todas essas redes, concentram grandes bancos de dados a respeito do perfil de seus clientes, armazenados desde o dispositivo responsável pela captação, até aos enormes servidores online, que são capazes de guardar essa infinidade de dados, espalhados por todo o mundo.

Um grande volume de dados agrupados, em um SI, assim Morais *et al* (2018) define o conceito de *Big Data*. O constante aumento no número de conexões gera, cada vez mais informação, que é armazenada e precisa ser trabalhada para a geração de resultados. As metodologias anteriormente utilizadas para organização sistêmica desses dados precisaram evoluir de acordo com seu crescimento exponencial. Esses dados podem ser distinguidos em dois grandes grupos, de dados estruturados, que representam aqueles que possuem uma formação definida, como datas, números e grupos de palavras. Já os dados não estruturados são os que não possuem formatos específico, como imagens, textos, dados de mídias sociais, estes precisam ser armazenados e processados por dispositivos que deem o suporte e melhor resultado

da análise. Todos esses dados armazenados podem servir de base para geração de conhecimento, mas para isso precisam ser explorados e analisados. Atualmente os SI já possuem ferramentas específicas capazes de trazer resultados detalhados para buscas específicas, com modelos padrões e repetições.

Grandes organizações se formaram por trás das “fábricas de aplicativos”, bem como da gestão de dados de usuários. A responsabilidade pela triagem, armazenamento e proteção desse patrimônio virtual, pertencente aos próprios usuários, é então gerida pela empresa responsável pela administração das plataformas de redes online, que muitas vezes terceirizam a empresas especializadas. Conforme Matos (2004) de certa forma há muito tempo ocorre a violação de dados pessoais de usuários e na era da internet essa prática se tornou ainda mais facilitada, devido às formas de coleta e envio de informações. Existem “Corretores de Informações”, os quais comercializam informações pessoais identificáveis de inúmeros cidadãos. Esses adquirem, de maneira informal um conjunto de dados de fontes diversas e realizam o cruzamento dos mesmos, sendo capazes de traçar perfis cada vez mais específicos. Após essa compilação, comercializam então esses perfis, muitas vezes com informações que variam de nome completo, CPF, e-mail e telefones de contato, chegando até mesmo sobre histórico de compras e suas preferências. Com a disponibilidade no mercado informal de dados de usuários, então as empresas comerciais podem agir de maneira proativa com relação à sua abordagem ao cliente.

### 2.1.2 Arquitetura Informacional

No conceito concebido por Wurman (1997), a arquitetura da informação pode ser entendida como uma expressão que determina a organização dos dados dentro da interface de um sistema. Essa organização diz respeito à similaridade do processo de projetar uma residência ou edifício por parte de um arquiteto, que necessita transcrever suas ideias primárias, utilizando um sistema de medidas padrão, criando assim um escopo, que será desenvolvido, posteriormente aplicado na construção. Para a Tecnologia da Informação, utilizando essa analogia, entende-se como necessário a criação de um projeto de dados, para o desenvolvimento de novos sistemas de informação.

As perspectivas de dimensão são as ferramentas de destaque desse caso análogo, tendo em vista que a projeção dos sistemas se baseia num dado planejado. Essa projeção permite aos gestores desses ambientes virtuais uma melhor organização dos dados, para facilitar o seu acesso posterior (Camargo e Gregório 2011). Essa metodologia procura estabelecer maior organização na criação e desenvolvimento de ambientes digitais. Tais como as plantas de imóveis, que servirão de base aos engenheiros e demais profissionais da área da construção civil, os projetos de AI visam estabelecer, de forma otimizada, o local e o formato dos dados inseridos nesse plano digital. Seu principal objetivo é o de mensurar a melhor maneira para a construção de um sistema de informações, analisando desde os recursos tecnológicos disponíveis, bem como o que se busca atender com sua projeção, para atender às demandas da organização com relação ao produto informacional.

Tendo por objetivo principal facilitar a gestão dos dados no ambiente virtual, o uso da Arquitetura da Informação também promove vantagem competitiva, pois proporciona aos gestores uma visão ampla e previsível do projeto como um todo, podendo inferir na programação de conteúdo antes mesmo da sua alocação. Já o benefício destacado por Rocha *et al* (2020) é o de resgatar dados compilados em um sistema complexo, uma vez que na história da criação de sistemas informacionais, uma das maiores dificuldades enfrentadas por técnicos e analistas tinha relação direta com a recuperação das informações já geradas, em meio a um grande volume de dados de maneira desordenada. Uma vertente que se abre para análise sobre esse estudo, tem relação direta com a falta de segurança a qual estes dados estavam

submetidos, uma vez que não havendo protocolos prévios para a organização, o acesso a esse conteúdo por parte de invasores torna-se ainda mais suscetível.

Para Zachman (1987) a definição de *Framework* está ligada à Arquitetura de Sistemas Informação, a qual em sua visão na época tratava-se de uma figura de linguagem bastante técnica e restrita à visão acadêmica. O *Framework* é tido como uma base codificada de dados genéricos, que serve de modelo para o desenvolvimento de novas aplicações. Um dos pioneiros da arquitetura corporativa, desenvolveu um modelo capaz de auxiliar desenvolvimentos futuros neste âmbito. Em seu escopo 5W1H, buscava delinear em colunas e linhas matriciais, perguntas organizacionais e direcionadoras. A sigla refere-se às letras iniciais das perguntas anteriormente mencionadas, no idioma inglês, sendo elas: "*What* – O que?", "*Where* – Onde?", "*Who* – Quem?", "*When* – Quando?", "*Why* – Por quê?" e "*How* – Como?". Esse modelo concebido por John Zachman, em meados da década de 1980, quando este prestava serviço à *IBM* estabeleceu um ponto de extrema importância na Arquitetura Informacional, pois foi com base nesse modelo aplicado que muitas empresas passaram a desenvolver suas matrizes.

Embora represente um grande marco para a Arquitetura de Sistemas, o modelo de Zachman também foi alvo de apontamentos acerca de sua efetividade, pois trata-se de um produto que passou a ser comercializado. Define Belloquim (2010) que o *The Open Group Architeture Framework* também se trata de um modelo de framework relacionado à arquitetura corporativa, desenvolvido por uma entidade sem fins lucrativos denominada "*The Open Group*", que se estabeleceu através do estudo prático das limitações encontradas nos modelos propostos por Zachman, tendo em vista que essas ideias de aperfeiçoamento estariam restritas às empresas administradas por Zachman, através apenas de consultorias prestadas. Esse modelo trata-se de uma aplicação aberta, ou seja, de forma gratuita, com a possibilidade de customização. Embora as divergências no contexto dos negócios, ambos os modelos expressam a preocupação com a arquitetura organizacional das empresas, tendo em vista que a gestão dos dados de maneira ordenada tem por base estabelecer e otimizar princípios da Segurança da Informação a fim de garantir a privacidade dos indivíduos cujos dados são coletados, tratados e armazenados pelos diversos SI.

### 2.1.3 Segurança da Informação e Privacidade

Em termos gerais, segurança se define como um conjunto de medidas e proteção de riscos, perigos ou perdas a pessoas ou coisas (Michaelis, 2020). Entende-se como um processo contínuo de fortalecimento de mecanismos que visam a proteção de algo, com ações de prevenção a fim de estabelecer medidas inibidoras de riscos. Está atrelado a ideia de manter-se em equilíbrio, contra ações fortuitas no ambiente social, para que possa gerar tranquilidade e bem-estar aos indivíduos. Já o conceito de privacidade está diretamente relacionado ao resguardo daquilo que não se pretende mostrar, exibir ou compartilhar com outro (s) indivíduo (s), relativo à vida íntima, aquilo que se deseja manter oculto.

Para Baars (2011) a segurança da informação é algo que existe desde o antigo Egito, há mais de 2.000 anos, onde utilizavam hieróglifos não padronizados esculpidos em monumentos para restringir a leitura de um dado, apenas por pessoas designadas a tal atividade, a fim de promover até mesmo a segurança física dos seus bens e dos seus impérios. Nota-se até os dias atuais que a segurança da informação tem sua importância relacionada desta forma, ou seja, os protocolos de restrição de acesso aos dados organizacionais ou pessoais tem como principal objetivo de resguardo do seu valor, bem como da privacidade dos indivíduos.

Entende-se com Agra *et al* (2018), que avançando na era da informação, um dos princípios os quais necessitou se aprofundar, para estabelecer uma melhor relação entre os agentes deste universo conectado, foi o desenvolvimento de medidas de segurança da informação. Diversos cenários, anteriormente considerados comuns e livres de perigos, passaram a ser vistos como vulneráveis e suscetíveis a ameaças. Os sistemas outrora desenvolvidos, que não contavam com o planejamento e todo escopo estabelecido, pelos meios da arquitetura de informação, passaram a ser estruturados com tecnologias mais inovadoras, empregando ferramentas capazes de salvaguardar o patrimônio informacional das organizações.

O estabelecimento e a manutenção da Segurança Informacional representam relevantes desafios para a Tecnologia da Informação (TI), de acordo com Barreto *et al* (2018), pois o aumento no número de episódios de invasão aos sistemas empresariais, nos quais se obtém acesso às informações de clientes, funcionários, dados financeiros, etc., requer a necessidade de revisão de políticas já estabelecidas

no intuito de avaliar as suas vulnerabilidades. As empresas investem em mecanismos cada vez mais modernos, visando a diminuição do risco.

Dentro das concepções aprimoradas, de metodologias desenvolvidas, para novo protocolos de segurança, que visam garantir a eficiência na gestão de dados, são inúmeros os manuais técnicos e ferramentas para os profissionais. De acordo com Barreto *et al* (2018), são três os fatores básicos que devem ser associados com relação à segurança do patrimônio informacional, como seu valor e contexto organizacional, seu ciclo de vida e sua classificação quanto à confidencialidade. Partindo dessas premissas, pode-se então desenvolver uma sólida Política de Segurança da Informação (PSI). Também é ressaltado que a engenharia social pode se desenvolver livremente num universo onde os técnicos de TI não buscam a atualização de suas ferramentas, sem a realização adequada de um inventário informacional, capaz de aferir um valor a este patrimônio.

Um dos fatores de extrema importância para as definições de PSI, de acordo Agra *et al* (2018), é a definição de usuários e seus níveis de acesso. Quais áreas da organização detém controle sobre os dados e seu processamento, aferindo liberações de acordo com os procedimentos adotados. Essa medida visa delimitar acesso às informações apenas a quem for necessário, na tentativa de estabelecer um alto nível de privacidade dos dados. Essa ferramenta gerencial de controle deve ser compartilhada entre as esferas de Gestão e de TI da organização, estabelecendo diretrizes resguardem os níveis de privacidade.

Silberschatz (2020) destaca que as persistentes falhas nas políticas de segurança é que deram início à preocupação com a manutenção do direito à privacidade dos indivíduos. Essa preocupação diz respeito aos governos nacionais, que precisaram estabelecer regulamentações, além de instituir meios de conscientização sobre segurança virtual. Falhas de grandes proporções trouxeram aos noticiários e à mídia uma série de relatos de episódios, cada vez mais frequentes de vazamentos de dados.

Uma das primeiras legislações acerca do tema de privacidade surgiu na Europa na década de 70, mais especificamente na Alemanha, em Hessen. Naquele tempo o desenvolvimento da tecnologia de comunicação e informação que serviria de base para a criação de computadores atuais era bem primária e pouco acessível, porém seu avanço estava em constante desenvolvimento. Com a introdução desses

mecanismos, o estado alemão viu a necessidade de elaborar normativas referentes à privacidade no país. Aí então o conceito de proteção de dados passou a ser estabelecido no âmbito jurídico. Com o surgimento dessa regulamentação, diversos países europeus como Áustria, França, Noruega e Suécia passaram a tratar com mais importância esse tema e criar suas próprias leis referentes a proteção das informações dos cidadãos. Anos mais tarde, na década seguinte, o então Conselho Europeu auxiliou no desenvolvimento da unificação dessas normas sobre tratamento automatizado de informações pessoais. Então, em 1995 passou a vigorar a Diretiva da União Europeia, que reúne regulamentações de privacidade de 28 países (Russel, 2017).

## 2.2 ENGENHARIA SOCIAL:

A Engenharia Social pode ser definida como um conjunto de técnicas de manipulação de pessoas, capaz de persuadi-las a executar ações que podem ser prejudiciais a si mesmas (Mann, 2018). Essas ferramentas de manipulação têm associação direta com o objetivo de subtrair para si algo de posse de terceiros.

No estudo de Popper (1945) a respeito da Mecânica Social, que pode ser entendida como uma forma de planejamento para uma ação intervencionista, que busca intervir no itinerário do grupo social, direciona a ideia de que a correlação dos termos Mecânica e Engenharia denota essa manipulação em um sistema intangível, a fim de atender interesses de um grupo específico, que deseja obter o controle.

Mitnick (2003) estabelece que o termo foi popularizado na era da internet, porém teve sua origem há muito tempo atrás, quando era utilizado para definir o ato de ludibriar pessoas. Num tempo onde a checagem das informações era bem mais precária, a confiança na palavra de um cidadão era algo de grande valia. Os Engenheiros sociais, que podem ser entendidos como estudiosos informais do comportamento, utilizavam desses meios para captar as maiores fraquezas dentro dos sistemas sociais, principalmente àqueles relacionados a aquisição de bens, para que pudessem tirar vantagens.

Para Peixoto (2006) existem milhares de engenheiros sociais pelo mundo, que agem de formas diversas, trabalhando em prol de seus próprios objetivos e às vezes de terceiro, porém existiram na história dois dos que mais se destacaram nesta atividade, sendo um deles Frank Abgnale W. Jr. e outro Kevin D. Mitnick.

De acordo com Peixoto (2006), Frank Abgnale foi um dos maiores fraudadores já identificados nos EUA, na década de 1960. Através de sua inteligência observacional, conseguiu desenvolver formas de falsificar cheques bancários, através dos quais trouxe prejuízo de alguns milhões de dólares aos bancos da época. Usava técnicas para descobrir o funcionamento do sistema bancário, as lógicas numéricas sequenciais impressas nos documentos e assim foi capaz de configurar mecanismos próprios para enganar o sistema. Além de fraudador, também foi condenado por falsidade ideológica, tendo se passado por diversos personagens, que protagonizavam papéis influentes no ciclo social em que se inseria, como médico, advogado e piloto de aeronaves. Sua história ficou conhecida mundialmente e após

sua prisão, passou a trabalhar no serviço de identificação de fraudes do FBI (Federal Bureau of Investigation – Departamento Federal de Investigação em português). Frank cresceu na era das negociações formalizadas em meios físicos não eletrônicos, as falsificações faziam parte do arsenal de ataque dos Engenheiros Sociais, que estruturavam metodologias de aplicação de golpes por meio da forja de documentos frios, se passando por verdadeiros. Assim os alvos mais atacados eram comércios e bancos. As técnicas aplicadas geralmente permeiam em torno de usar da psicologia para analisar as falhas dos sistemas e das pessoas nele envolvidas. Através dessa análise é possível verificar brechas que podem ser tidas como a porta de entrada para atuação dos golpes. O fator humano da análise para validação pode ser apontado como o elo mais fraco dessa corrente, pois nele se incidem as aplicações de golpes. A história tornou-se tão conhecida mundialmente que foi transformada em filme, pelo estúdio da produtora americana Dreamworks, em 2002. Com o título “Catch me if you can” (Prenda-me se for capaz, em inglês), narra a história de Abgnale desde sua infância e adolescência, com aprendizado de pequenos golpes até a sua prisão pelo FBI, onde passou a integrar a equipe de investigação de aplicações de golpes no país.

Também em Peixoto (2006) é observado que Kevin D. Mitnick começou a sua trajetória no início da era das tecnologias digitais e informatizadas nos EUA, quando era apenas um adolescente, que através de dos seus dons de análise e observação descobriu formas de viajar “gratuitamente” de ônibus pela cidade, utilizando bilhetes descartados na lixeira. Com estudo prévio sobre a forma de confecção das validações mecânicas nos bilhetes, passou então a emitir seus próprios *tickets*, que lhe permitiam circular por toda sua cidade. Depois disso, aprendeu também a fraudar sistemas de companhias telefônicas, através da violação das centrais dispostas em ruas e avenidas pouco movimentadas, onde pode, com o uso de ferramentas simples entrar em contato com as centrais de suporte, para realizar ligações sem que fosse cobrado por elas. Com o tempo passou a acompanhar outros jovens que tinham como hobby a prática de invasão em sistemas online, para divertimento, o que acabou se tornando uma atividade rotineira. Ficou conhecido mundialmente como um dos maiores crackers da história, após sua prisão, pela invasão de sistemas e acesso de dados de pessoas em importantes posições do governo norte americano. Atualmente está à frente de uma grande empresa de segurança da informação, onde faz o uso de seu

conhecimento em prol da criação e gerenciamento de sistemas capazes de barrar invasores.

Relata Mitnick (2003) que a Engenharia Social não é utilizada apenas em sistemas mecanizados e informatizados que envolvem tecnologias, é também empregada sobre o ser e o grupo social, do qual se obtém informações acerca do seu funcionamento, através de uma análise minuciosa de comportamentos e o emprego de formalidades, que podem ser tidas como chaves, que acessam a informação pretendida.

Em ambos os casos destacados por Peixoto (2006), a inteligência que outrora foi utilizada em benefício próprio e rendeu aos seus autores o peso de diversos crimes cometidos, posteriormente foram direcionadas na forma de apoio aos sistemas que trabalham para combater as fraudes.

Num contexto mais atual, apresentado no formato de documentário a *Netflix* relata a história vivida por diversas mulheres na Europa, vítimas do intitulado “Golpista do Tinder”, que dá o nome à atração. O relato conta os casos de estelionato aplicados pelo israelense Simon Leviev, que através do aplicativo de relacionamentos *Tinder* usava suas técnicas para atrair as vítimas. Em seu perfil exibia uma série de fotos e vídeos ostentando sua suposta posição social e financeira, se passando por filho de um bilionário herdeiro de uma empresa do comércio de diamantes. Nesse incluía uma série de viagens em jato particular, acessórios e roupas de marca, festas exclusivas, restaurantes e hotéis de alto nível, carros importados, etc. Após fisgar suas vítimas, passava a se entrelaçar com as mesmas em relacionamentos amorosos, nos quais conseguia estabelecer a confiança destas. Com o passar do tempo, consolidado o envolvimento, passava então a criar situações de pânico nas vítimas, relacionadas a sua segurança, como supostos ataques sofridos por grupos comerciais inimigos que estariam o perseguindo e o ameaçando. Com isso, solicitava empréstimos rápidos às vítimas para poder se manter. Nesse tempo criou uma rede de vítimas, com as quais mantinha contato simultaneamente, chegando aos valores estimados de cerca de US$ 10 milhões em golpes aplicados. Rosa (2022) aponta o direcionamento da ação de Simon sobre a vulnerabilidade afetiva das pessoas envolvidas nos golpes, como uma lacuna emocional. Na tentativa de suprir carências afetivas, as vítimas acabavam se envolvendo sem se questionar sobre os possíveis impactos.

### 2.2.1 Agentes Envolvidos na Cadeia da Engenharia Social:

Para McClure *et al* (2014) *Hacker* ou invasor é a nomenclatura utilizada na Segurança da Informação para definir o agente do sistema que, através de suas habilidades e conhecimentos técnicos, é capaz de burlar ferramentas de proteção dos sistemas e obter acesso às informações nele contidas. Essa figura geralmente possui experiência na análise das estruturas de rede, das quais se baseiam as formações de sistemas. Nessa cadeia ele pode também ser identificado como Engenheiro Social, figura que exerce o papel da aplicação dos mecanismos de persuasão, a fim de ludibriar suas vítimas para obtenção de vantagens sobre elas.

Em Barreto (2018), se tratando do invasor, este pode assumir diferentes papeis, definidos pela sua forma de atuação. Um impostor seria definido como um atacante que utiliza as credenciais com identificação de um usuário legítimo. Já o infrator se destaca por ser um usuário legítimo realizando ações cujas autorizações não lhe são concedidas. De outra forma, o usuário clandestino se define pela ação de tentativa de bloqueio ou exclusão dos registos de sua presença e suas ações no sistema.

Os crackers, do inglês “crack”, traduzido livremente como “quebra”, são popularmente conhecidos por essa nomenclatura por estarem diretamente ligados à quebra dos protocolos de segurança da informação, estabelecidos nos SI, na busca da obtenção de dados sigilosos que possam ser úteis para as suas futuras ações. Geralmente são indivíduos com forte ligação à prática do uso de sistemas diversos e vasto conhecimento da área de informática. Suas principais ações envolvem ataques cibernéticos em sistemas empresariais, dos mais simples aos mais complexos, para obter a matéria prima de suas futuras ações. O termo cracker se diferencia de hacker, na atual concepção, por se tratarem de perfis mais voltados ao crime, desestabilizar sistemas, estabelecer o caos e a autopromoção. O Hacker pode ser entendido como um indivíduo preocupado com o auxílio aos usuários e promoção do conhecimento (Techmundo, 2012).

Além desses agentes e suas definições de atuação, existem também os mecanismos utilizados para atuarem como invasores, ou seja, programações de sistemas para invasão automática. Os *masters* são tidos como computadores controlados pelos *crackers,* que são programados e realizam infinitas tentativas de invasão. Os zumbis que também são máquinas programadas e controladas pelos

crackers, possuem ferramentas de disparos automáticos de ataques aos usuários de meios eletrônicos, a fim de realizar a captação de dados. Barreto (2018).

Já as vítimas podem ser apontadas como usuários de sistemas, redes sociais digitais, clientes e funcionários de empresas, etc. São cidadãos comuns, os detentores primários desse bem de grande importância, capaz de identifica-los ou às suas organizações. Através do uso e manutenção dessas relações com os meios virtuais é que se constituem transações, de acesso em troca de informações pessoais. McClure (2014) estabelece que qualquer usuário estaria sujeito à aplicação de golpes, sendo as informações que este possui, de relevância para obtenção de alguma vantagem. Assim sendo, a ação dos Engenheiros Sociais pode se aplicar a qualquer pessoa.

### 2.2.2 Tipos de Engenharia Social na Atualidade:

Na era da informação, de forma estruturada, se estabeleceram diversos tipos de ferramentas da Engenharia Social, as quais são tipificadas de acordo com o mecanismo para sua atuação. A categorização, proposta pelo autor e disposta no Quadro 1, visa evidenciar os critérios pelos quais são tipificadas essas ações:

QUADRO 1 – TIPOS DE ENGENHARIA SOCIAL:

| TIPO | Descrição | Mecanismos | Ferramentas | Objetivos | Alvos |
|---|---|---|---|---|---|
| **DUMPSTER DIVING** | Roubo de materiais descartados pelas vítimas, que possam conter informações de valor. | Vasculhar o lixo de pessoas ou empresas. | Lixeiras e descartes de materiais. | Obter dados pessoais da vítima ou da empresa a que está vinculada, para aplicação de outros golpes. | Pessoas Físicas, Empresas |
| **PHISHING** | São encaminhados links falsos para e-mail ou celular das vítimas, que acessam páginas falsas que capturam seus dados. | Endereços da web abreviados ou links errados que direcionam para páginas falsas. | Telefone, SMS, E-mails; | Obter dados pessoais da vítima ou da empresa a que está vinculada, para aplicação de outros golpes. | Pessoas Físicas, Empresas |
| **PRETEXTING** | Os criminosos entram em contato com funcionários de empresas, buscando realizar testes/confirmação de dados. | Ligações de voz ou e-mails de supostos técnicos, solicitando confirmação de dados de acesso. | Telefone, E-mails; | Acessar sistemas internos de empresas, para roubo de dados, para aplicação de outros golpes. | Empresas |
| **QUID PRO QUO** | Invasores entram em contato com vítimas, se passando por técnicos de suporte, para supostamente oferecer ajuda às vítimas | Arquivos maliciosos que são instalados em conjunto com programas baixados pela própria vítima. | E-mails, downloads de arquivos; | Instalar softwares mal intencionados nos dispositivos das vítimas, para roubo de dados pessoais. | Pessoas Físicas, Empresas |
| **SCAM** | Envio de cartas falsas para estrangeiros, com histórias falsas a respeito de doações de dinheiro ou envolvimentos afetivos. | Textos persuasivos a respeito de vantagens financeiras e afetivas para a vítima. | Cartas, E-mails, Mensagens; | Extorsão das vítimas através do envolvimento afetivo | Pessoas Físicas |

| | | | | | |
|---|---|---|---|---|---|
| **SEXTORSÃO** | Captura de arquivos confidenciais de caráter íntimo que são utilizados para chantagear as vítimas. | Extorsão através do uso da imagem da vítima, em situação íntima. | Chats de Relacionamento, Redes Sociais digitais. | Extorsão das vítimas através de chantagem. | Pessoas Físicas |
| **SHOULD SURFING** | Análise das vítimas no uso de seus dispositivos pessoais, no objetivo de capturar senhas. | Observar o uso dos dispositivos pelas vítimas, na expectativa de visualizar senhas. | Celulares e Computadores | Obter senhas de acesso aos dispositivos da vítima. | Pessoas Físicas |
| **SMISHING** | Compartilhamento de links maliciosos, via mensagens de texto. | Endereços da web abreviados ou links errados que direcionam para páginas falsas. | Telefone (SMS/Mensagem); | Obter dados pessoais da vítima ou da empresa a que está vinculada, para aplicação de outros golpes. | Pessoas Físicas |
| **SPEAR PHISHING** | Na posse de informações personalizadas, os invasores têm acesso aos setores de empresas. | Disseminação de informações falsas, como alertas, para funcionários e até mesmo clientes de empresas. | Telefone, E-mails; | Causar pânico e confusão nas vítimas. | Empresas |
| **TAILGATING** | Através da boa vontade das vítimas, criminosos se passam por entregadores ou prestadores de serviços e solicitam acesso, para adentrar ambientes restritos e realizar furtos. | Acesso a locais físicos restritos. | Conversação presencial / Interfones | Realizar furtos de objetos em residências ou empresas. | Pessoas Físicas, Empresas |
| **VISHING** | Criminosos realizam abordagem por chamadas de voz, informando sequestro de pessoas próximas da vítima. | Técnicas de persuasão, se fazendo passar por parentes, conhecidos, colegas de trabalho. | Telefone (voz); | Extorsão das vítimas através do medo. | Pessoas Físicas |

Fonte: COMPUGRAF (2020).

De acordo com as informações apresentadas no Quadro 1, se evidencia que os ataques mais comuns são realizados via meios digitais, principalmente através do uso da conexão com a internet, através de mecanismos de comunicação entre usuários, como mensagens instantâneas, chats e e-mails e até mesmo ligações. O

uso da formalidade e padronização, de acordo com modelos empresariais padrões darão mais credibilidade às comunicações, a fim de conquistar algum nível de confiança das vítimas. O foco contido nos ataques está sempre ligado à obtenção de informações mais precisas, com objetivo de aplicar novos (e maiores) golpes, onde se possa obter até mesmo ganhos financeiros. No entanto, os ataques não se resumem àqueles que ocorrem via meios digitais, através da internet, mas também pelo telefone ou mesmo presencialmente, como abordagens de falsos vendedores ou funcionários de empresas de prestação de serviços, para adentrar casas, condomínios ou empresas, para obtenção de acesso aos locais e possíveis furtos. Também existem casos mais extremos, com a ação dos invasores de vasculhar o lixo das vítimas na procura de dados e informações que possam ser de utilidade para outros golpes mais elaborados (Compugraf, 2020).

### 2.2.3 Natureza da Engenharia Social:

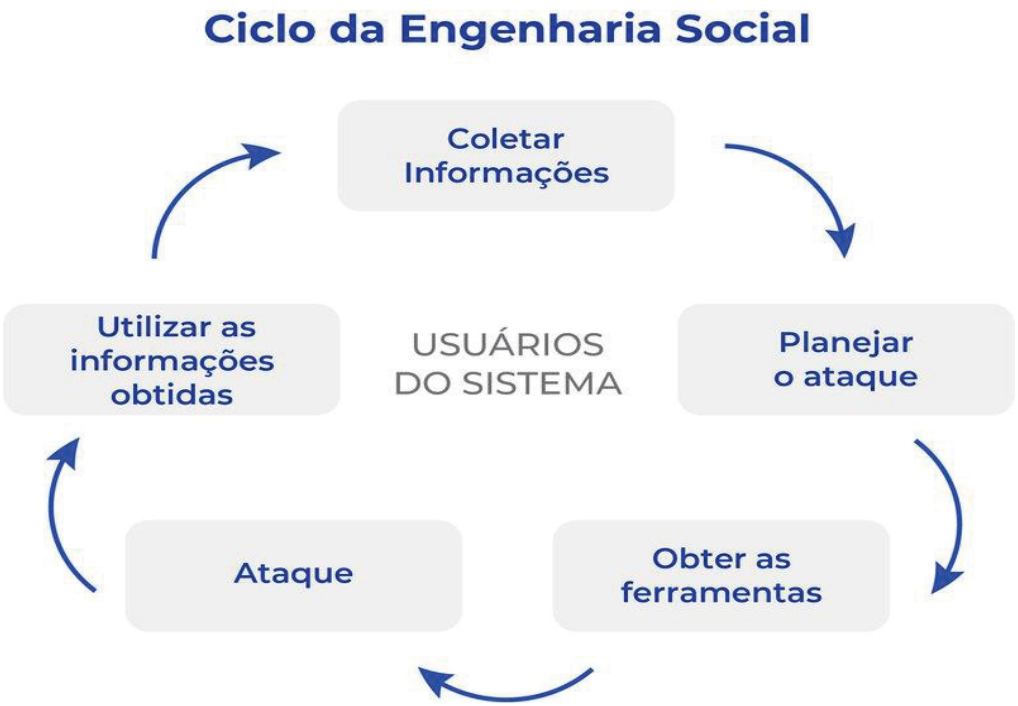
Para Topolniak *et al* (2021) a Engenharia Social não é uma ferramenta que se aplica somente ao universo da Internet, porém essa tecnologia é que trouxe maior espaço para sua atuação. Uma vez que a navegação de dados pode fluir um conjunto infinito de informações de uma ponta a outra do mundo no mesmo instante, traz consigo a facilidade exploratória dessas técnicas. Os bancos de dados formados por instituições, que coletam e armazenam informações cadastrais dos seus clientes, são similares ao baú de um tesouro para os engenheiros sociais. Através do seu acesso é que se obtém uma ferramenta muito importante para sua atuação, os dados sensíveis. Quando ocorre a identificação do indivíduo dentro desse compilado de informações é que se possibilita a aplicação de golpes. Em posse de seus contatos e informações pessoais, uma pessoa ou mesmo grupo criminoso organizado poderá atuar. Então, em contato com esse usuário é possível ofertar-lhe produtos ou serviços enganosos, se passando por funcionário de empresas comerciais conhecidas.

No contato com as vítimas também é possível ampliar esse banco de dados, coletando novas informações que está repassa, sem perceber o risco. Chamadas telefônicas de supostos funcionários de bancos, solicitando confirmações, ou mesmo via *e-mails*, mensagens *sms*, alertando fraudes e requerendo confirmações eletrônicas de dados cadastrais ou senhas são tidos como portas de entrada para os invasores. Através da coleta desses dados, poderão atuar então nas fragilidades das vítimas e assim podendo obter recursos de valores subtraindo da mesma.

O ciclo da Engenharia Social se configura através do passo inicial da coleta de informações e dados das possíveis futuras vítimas, o que abre espaço para planejamento do ataque/golpe, pois é através desses dados que se pode traçar um perfil e suas vulnerabilidades. Ao se planejar o golpe, é necessária a obtenção de ferramentas para sua execução, seja a criação de textos falsos de e-mails, mensagens *sms* ou de aplicativos próprios, até os mais sofisticados, como geração de documentos, cartas, certificações falsas. O ataque em si é a interação do Engenheiro Social com sua (s) vítima (s) através do mecanismo de escolha a ser utilizado, mais adequado para sua execução. Nesse ataque, geralmente o Engenheiro Social irá obter informações amis precisas, que lhe concederão acesso a outros mecanismos, como contas bancárias, acesos a contas de e-mail, aplicativos de

compras, cartões de crédito e isso lhe possibilitará a aplicação de novos golpes, gerando assim uma cadeia de aplicações (Compugraf, 2020).

Figura 1 – Ciclo da Engenharia Social




Fonte: COMPUGRAF (2020)

O enfoque dessa relação gira em torno da obtenção de informações e essa cadeia é retroalimentada pela produção infinita de dados, diariamente, tendo em vista que o uso e acesso das redes produz cada dia mais milhares dessas informações, que quanto mais detalhadas, tornam mais próximas para sofrer os ataques. O fenômeno do Big Data exige das organizações o desenvolvimento e uso de ferramentas mais aprimoradas para compilação das informações coletadas e armazenadas. Os protocolos para segurança dessas informações requerem também constantes atualizações, para salvaguarda do patrimônio informacional. Para Coelho *et al* (2013), da mesma forma como as ferramentas de tecnologia para defesa dessas informações são aprimoradas, as mecânicas para quebra de sua proteção também serão ampliadas, uma vez que se conhecendo o caminho para o desenvolvimento de um sistema, poderá então se conhecer as suas falhas e mecanismos básicos de atuação.

## 2.3 LEI DE PROTEÇÃO DE DADOS

Na concepção de Rohling (2014) a origem etimológica da palavra Lei vem do latim "*lex*", do verbo legere, lectum – ler. E é um sistema de regras que são criadas e executadas por meio de instituições sociais ou governamentais para regular comportamentos. É também definida por ele como "ciência ou arte da justiça". Para uma sociedade, esse sistema de regras permite organizar os campos em que se dividem a sociedade, a fim de estabelecer direitos e deveres de cada personagem dentro deste universo. Sendo necessário, para cada novo segmento que surge, oriundo das vivências dessa sociedade, pautar novas regras para que se enquadrem como as demais já existentes.

Com base em Pereira (2010), pode-se entender que o meio social se desenvolve através das relações dos seres sociais, existentes nesse grupo. Para cada nova relação, de acordo com os costumes, crenças e princípios da época, são adotadas normas cada vez mais específicas, na busca de padronizar a forma como os indivíduos deverão se portar diante daquela vivência. A Lei pode ser tida então como um manual de regras sociais, que visa instruir os seres sociais.

Na era a qual vivenciamos, o valor dos ativos de dados continua a ser visto com a mesma ótica das sociedades pré-históricas, diferenciado é claro, pelos processos de gestão, que evoluíram a cada período, trazendo mais segurança à armazenagem e acesso. Para Oliveira (2019), a informação como um ativo imprescindível de uma organização, independentemente da sua dimensão ou área de atuação, sendo que o profissional responsável pela gestão desse ativo necessita possuir a capacidade de mensurar sua importância e valor.

Nunes (2019) entende que tratamento de dados inclui toda a operação realizada com dados pessoais, desde a sua coleta, produção, recepção, transmissão até a sua difusão ou extração. Para todos esses processos, existe a necessidade prévia de consentimento do seu titular, de como serão utilizadas essas informações, então é preciso que este autorize expressamente esse tratamento. Com o passar dos anos, através de marcos legais, é que foi estabelecida a ideia de que o ser social é o detentor e proprietário de seus próprios dados e cabe a ele definir se gostaria de fornecê-los a terceiros.

Com o avanço da tecnologia e das ciências informacionais é que foi possível estabelecer novos e otimizados meios de resguardar os dados de usuários, através de sistemas de armazenamento eletrônicos, protegidos por senhas e até mesmo criptografias, com o intuito de dificultar a ação de terceiros sobre esses dados. De acordo com César Júnior (2011) é prudente refletir sobre a necessidade de um tratamento adequado que viabilize o processo de armazenamento, organização, busca, recuperação e preservação dos dados e das informações geradas a partir de pesquisas. Caso contrário os dados coletados podem se tornar inelegíveis ou o que seria mais drástico, se perder em um grande volume de dados, por falta de tratamento técnico adequado.

Além disso, de acordo com Sayão (2012) dados e informações digitais gerados pelas atividades de pesquisa necessitam de cuidados específicos, tornando-se necessário a criação de novos modelos de custódia e de gestão de conteúdos científicos digitais que incluam ações de arquivamento seguro, preservação, formas de acrescentar valor a esses conteúdos e de otimização da sua capacidade de reuso.

Como visto em Pereira (2010) tendo então por base que o princípio legal é a regra que permeia a sociedade, então através dos tempos tornou-se necessário regulamentar o que ainda não estava regulamentado, ou mesmo explicitar de forma mais detalhada àquilo que ainda não havia sido pensado pelo grupo social. Entendendo-se a importância da segurança dos dados, dos cidadãos de uma sociedade, e constatando-se que não haviam mecanismos legais precisos para que resguardassem esse direito é que foram surgindo discussões acerca deste tema, afim de estabelecer a ferramenta pela qual se pode instruir os seres sociais.

Para Assis e Mendes (2020) em países como os EUA e também na União Europeia, essas discussões foram levantadas mais cedo, pela ocorrência de séries de episódios de vazamento de dados, onde foi evidenciada a vulnerabilidade dos cidadãos diante da situação em questão.

### 2.3.1 Marcos Legais

#### A) Lei 12.965/14 - Marco Civil da Internet:

Leite (2014) define como um “presente” aos brasileiros, o instrumento conhecido como Marco Civil da Internet. Sancionado no ano de 2014 pela então presidenta Dilma Rousseff, este prevê os princípios que devem nortear o uso da internet em todo o país, a partir de então. Suas garantias aos usuários visam estabelecer a liberdade da expressão, comunicação e manifestação do pensamento, tal qual é previsto na CF.

Esse instrumento media as formas de relações que podem se estabelecer através do uso dessa rede, bem como do seu acesso, com enfoque na organização do espaço a fim de impor medidas de controle sobre as ações, que há muito vinham sendo debatidas, como por exemplo sobre fluxos de navegação. Se destaca em sua composição um item que se desdobra em diversos fatores, relacionados principalmente com a privacidade e a proteção de dados dos usuários. Após episódio de invasão e exposição de comunicações de agentes governamentais, que gerou certa instabilidade política no país, essas instituições se viram na necessidade do estabelecimento de normativa legal que pudesse resguardar seu direito à privacidade enquanto cidadãos.

Sua formulação foi amplamente debatida entre os membros da câmara dos deputados, por se tratarem de definições já previstas na constituição e que possuíam vasta jurisprudência para sua resolução (Gonçalves, 2016). O enfoque em mediar relações no âmbito digital pode ser tido como uma instrumentação para o atual cenário tecnológico. As determinações sobre privacidade e direito de expressão, contidas na CF, foram detalhadas a fim de se estabelecesse um protocolo de atuação dos agentes nesse ambiente já conhecido e explorado. Com a definição dos papéis principais, com direitos e deveres, visa exprimir a regulação da atividade de cada membro desse sistema.

A constante evolução das tecnologias digitais e o salto exponencial do número de usuários com acesso à internet trouxeram mudanças às relações sociais. A informação trazida de forma quase que imediata propicia aos indivíduos a ampliação do seu conhecimento. Esses representam resultados benéficos possibilitados através

da era digital. Conforme detalha Gonçalves (2016), os cidadãos enquanto usuários, passam a ter o pleno direito ao acesso à internet, como exercício de sua cidadania. A liberdade de expressão e pensamento, com previsão ao seu anonimato para proteção de sua imagem e segurança. O dever é de estar de acordo com as medidas impostas relacionadas ao respeito aos demais usuários. Também há previsões quanto à privacidade e sigilo dos seus dados, pela não exposição do seu fluxo de comunicações, salvo por ordem judicial. Aparecem também especificações a respeito do trânsito de dados, garantindo ao cidadão o direito de propriedade das suas informações, proibindo o fornecimento à terceiros por quaisquer detentores intermediários, se não em casos específicos já previstos, relacionados às medidas de ordem jurídica. As empresas, detentores de patrimônios informacionais, o dever de resguardá-los sob sua tutela, com responsabilização legal para o caso de divulgação e comercialização indevida. A regulamentação devida e detalhada para o comércio eletrônico, ferramenta amplamente difundida até então e que não possuía bons e específicos direcionamentos. Os agentes governamentais, recebem então a ampliação das suas responsabilidades no exercício da função de auditores das atividades nesse âmbito tecnológico.

**B) Lei 12.737/12 – “Carolina Dieckmann”:**

Antes mesmo da homologação do Marco Civil da internet, de acordo com a repercussão obtida pelo episódio envolvendo a atriz global Carolina Dieckmann, no qual teve seu computador pessoal invadido por *crackers* e suas fotos e conversas íntimas foram divulgadas sem a sua autorização, foi sancionada a Lei 12.737/12 que ficou conhecida como “Lei Carolina Dieckmann”, que se trata de uma alteração no Código Penal Brasileiro, para tipificação de crimes cometidos em meios cibernéticos. Essa ação tornou-se necessária pelo crescente número de episódios envolvendo casos similares ao da atriz, os quais não possuíam jurisprudência e meios legais adequados para seu julgamento. Destaca essa alteração a citação da Segurança em ambientes virtuais, especificando o que diz respeito à privacidade online. Os artigos de relevância tratam de crimes de invasão de dispositivos digitais, interrupção, impedimento ou imposição de dificuldades para serviços públicos de informação,

previsão legal sobre a equiparação de cartões de crédito e débito com documentos pessoais, tornando sua cópia não autorizada e falsificação crime (FMP, 2021).

**C) Lei 12.527/11 – Acesso à Informação:**

Resgatando também um direito já previsto pela constituição, o do cidadão de receber dos órgãos públicos as informações de seu interesse particular, coletivo ou geral, excetuando-se pelas informações protegidas pelo sigilo ou imprescindíveis à segurança da sociedade e do estado. Foi então necessário estabelecer a facilidade de acesso às informações públicas, produzidas pelos órgãos do governo, em todas suas esferas, dando assim o incentivo à cultura da transparência. A disponibilização das informações foi então dividida nos seguimentos que dizem respeito ao interesse particular, especificadas pelos seus solicitantes, bem como as informações de interesse coletivo, que devem ser divulgadas sem que haja requerimento prévio (Câmara, 2022). O instrumento legal define como regra o acesso às informações públicas e o sigilo como exceção. Também aponta os prazos com relação à disponibilização, conforme requerimentos dos cidadãos. A criação do sistema e-SIC (Serviço de Informação ao Cidadão) e sua instituição como canal oficial para solicitações.

Desde a constituição de 1988 até 2011 já existiam mecanismos legais que previam o direito de acesso à informação, porém os mesmos encontraram-se de maneira dispersa e não específica, com relação ao direito de acesso. Muitas leis que tratavam de outros assuntos, como por exemplo, a responsabilidade fiscal, meio ambiente ou modelos de gestão de arquivos traziam em seu escopo a previsão desse direito. De acordo com a evolução do meio social, as necessidades surgiram para atualização desses instrumentos, uma vez que a especificidade do assunto que tratam diz respeito a uma demanda evidente do grupo social na atualidade. A tecnologia digital ampliou ainda mais essa demanda.

### 2.3.2 Cenário Global

**A) *GDPR*:**

Em 2016 a União Europeia formalizou essa regulamentação, atualizando seu último instrumento legal, uma diretiva datada de 1995, que fazia referência à Proteção de Dados Pessoais, criando assim a *General Data Protection Regulation* – *GDPR* (em português: Regulamento Geral de Proteção de Dados) (Freitas, 2021). Esse regulamento atualizado inclui bases mais específicas, com relação aos meios eletrônicos e a internet, visando o uso de dados de usuários de redes, bem como bancos de dados de empresas comerciais, prestadores de serviços e entidades governamentais, sobre a forma como devem administrá-lo a partir do marco.

A *GDPR* foi um dos primeiros e mais abrangentes instrumentos de base, para a proteção de dados no mundo, sendo referência para o desenvolvimento de regulamentações posteriores em outros países. Está instituída de forma regulatória como um manual de orientações previstas às pessoas físicas e jurídicas que coletam, armazenam e tratam dados pessoais de cidadãos da UE pelo mundo. Para Marinho (2020) é vista como um conjunto de normas técnicas, na forma de regulamento, que traz no seu escopo uma série de normas previstas na ISO que tratam tanto de Segurança da Informação como das Políticas de Privacidade.

De acordo com NetApp (2021) a *GDPR* tem como principal finalidade de proteger os dados do cidadão europeu, dentro da UE, ou mesmo que seja processado em qualquer outro lugar do mundo. Esta regulamentação define "dados pessoais" como qualquer informação que possa vincular à identificação de um cidadão; já o termo "Processamento" refere-se à comercialização desses dados. O regulamento prevê que deve haver consentimento para coleta de dados, bem como caso sejam utilizados para outra finalidade, a qual não estiver prevista no termo de consentimento, configura-se transgressão. O tráfego dos dados pessoais é delimitado ao Espaço Econômico Europeu. O direito à privacidade dos dados pessoais dos cidadãos europeus, contempla a ciência de que dados foram coletados, porque e como estão sendo processados e armazenados, e se estão sendo compartilhados e com quem. Além desses, a normativa também prevê o direito de solicitar um relatório atualizado, que contemple dados relativos a todos os direitos anteriormente mencionados, bem

como a exclusão total ou parcial desses, dos bancos de armazenamento das empresas. O cidadão também pode se opor a ter seus dados processados, existindo até mesmo normativas específicas a respeito de campanhas de e-mails de marketing. Em caso de violação, as empresas têm até 72 horas para informar ao usuário sobre exposições não autorizadas de suas informações pessoais. Também é necessário que as empresas disponibilizem com fácil acesso sua política de privacidade de dados. As equipes para auditoria e controle dos processos relativos à proteção de dados fica a cargo dos "Oficiais de Proteção de Dados" e dos "Diretores de Privacidade". O primeiro atual em nível hierárquico mais independente dentro da organização, realizando a auditoria interna. Os Diretores de Privacidade ficam responsáveis por estabelecer estratégias que visem cumprir com as determinações legais neste ambiente organizacional. As sanções previstas ao descumprimento da GDPR são rígidas, estando sujeitos por não conformidade a € 10mi ou 2% do seu faturamento anual, sendo o valor maior. Já para as violações, esse valor dobra para € 20mi ou 4% do faturamento anual da empresa, sendo também pelo valor maior.

Esse instrumento integra políticas regulatórias gerais de 28 membros do grupo da UE, porém pode abranger um alcance mundial, no que diz respeito às previsões de proteção de dados dos cidadãos europeus, ou mesmo de empresas que colete, armazene e trate seus dados em outras regiões do planeta. Apresenta os principais personagens deste ambiente e define algumas de suas atribuições, como o processador, que é o entre que efetua o tratamento dos dados, bem como o controlador, que é a peça chave para o tratamento desses dados (Peck, 2020).

A preocupação com a privacidade dos cidadãos nasceu da constante evolução das tecnologias digitais, que passaram a integrar informações de usuários em bancos de dados, através de plataformas online, onde o acesso a esses dados poderia gerar impactos negativos. Inicialmente os dados armazenados eram de nível mais primário e com informações cadastrais básicas, porém com o passar dos anos essa integração possibilitou a coleta de dados mais específicos, que trouxeram ainda mais vulnerabilidade aos usuários. De acordo com a revista ISTO É (2016) a empresa Uber, de transporte de passageiros, em 2016 sofreu ataques de invasores, expondo os dados de cerca de 57 milhões de usuários, tendo como resultado aplicação de multa de U$ 500mi nos EUA e 4,5mi no Reino Unido e Holanda. Além dos dados cadastrais que integram CPF, nome completo e e-mail dos usuários, os invasores

também tiveram acesso a centenas de carteiras de habilitação de motoristas cadastrados no *app*.

### *B) CCPA:*

No estado da Califórnia, nos EUA, foi em 2018, com base nos moldes da *GDPR,* por até então não existirem dispositivos legais acerca da proteção de dados pessoais no país, foi aprovado o California Consumer Privacy Act – CCPA (em português: Ato de Privacidade do Consumidor da California). Vale ressaltar que não existe uma lei federal que estabeleça esses parâmetros, apenas o *Privacy Act of 1974* (em português: Ato de Privacidade de 1974) (Gradim, 2020).

Para NetApp (2021) a CCPA Visa estabelecer maior transparência com relação à coleta e armazenamento de dados de usuários. Ela surgiu como complemento de outras legislações acerca de proteção de dados e privacidade, veiculando novas imposições. Formalmente, essa normativa prevê a necessidade do estabelecimento de algumas ferramentas, por parte das empresas. A lei abrange a proteção a todos os consumidores residentes na Califórnia, sendo americanos ou não. Os deveres aplicam-se às empresas com fins lucrativos, que possuem sede, funcionários, imóveis ou que comercializem em grande fluxo com consumidores da Califórnia, atendendo um ou mais dos seguintes requisitos: faturamento bruto anual mínimo de US$ 25 mi; colete dados pessoais de mais de 50mil usuários ou dispositivos no estado; gere mais de metade da sua receita total anual com a comercialização de dados pessoais de consumidores do estado. Tem por sua definição que os dados pessoais são aqueles fornecidos pelos próprios usuários, através de formulários online ou mesmo aqueles coletados por ferramentas de rastreamento e afins. Dados esses capazes de identificar um indivíduo ou sua família. Essa regulamentação dá às empresas o direito de comercializar os dados dos consumidores, uma vez que os mesmos atestem ciência no fornecimento desses dados, podendo os mesmos se recusarem a disponibilizá-los para tais operações comerciais. Diferentemente da GDPR, não prevê a proibição da transferência de dados para espaços externos aos EUA. Os consumidores têm direito de solicitar relatório gratuitamente, dos seus dados, que as empresas possuem armazenados e os mesmos devem ser entregues num prazo de até 45 dias, sendo possível também

solicitar a sua exclusão. Aos menores de 13 anos, será necessário a autorização dos seus responsáveis legais, para consentimento a respeito da comercialização de seus dados. Essa normativa não prevê a nomeação de entidades específicas para a regulamentação da proteção de dados no ambiente corporativo. Esta lei não possui especificidade, com relação à notificação aos usuários pela exposição de seus dados, porém existem outras regulamentações vigentes no estado que já preveem algo do tipo. As penalidades financeiras limitam-se ao valor de até US$ 7.500 por ocorrência, no prazo de 30 dias. Os cidadãos têm o direito de requerer danos de até US$ 750 por incidente, em caso de exposição.

Segundo Andrade *et al* (2019), a holding formada pelas empresas Yahoo e Verizon foi condenada pelo governo norte americano a pagar uma multa de U$ 35mi, pelo vazamento de dados de 200 milhões de usuários em 2014. Dentre os dados mencionados, estavam nomes, datas de nascimento, endereços, e-mails e contatos telefônicos. Com o acesso a esses dados, os invasores podem agir de diversas maneiras na aplicação de golpes contra os usuários.

Para Robertson (2019) em “The Great Hack – Privacidade Hackeada”, documentário lançado pela Netflix em 2019, sobre a empresa Cambridge Analytica e seu envolvimento direto com a campanha para a presidência dos Estados Unidos da América de Donald Trump em 2016, a qual utilizou dados de usuários, fornecidos pela rede social digital *Facebook*, para que pudesse gerar campanhas de influência nacional com grande alcance, reproduzindo conteúdos direcionados aos eleitores, manipulando assim o resultado das eleições.

**C) *POPIA*:**

Entrando em vigor em junho de 2020, o regulamento de proteção às informações pessoais sul africana, também possui os mesmos princípios norteadores da *GDPR*, bem como da *CCPA*. O título *POPIA - Protection Of Personal Information Act* - (Ato de Proteção às Informações Pessoais, em inglês), define a normativa que regula a privacidade dos dados de usuários na África do Sul. Esta surgiu em 2013, antes mesmo da legislação análoga europeia, porém ficou estagnada para aprovação de autoridades do governo, durante vários anos. Suas diretivas incluem responsabilidade, transparência, segurança, minimização de dados, limitação de

propósitos e direito de titularidade dos dados. A definição de dados pessoais deste instrumento é mais extensa que da *GDPR*, pois incluem também os dados empresariais e organizacionais. Também possui previsão sobre a categoria de dados sensíveis, que devem ser tratados sob princípios mais rigorosos, como crenças religiosas ou filosóficas, raça ou origem étnica, filiações sindicais, filiações partidárias, saúde, vida e orientação sexual e dados biométricos. Diferentemente da regulação europeia, este visa defender os dados de qualquer cidadão sujos dados sejam tratados em território ou por uma empresa sul-africana. O consentimento é obrigatório apenas para a coleta de dados sensíveis ou mesmo de crianças e adolescentes menores de 17 anos de idade, que deverão ser autorizados pelos responsáveis legais. O processamento de dados pessoais pode ser utilizado como ferramenta para Marketing direto quando o indivíduo for cliente da empresa ou mesmo tenha fornecido consentimento a respeito. Essas comunicações deverão obrigatoriamente ofertar a adesão ou exclusão à lista de marketing. A identificação da entidade por trás das coletas, o que ela está coletando, o seu motivo e os direitos de titularidade devem ser apresentados em todo e qualquer formulário/cadastro para preenchimento de usuários e empresas. A partir do momento em que esses dados foram coletados, passarão a fazer parte da política de privacidade online das empresas. Seguem os mesmos critérios para concessão de direito de acesso, correção e exclusão dos dados aos titulares. Há proibição quanto ao trâmite dedados pessoais e informações dessa natureza para fora do território sul-africano. Prevê a criação de entidade governamental para monitoramento das atividades sobre políticas de segurança e privacidade violadas no país. Os responsáveis legais das empresas tornam-se os responsáveis pelos trâmites sobre informações e nas entidades governamentais, é obrigatória a instituição do papel do DPO - *Data Protection Officer* (Oficial de Proteção de Dados, em inglês). As empresas ficam obrigadas à emissão de relatórios de violação de dados e à notificação dos usuários, estando sujeitas às penalidades por não conformidade, que podem chegar a 10 milhões de Rands sul-africanos (equivalente a R$ 3,1 mi) (NetApp, 2021).

**D) *APPI*:**

Desenvolvida com base na sua primeira regulamentação de proteção de dados criada em 2003, o *APPI – Act on the Protection of Persinal Information* (Ato de Proteção das Informações Pessoais, em inglês) foi homologado em 2015, tendo sua validade datada de 2017, um ano antes da *GDPR*. Em seu escopo traz as definições de dados pessoais e dados sensíveis, semelhantes aos demais instrumentos, atribuindo maior rigidez aos dados sensíveis. Aplica-se aos dados tratados por empresas situadas em território japonês, bem como de cidadãos japoneses tratados fora do seu território. Da mesma forma também há previsão sobre necessidade de consentimento da coleta de dados por seus titulares, bem como da possibilidade de solicitar um relatório dos mesmos os quais as empresas possuem e acioná-las para solicitação de exclusão do seu banco de dados (Durbano, 2020).

**E) *LPDP*:**

O regulamento Argentino de Proteção de dados, LPDP – Ley de Proteción de los Datos Personales (Lei de Proteção de Dados Pessoais, em espanhol), criada em 2016 com o principal objetivo de proteção aos dados pessoais de indivíduos, armazenados em bancos de dados de registros públicos e privados. Esse marco legal foi atualizado de decretos anteriores datados de 2001 e também de 1994, para inclusão de informações contemporâneas adequadas à nova realidade virtual dos cidadãos, com relação aos dados sensíveis, principalmente os biométricos. Desde sua primeira versão já previa a criação da Agência Argentina de Acesso à Informação Pública, responsável pela regulação e controle dessa normativa, também prevê o direito de acesso aos titulares, de suas informações armazenadas e da solicitação de exclusão desses (Durbano, 2020).

**F) *PIPL*:**

A *Personal Information Protection Law – PIPL* (Lei de Proteção de Informações Pessoais, em inglês), homologada na China em novembro de 2021, foi submetida ao Congresso Nacional em outubro do ano anterior e posteriormente

publicada para comentários da população. Esse regulamento não se aplica apenas às pessoas físicas e jurídicas que processam dados no território da China, mas também àquelas que processam dados de cidadãos chineses. Seu conceito central está focado em informações pessoais, definidas como dados que identificam um indivíduo, excluindo dados anônimos. Define como controladores de informações pessoais as organizações ou indivíduos que realizam o seu processamento. Prevê direito de titularidade aos usuários, bem como sanções administrativas aplicáveis às organizações e órgãos governamentais que não cumprirem suas designações (Blum, 2022).

**G) *LGPDP*:**

A *Ley General de Protección de Datos Personales – LGPDP* (Lei Geral de Proteção de Dados Pessoais, em espanhol), aprovada no México em 2010, regula a proteção dos dados pessoais tratados no país, desde sua coleta até sua exclusão. Há concessão de direito de acesso, também exista a previsão da aplicação do conceito de titularidade. Geriu a criação do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais, que é ligado ao governo nacional e tem a função de regular as atividades de tratamentos de dados realizados por indivíduos, empresas e órgãos governamentais, Paixão (2018).

**H) *PA*:**

O *Privacy Act – PA* (Ato de Privacidade, em inglês), foi estabelecido em 1993, que cria a DPA, entidade responsável pela regulação das normativas relativas à proteção de dados no local. Esse agente governamental tem também como função a mediação dos conflitos entre tratadores de dados e os indivíduos titulares desses. Esse marco regulatório teve atualizações em 2018, para concessão da ampliação dos poderes da autoridade nacional. Diferentemente dos demais regulamentos de proteção, este visa tratar de maneira conciliadora entre as partes. Embora haja intensão de mediar esse conflito, ainda é previsto o direito de petição judicial dos titulares de dados, sobre infrações cometidas pelos processadores de dados (Botino *et al*, 2020).

### 2.3.3 Lei Geral de Proteção de Dados Pessoais no Brasil - LGPD:

Todos os marcos legais de proteção de dados estabelecidos pelo mundo, destacam a importância que as administrações nacionais passaram a dar com relação à vulnerabilidade das informações dos seus cidadãos e os prejuízos que esta poderia causa-los. No Brasil, tendo em vista a exposição dessas situações, nas grandes nações a fora, tornou-se necessário também a discussão com relação aos mecanismos de defesa dos usuários. Também já havia na história, casos de vazamentos de informações pessoais no país, como exemplo do caso do Banco Inter, que em 2018 foi condenado pelo Ministério Público – DF a pagar multa de R$ 1,5 mi, por conta de um episódio onde foram expostos dados de mais de 19 mil correntistas (Andrade *et al*, 2019). Na ocasião, o Banco teve seus sistemas informacionais invadidos por crackers, que tiveram acesso aos dados cadastrais básicos dos clientes, tais como CPF, e-mail e nome completo, o que para os golpistas representa uma fonte de oportunidade, sendo possível a utilização desses dados para aplicação de golpes de Engenharia Social.

A lei brasileira de proteção de dados foi promulgada em 2018 e entrou em vigor em agosto de 2020. Levou grande espaço de tempo para passar a vigorar, sendo adiada pelo governo para dar um prazo maior às empresas para que se adequassem às regulamentações. Surgiu pela necessidade de reforçar o direito constitucional da privacidade, aos cidadãos brasileiros. Possui a mesma definição de "dados pessoais" que a sua versão europeia, estando relacionado à identificação da pessoa natural, física ou jurídica, enfatizando o que diz respeito às informações relacionadas a origem étnica e racial, de saúde, filiação a grupos partidários e sindicatos, etc., caracterizando estes como dados sensíveis e estabelecendo regras especiais para tratamento dessas informações. Este marco vem assegurar ao cidadão o direito de consentimento com o processamento de seus dados, ou seja, sempre que houver uma coleta informacional por meio de cadastro, por parte de indivíduos ou empresas cuja intenção seja o tratamento desses dados, existe a necessidade de concordância do titular. Uma de suas fragilidades apontada é a de que se permite que as instituições de crédito utilizem o processamento de dados, para garantir a "proteção" do score do consumidor, tendo as empresas que funcionam como *bureau* de crédito a prerrogativa legal, para tráfego dos dados financeiros dos indivíduos, para que se possa traçar um

perfil de crédito ao mesmo, garantindo uma concessão mais “justa” de acordo com o score atingido. Com o advento da LGPD, torna-se ainda mais importante às empresas o uso de ferramentas que garantam a sua segurança de dados, pois sua responsabilização pela exposição dos mesmos pode acarretar sem sanções. A lei prevê a instituição de autoridade nacional para proteção de dados (ANPD), que será responsável pela regulamentação e a proteção de dados no país. Se aplica à todas as empresas do mundo que possuem relações comerciais de bens e serviços com o mercado brasileiro (NetApp, 2021).

Também fortemente influenciada pela *GDPR*, a Lei Geral de Proteção de Dados pessoais – LGDP trouxe em seu arcabouço uma série de definições e regulações a respeito da proteção de dados, detalhando diversos aspectos desse universo, a fim de reestabelecer àquilo que já era previsto no Art. 5º da CF (1988) como uma garantia fundamental, a privacidade do cidadão. Desta forma, baseada na necessidade social da implementação de medidas mais rígidas e específicas a respeito do tema. Passareli (2019) descreve os principais pontos da LGPD e aponta sua importância, de mesmo nível do que nos países da Europa e dos EUA, comparando que a lei brasileira se diferencia dos demais países pelo seu nível de detalhamento, que é mais raso em questões, que precisarão ser disciplinadas posteriormente. Um desses pontos principais tem relação com a penalidade indicada no caso de vazamento de dados, por parte das empresas detentoras desse bem informacional, estando os regulamentos dos outros países mais rígidos e incisivos em suas penalizações.

Sendo uma das principais razões pela instituição dos marcos legais de proteção de dados a garantia da segurança informacional dos cidadãos, Andrade (2019) entende como benefício proposto pela LGPD o de que o titular das informações pessoais ganha uma série de direitos, como o de solicitar às empresas os dados que possuem sobre ele, para quem foram repassados e para qual finalidade. Além disso, caso os registros estejam incorretos, o mesmo poderá solicitar a correção. O indivíduo também pode se opor ao tratamento dado às informações, tentando estabelecer uma relação de maior autonomia nas decisões a respeito do seu próprio patrimônio de informação.

Nos termos da LGPD (2018), dados pessoais são definidos como quaisquer informações que possam identificar uma pessoa. Já o dado sensível é aquele que

pode aprofundar essa identificação, com relação à sua origem racial ou étnica, opção religiosa, política, filosófica, vida sexual, dados genéticos, de saúde e biométrico. Esses compõem o objeto do apelo principal da instituição do marco legal, que visa a sua proteção. São tidos como sensíveis pois a sua exposição pode gerar distinção entre os demais indivíduos da população, de forma a segregar um grupo de pessoas.

A definição dos agentes os quais devem compor a cadeia do ciclo dos dados, auxilia na visualização da responsabilização de cada um dos membros do processo, estabelecendo o papel do controlador, figura responsável pelas decisões referentes ao tratamento de dados, o operador que é quem realizará o tratamento dos dados em nome do controlador, o encarregado que será o responsável pela comunicação entre o controlador, o titular e autoridade nacional de proteção de dados e incluindo também a entidade reguladora associada ao governo, cuja atribuição de fiscalização das atividades de proteção de dados deverá assegurar o cumprimento dessa normativa.

No art. 6º da LGPD (2018), se estabelecem os princípios pelos quais devem ser norteadas as atividades de tratamento de dados, especificando suas finalidades. Seu inciso VII, que trata do tema de segurança ressalta o uso de medidas técnicas para proteção de dados contra o acesso de agentes não autorizados, preocupação esta que deve ser englobada pelas empresas a fim da execução das medidas legais. A responsabilidade sobre o uso de dados por parte dos agentes controladores, definição das empresas que realizam o tratamento dos dados pessoais, é bastante explorada com vistas à geração de um escopo de trabalho/ação para a coleta de dados. No art. 7º, se destaca a necessidade do consentimento do titular, para o tratamento que seus dados serão submetidos, inclusive sobre a comunicação desses dados com outros agentes controladores, podendo o titular declinar desta autorização em momento posterior, bem como solicitar que seus dados sejam excluídos da base de dados das empresas. Também é prevista a necessidade do controlador e do operador manterem relatórios sobre suas ações de tratamento, o que pode auxiliar no mapeamento de ocorrências. Outra obrigatoriedade mencionada é a de notificação à autoridade nacional, por parte dos agentes controladores, sobre os episódios de incidentes de segurança, previstos no art. 48º, como o caso de vazamentos de dados, que pode gerar uma série de impactos aos titulares envolvidos.

Na Seção III do CAP VI, que trata das responsabilidades e do ressarcimento de danos, se fixam os pontos referentes às medidas cabíveis quanto ao

descumprimento dos termos enunciados. Logo após, no CAP VIII, Seção I que trata das Sanções Administrativas, se estabelecem as penalidades a serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), desde multas até o bloqueio dos bancos de dados das empresas infratoras até que se enquadrem nos parâmetros requeridos.

## 3 PROCEDIMENTOS METODOLÓGICOS:

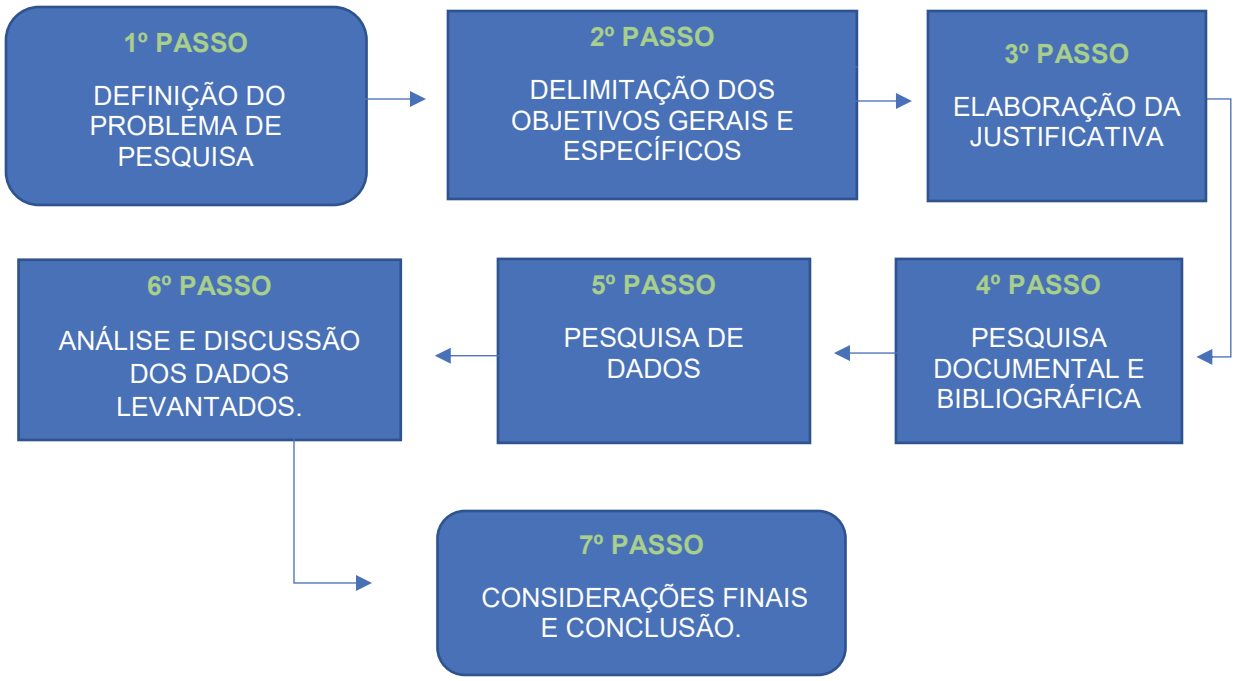
De acordo com Lozada e Nunes (2019) o conhecimento pode se classificar, dentro de uma escala progressiva, sendo mítico, em uma de suas formas mais primitivas, até à sua forma mais aprimorada, o científico-tecnológico. O ponto determinístico entre eles seria a etapa de desenvolvimento, em que o homem se encontra na sociedade. Para o progresso e evolução das escalas de conhecimento, torna-se necessário o estabelecimento de parâmetros, os quais são adotados para novas definições, com base em experiências e vivências do próprio ser social. Também trazem a compreensão de que o método se define como um conjunto de processos, adotados para a execução de um projeto, que possibilite a sua resolução, de acordo com os objetivos definidos previamente.

Dentre os vários métodos científicos para debate e contextualização de um conhecimento, novo ou já explorado, Rother (2007) descreve a revisão bibliográfica como um método de abordagem amplo, apropriado para a discussão sobre o estado da arte de um tópico ou assunto específico. Esse método visa explorar a literatura e interpretações acerca do tema, de maneira não sistemática, trazendo engajamento de novas discussões acerca dos temas relacionados à pesquisa.

Lozada e Nunes (2019) também apontam o levantamento documental e bibliográfico como ferramenta essencial, para poder trazer informações conceituais ao projeto e explanação dos temas inseridos no problema de pesquisa. Destacam como “não rígida” a estrutura de tópicos para confecção do projeto, tendo desta forma, os princípios básicos sugeridos de estrutura, que perpassam pela definição do tema, formulação do problema de pesquisa, determinação dos objetivos gerais e específicos, identificação do tipo de pesquisa, construção de hipóteses. Elaboração de justificativa, revisão bibliográfica e documental da literatura e definição de referenciais teóricos, chegando à definição dos procedimentos metodológicos e dos recursos necessários para a pesquisa.

Desta forma, de acordo com o problema de pesquisa apresentado e os objetivos propostos pelo presente projeto, foi necessária a adoção de determinados procedimentos metodológicos para sua realização:

FIGURA 2 – FLUXO DE PROCEDIMENTOS METODOLÓGICOS




Fonte: O autor (2022)

Conforme fluxograma acima, destacam-se os principais passos citados que seguem:

I – O passo inicial da pesquisa foi o levantamento bibliográfico e documental, visando a compreensão do tema e embasamento para realização da atividade de coleta de dados. Primeiramente foram levantados os procedentes legais, os principais tipos de vazamentos e ações da Engenharia Social. Essa pesquisa visa descrever o contexto histórico para a concepção da LGPD e suas bases conceituais. Também teve como objetivo definir a Engenharia Social e suas ferramentas.

II – O tema escolhido trata-se de um aspecto sensível das organizações, pois ele demanda destas a exposição de suas fragilidades, o que pode acarretar em consequências comerciais e estratégicas. Por esse motivo, foi incluída na pesquisa a busca de dados em revistas e jornais digitais, por não possuir acesso a outras fontes e as empresas não estarem disponíveis à divulgação de seus incidentes. A Busca realizada em sites da web, sem delimitação de tempo e espaço da ocorrência dos eventos, com relação aos episódios noticiados na mídia, a respeito de casos de vazamento de dados, ocorridos em grandes empresas pelo mundo, visando destacar

seus itens de maior relevância, como data da ocorrência, nome da empresa envolvida, breve descrição do episódio, se houve sanção e valor da mesma, em moeda corrente no país. Foi realizada entre Set/2020 e Nov/21, com casos de vazamento de dados e exposições devidas a mecanismos de engenharia social, visando o cumprimento de um dos objetivos específicos deste trabalho, resultando no Quadro 2.

III – Foram realizadas exposições, dos dados apontados nos estudos, que visem responder aos questionamentos indicados pelo problema de pesquisa, na perspectiva de solucioná-lo. Com o auxílio dos dados compilados no site da web GET – *GDPR Enforcement Tracker*, foi possível realizar uma explanação sobre a efetividade da *GDPR* desde sua homologação, para que se pudesse definir quais os seus aspectos mais relevantes. O objetivo dessa exposição foi de trazer para a pesquisa o contexto internacional da *GDPR* e a forma de ação dos seus agentes reguladores, para estabelecer um cenário comparativo com o quadro nacional, com dados documentados e agrupados pelo portal ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados, que expõe casos de sanções aplicadas pela LGPD desde sua homologação.

## 4 ANÁLISE DE DADOS E DISCUSSÃO

Das sociedades primitivas aos dias atuais, o conceito da informação e o valor dado a mesma vem sendo cada vez mais ampliado, conforme a percepção de que seu acesso pode trazer benefícios e vantagens. Nas eras pré-históricas o objetivo da geração da informação, através de seu registro, era o de auxiliar na memorização da contagem de pertences, animais de rebanho, períodos de plantio, dentro outros. Uma história da vida cotidiana se transporta pelo tempo e espaço aos dias atuais, onde podemos observar essa realidade distante e próxima. O avanço das tecnologias proporcionou ao homem que se otimizasse o formato desses registros, perpassando pela criação da escrita, posteriormente se desenvolvendo os meios de registro, com a invenção dos pergaminhos, papéis, cartas, prensas, livros, chegando ao momento em que a informação se constitui em meios digitais e possui um tamanho imensurável. O advento da Gestão da Informação, como ciência, vem de encontro com a necessidade de organizar os bens informacionais, para geração de melhores resultados às organizações.

Na era da informação digital, vivenciamos as transferências de um grupo significativo de dados, em poucos instantes, através das redes. Isso traz avanço para a comunicação e benefícios à sociedade como um todo. As formas como as pessoas se comunicam evoluíram através dos tempos, trazendo mais proximidade nas distâncias físicas, através das ferramentas de interação online. O mundo virtual que se criou com esse avanço trouxe uma série de conquistas aos seres sociais, otimizando suas relações interpessoais, sua organização social, etc.

Para chegar a esse resultado, foram necessárias diversas análises e tentativas, através da construção de ferramentas e conceitos de base para estruturar os fluxos informacionais. A arquitetura da informação pode ser entendida como um modelo de referência para a organização dos dados, dispostos num sistema de informações. Através dessa concepção tornou-se possível evidenciar a necessidade da criação dessa estruturação, que permite aos profissionais envolvidos nos projetos de SI estabelecer um ponto de partida para elaboração de novos sistemas e implementação de melhorias nos já existentes.

Outro ponto importante observado é que, de acordo com o estabelecimento de novas técnicas de organização informacional nos SI, também é importante a

definição dos protocolos básicos das Políticas de Segurança da Informação, pois é através delas que serão norteadas ações para redução do risco de exposição indevida do patrimônio informacional, bem como garantir o direito à privacidade dos usuários.

No contexto das ameaças que a integridade dos dados dos cidadãos vem sofrendo, os agentes governamentais passaram a trabalhar em torno da necessidade de estabelecer políticas regulatórias com relação à proteção desses dados. Nas sociedades atuais, o fluxo de dados aumenta de tamanho a cada instante e isso gera certa vulnerabilidade para sua segurança. No Brasil a CF (1988) já previa o direito à privacidade dos cidadãos, desta forma, é possível compreender que qualquer violação que esta venha sofrer deverá ser julgada com base nesse princípio, porém de acordo com as políticas sociais que se estabeleceram com o tempo, houve um aprimoramento, no sentido de especificação, dessa garantia fundamental, através de instrumentos atualizados mais detalhados. A lei de acesso à informação, sancionada no Brasil em 2011 reafirma o direito do cidadão ao acesso às informações de domínio público, tornando exceção apenas aquilo que possui caráter sigiloso, sendo o sigilo uma garantia de não exposição de informações pessoais/privadas que possam oferecer risco aos cidadãos ou à sociedade, de forma geral. Após o episódio de ataque cibernético sofrido pela atriz Carolina Dieckmann, onde a mesma teve sua intimidade exposta, e também pela grande pressão da mídia, houve aprovação da lei 12.737 de 2012, que tornou um ato criminoso a invasão de dispositivos eletrônicos, assim como trouxe a reafirmação da segurança da privacidade dos cidadãos nos ambientes digitais, tendo este marco sido impulsionado pelo crescimento constante de casos de invasão de dispositivos e roubo de dados pessoais por crackers ou invasores.

Partindo de uma época onde as informações eram coletadas de forma individual e os golpes posteriormente aplicados eram estruturados, com base numa cadeia de um pequeno número de usuários, atualmente o mundo coorporativo lida com a situação de grandiosos sistemas desenvolvidos, capazes de interagir com suas fortalezas de patrimônio informacional, na busca de sua ruptura e coleta do maior volume de dados possível. Não se beneficiam apenas os agentes individuais, identificados na mídia como crackers ou invasores, que utilizam das informações capturadas para golpes pouco estruturados, mas também o mercado consumidor desses bens violados, a indústria do marketing, que supre suas bases de dados de clientes com cadastros obtidos de terceiros, de maneira informal, gerando assim uma

matriz de disparos eletrônicos de propaganda, na busca incessante de atingir um público cada dia maior. Essa busca obsessiva pelo acesso aos dados de usuários deixa marcas significativas, na história de diversas empresas. Muitas delas, até conseguem mascarar essa realidade, fazendo com que o registro de quebra do sigilo de seus clientes/usuários seja apagado, não de maneira operacional, mas da mídia que costuma sempre divulgar, de forma alarmante, esses episódios. Mesmo com a prática das tentativas de limpar a imagem na mídia, a qual muitas empresas se submetem, para extinguir relatos negativos a respeito dos seus históricos de falhas sistêmicas, geradoras de significativos impactos, ainda é possível, através da busca em sites da internet, verificar que alguns informativos permanecem ativos, dada sua importância, conforme Quadro 2 que segue com os relatos encontrados:

Quadro 2 – Episódios de Vazamento de Dados

| EMPRESAS | ANO | | LOCAL | DADOS VIOLADOS (Nº DE USUÁRIOS) | MULTAS |
|---|---|---|---|---|---|
| | OCORRÊNCIA | CONDENAÇÃO | | | |
| CITIBANK | 2011 | - | EUA | 360.000 | 0,00 |
| | G1 GLOBO | Dados cadastrais de clientes do banco foram vazados após invasão de grupo de crackers às plataformas virtuais de banco de dados. Informações relativas aos contratos de crédito dos clientes foram afetadas e banco precisou realizar nova emissão de cartões para os mesmos. | | | |
| TARGET | 2013 | - | EUA | 70.000.000 | 0,00 |
| | CANALTECH | Além das informações cadastrais de usuários expostas, também foram vazadas informações bancárias dos mesmos. | | | |
| ADOBE | 2013 | - | EUA | 152.000.000 | 0,00 |
| | O GLOBO | Foram vazados dados dos usuários dos principais softwares da desenvolvedora, como e-mails, senhas criptografadas e dicas de senhas, que foram "disponibilizadas" em sites da deep web. | | | |
| FACEBOOK | 2016 | 2019 | EUA | 87.000.000 | US$ 5,000,000,000.00 |
| | G1 GLOBO | Estava envolvida a empresa Cambridge Analytica, que coletava e tratava dados do Facebook, a qual compartilhou indevidamente os dados para manipular eleitores e influenciar a vitória de Donald Trump no governo dos EUA. | | | |
| UBER | 2016 | 2018 | EUA | 57.000.000 | US$ 148,000,000.00 |
| | TECNOBLOG | A empresa sofreu um cibe ataque, que resultou na exposição de dados de seus usuários, como endereços de e-mail, número de celular, dados dos motoristas, até mesmo como documentos de habilitação. | | | |
| BANCO INTER | 2017 | 2018 | BR | 19.000 | R$ 1.500.000,00 |

| | | | | | |
|---|---|---|---|---|---|
| | TECNOBLOG | Por mais de um ano estiveram expostos os dados cadastrais dos correntistas. | | | |
| **NETSHOES** | 2018 | 2019 | BR | 2.000.000 | R$ 500.000,00 |
| | G1 GLOBO | Vazamento de dados pessoais de clientes cadastrados na plataforma de compras online, como CPF, data de nascimento, e-mail, histórico de compras. | | | |
| **C&A** | 2018 | - | BR | 2.000.000 | 0,00 |
| | TECMUNDO | Através de invasão do sistema de geração da "Cartões presente", comercializados pela empresa, crackers conseguiram ter acesso aos dados cadastrais dos usuários. | | | |
| **GOOGLE** | 2018 | 2019 | EUA | 500.000 | US$ 7,500,000.00 |
| | TECNOBLOG | Empresa indenizou usuários que tiveram seus dados de cadastro vazados através da extinta rede social Google+. | | | |
| **BRITSH AIRWAYS** | 2019 | - | UK | 500.000 | £$ 183.390.000,00 |
| | TECMUNDO | Episódio ocorreu por conta de um desvio do link do site principal da cia aérea para um endereço fraudulento. Dados cadastrais e até mesmo bancários ficaram expostos. | | | |
| **MICROSOFT** | 2019 | - | EUA | 250.000 | 0,00 |
| | TECHTUDO | Problemas nas configurações dos bancos de dados da equipe de suporte ao cliente acarretaram no vazamento de cerca de 14 anos de informações. | | | |
| **CLARO E VIVO** | 2019 | 2021 | BR | 2 | R$ 20.000,00 |
| | CONVERGÊNCIA DIGITAL | Empresas de telefonia móvel foram condenadas a indenizar consumidores, cujos dados vazados resultaram no bloqueio de uso dos seus aparelhos celulares. | | | |
| **BC CORP** | 2019 | - | BR | Não divulgado | 0,00 |
| | THE HACK | Administradora de empresas especializadas em saúde ocupacional teve o vazamento de dados sensíveis de seus clientes, como atestados médicos, peso, altura, condições de saúde, etc. | | | |
| **DETRAN - RN** | 2019 | - | BR | 70.000.000 | 0,00 |
| | JORNAL DO CARRO | Um problema no site do órgão deixou exposto os dados de milhões de usuários, que puderam ser pesquisados abertamente. | | | |
| **BANCO PAN** | 2019 | - | BR | Não divulgado | 0,00 |
| | TECNOBLOG | Após a exposição de um servidor de seus correspondentes bancários, os dados cadastrais de clientes foram vazados, como endereço, telefone, e até mesmo cópias de documentos pessoais. | | | |
| **TWITTER** | 2019 | - | BR | Não divulgado | 0,00 |
| | EXAME | Uma falha sistêmica expôs postagens marcadas como privadas, as tornando públicas. | | | |
| **BB PREVIDÊNCIA** | 2020 | - | BR | 153.000 | 0,00 |
| | EXAME | Uma falha sistêmica tornou vulnerável, nos portais da empresa, dados de cadastro de seus clientes. | | | |
| **NINTENDO** | 2020 | - | JAPÃO | 160.000 | 0,00 |

| | | | | | |
|---|---|---|---|---|---|
| | TECHTUDO | Contas de acesso às plataformas virtuais de jogos da empresa foram vazadas com dados cadastrais de usuários. | | | |
| **SERASA EXPERIAN** | 2020 | - | BR | 200.000.000 | 0,00 |
| | CARTA CAPITAL | Empresa é acusada de vazar dados pessoais de milhões de usuários, Pessoas Físicas e Jurídicas, sendo um dos maiores episódios na história, em número de usuários afetados. Além de dados cadastrais como CPF, RG, Telefone Celular e endereço, também continham dados pessoais como fotos e valores de remunerações. | | | |
| **EMBRAER** | 2020 | - | BR | Não divulgado | 0,00 |
| | COINTELEGRAPH | A fabricante de aeronaves brasileira teve seus sistemas "sequestrados" em troca de criptomoedas, porém não realizou nenhum tipo de negociação com os invasores. Cerca de 200 documentos foram vazados, os quais continham inclusive dados de funcionários. | | | |
| **YOUTUBE, TIKTOK E INSTAGRAM** | 2020 | - | EUA | 235.000.000 | 0,00 |
| | CANALTECH | Foi detectada falha de vulnerabilidade em servidor de armazenamento de dados que continha informações das três plataformas, relativas à identificação de perfil, fotos, estatísticas e indicadores próprios de cada rede, etc. | | | |
| **LATAM PASS** | 2021 | - | BR | Não divulgado | 0,00 |
| | ISTO É | Empresa de TI que presta serviço para companhias de transporte aéreo no país teve seu sistema invadido, vazando dados cadastrais de diversos usuários. | | | |
| **MC DONALDS** | 2021 | - | EUA | 2.300.000 | 0,00 |
| | THE HACK | Os dados referentes às franquias das lojas de fast food, bem como informações cadastrais de seus funcionários foram vazados por cyber criminosos, através de ataque aos seus sistemas de banco de dados. | | | |
| **VOLKSWAGEN** | 2021 | - | EUA | 3.300.000 | 0,00 |
| | CANALTECH | Informações de clientes ficaram expostas em servidores da companhia por cerca de dois anos, como nomes, endereços, telefones e preferências a respeito da compra de veículos. | | | |
| **ALIBABÁ** | 2021 | - | CHINA | 1.000.000.000 | 0,00 |
| | OLHAR DIGITAL | Grande empresa do ramo de e-commerce sofreu um ataque de crackers, acarretando no vazamento de milhões de dados dos seus clientes. | | | |
| **AIR INDIA** | 2021 | - | ÍNDIA | 4.500.000 | 0,00 |
| | THE HACK | Através do ataque à empresa SITA que também gerencia operações online da empresa Latam, Gol e Azul, foram vazados dados cadastrais de usuários. | | | |
| **PREFEITURA MUNICIPAL DE POÁ - SP** | 2021 | - | BR | 2.700 | 0,00 |
| | GAZETA REGIONAL | Dados pessoais de servidores foram vazados, em formato de planilha, que circulou por grupos de mensagens e redes sociais digitais. | | | |
| **LINKED IN** | 2021 | - | EUA | 700.000 | 0,00 |
| | UOL | Usuários da rede social digital tiveram seus dados vazados após os servidores da empresa sofrer ataques de invasores. | | | |

Os dados expostos evidenciam que a maior parte dos casos encontrados são relatos ocorridos nos EUA e Brasil, em sua maioria não houveram condenações legais aos tratadores dos dados vazados, por se tratarem de períodos que antecedem as instituições dos marcos legais de proteção de dados em seus respectivos países. Outro ponto de extrema importância é observado de acordo com o volume de dados vazados, relacionado com o número de usuários envolvidos (titulares), que tiveram suas informações expostas, como no caso envolvendo a empresa *SERASA EXPERIAN*, relatado pela Carta Capital, onde os dados até mesmo de indivíduos já falecidos foram expostos. O ramo das empresas envolvidas nos vazamentos é diversificado, desde órgãos públicos a grandes multinacionais comerciais de tecnologia. As informações contidas comumente nos vazamentos incluem nomes completos, CPFs e contatos de e-mail ou telefone, o que possibilita aos Engenheiros Sociais uma série de possíveis aplicações de golpes, como a geração e perfis falsos em sites de compras e redes sociais, etc. Já os vazamentos mais amplos, que incluem senhas e dados pessoais completos, como filiação, número de documentos, endereços residenciais e comerciais possibilitam a aplicação de golpes ainda mais estruturados, pois através da posse desses dados o invasor consegue atuar de forma mais precisa.

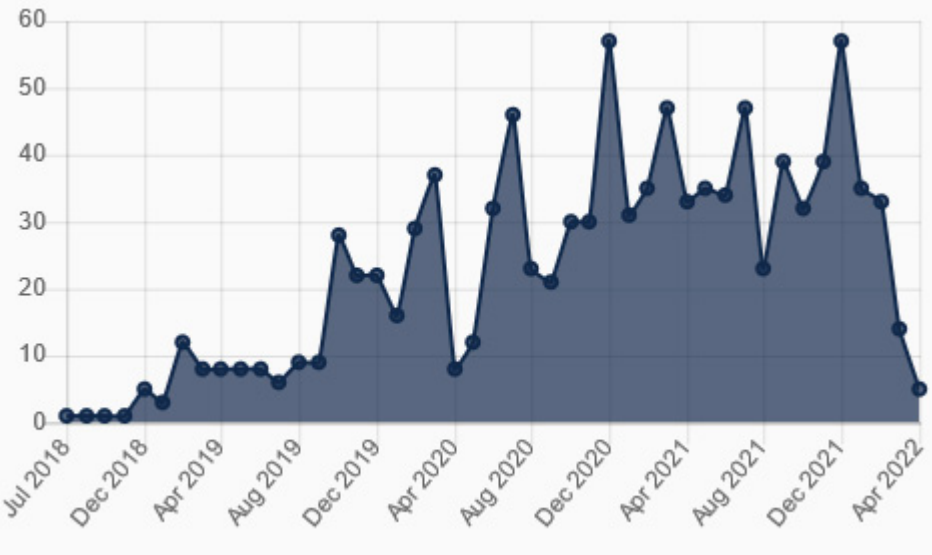
De acordo com os eventos relacionados no Quadro 2, entende-se que muitos destes poderiam enquadrar-se nas sanções aplicáveis, à luz da LGPD, pela transgressão de suas prerrogativas legais, tendo em vista sua recente homologação, que já tem validade para penalização dos agentes do seu descumprimento. O vazamento de dados se enquadra dentro do § 7º, Seção I – Das Sanções Administrativas. Utilizando a metodologia dos demais instrumentos legais de proteção de dados de usuários pelo mundo, fica evidente que a ferramenta punitiva ainda atua como principal fator para exigência de seu cumprimento. Quando a previsão legal emprega ao transgressor a responsabilidade da salvaguarda das informações de seus clientes/usuários e prevê sanções financeiras, aparentemente as normativas passam a ser levadas mais a sério.

Tão elucidativo quanto aos dados apresentados no Quadro 2, o portal *GDPR Enforcement Tracker* – *GET,* traz aos usuários do mundo uma perspectiva muito abrangente dos impactos financeiros gerados pela *GDPR,* para uma enorme variedade de empresas europeias, uma vez que após a homologação do instrumento

legal de regulação para proteção de dados, as sanções passaram a ser aplicadas de acordo com o previsto em seu texto, fazendo valer assim o direito dos cidadãos. Esse rastreador de aplicações da GDPR visa documentar de forma integralizada todos os casos de penalizações ocorridas, a fim de mapear de forma estatística esse compilado de dados. Suas fontes de dados são documentais, através das medidas judiciais de conteúdos públicos, computadas pelos idealizadores do portal, bem como de colaboradores externos que podem encaminhar suas contribuições.

O portal concentra dados gerais de empresas que sofreram sanções através da *GDPR*, informando seu nome e setor de atuação, um breve resumo do caso, a data da condenação e o artigo aplicável da lei, o tipo de categoria em que o crime se enquadra, o local da ocorrência, a autoridade legal aplicadora da sanção e o documento legal condenatório, bem como o valor, em euros, da multa aplicada. Já foram registrados pelo *GET* mais de 850 casos, desde julho de 2018, tendo uma perspectiva crescente com relação às estatísticas apresentadas, tanto relacionado ao número de casos como às multas aplicadas, que no seu primeiro ano teve uma média de cinco casos ao mês, subindo para média de cerca de 32 casos mensais, nos últimos 12 meses observados, bem como no seu valor, que variou de uma média de € 4.4 milhões para € 111,5 milhões nos períodos respectivos.

Gráfico 1 – Número de Multas Mensais Aplicadas Através da GDPR (Não cumulativo)




Fonte: GDPR Enforcement Tracker (2022)

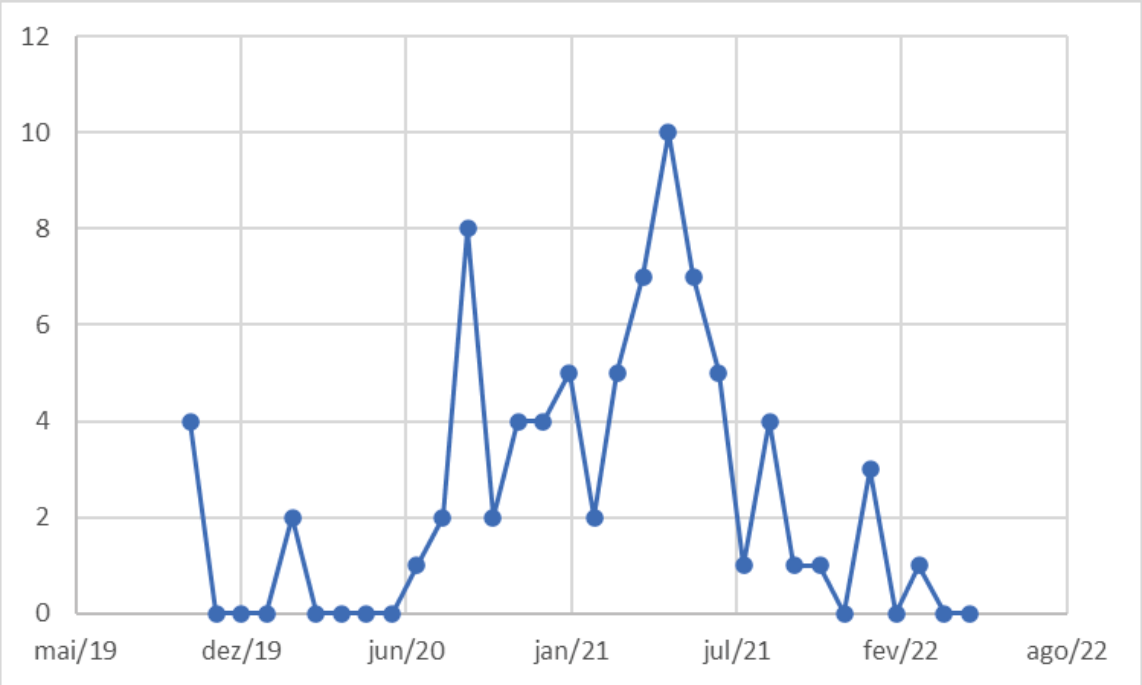
Outros dados de relevância extraídos do portal referem-se aos tipos de infração cometidas pelas empresas, como as que lideram o ranking das multas aplicadas por violação: encabeçam a lista as empresas que foram autuadas por insuficiência de base jurídica para processamento de dados, com 301 casos e não conformidade com os princípios gerais de processamento de dados, com mais de 180 casos. As empresas com maior número de autuações (20%) são do segmento da Indústria e Comércio, estando na sequência (17%) Mídia, Telecomunicações e Radiofusão. A multa mais alta foi aplicada em julho de 2021 à empresa Amazon, em Luxemburgo. Este cenário visa alertar às empresas que realizam transações de dados sensíveis, sobre suas responsabilidades legais, uma vez que muitas delas podem ainda não ter se adequado com o regulamento e estarem vulneráveis tanto aos ataques de invasores, como também pelo uso indevido de dados comercializados informalmente.

Numa proposta voltada ao cenário nacional, de acordo com as sanções já aplicadas pela LGPD, o Portal ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados apresenta uma compilação de casos de penalizações oriundas do descumprimento da lei de proteção de dados no Brasil. Nesse sentido, busca evidenciar a data da ocorrência e o local (estado), bem como o órgão emissor da sanção. Há ainda um breve relato do episódio, a categorização por segmento de atuação da empresa envolvida e um link de acesso externo ao conteúdo original noticiado. Os casos listados não atingem 100 ocorrências, por se tratar de uma vigência recente da imposição das penalidades. Nem todos os casos foram condenados diretamente pela LGPD, pois alguns deles englobam transgressões a outros mecanismos legais, como a própria CF, Lei de Acesso à Informação, Marco Civil da Internet, dentre outros. Dentre os casos que envolvem sanções da LGPD, quase metade deles foram aplicadas multas. O montante do somatório das empresas que foram penalizadas chega a 2,7 milhões de reais, sendo que esses valores variam individualmente de R$ 1000,00 a R$ 2.500.000,00. Mais de dois terços dos casos foram condenados em 1ª instância. Os dados também informam em que/quais artigo(s) se enquadram cada uma das situações. O maior número de descumprimentos de casos, refere-se ao artigo 7º da lei, que abrange a regulamentação do tratamento de dados, que delimita os casos onde se pode ou não realizar esse tratamento. Muitos descumprimentos são oriundos de bancos, que

aparecem em destaque por ocorrências de vazamentos de dados não notificados, que acarretaram em fraudes, gerando prejuízo financeiro às vítimas. Em segunda posição aparecem as entidades sindicais, que na maioria dos episódios relatados os mesmos solicitaram, de maneira irregular, dados dos empregados das empresas, onde os profissionais filiados a essas entidades atuam. Também em destaque estão as empresas que trabalham com comércio online, por transacionarem ilegalmente e de forma maciça os dados pessoais de clientes sem o seu consentimento.

De acordo com a perspectiva apresentada no quadro abaixo é possível identificar o cenário atual de aplicação da LGPD, de acordo com o número de casos relatados pelo portal:

Gráfico 2 – Número de Multas Mensais Aplicadas Através da LGPD (Não cumulativo)




Fonte: ANPPD (2022)

Para os aparelhos com interação humana, que coletam dados sensíveis, sobre a vida cotidiana de seus usuários, há pouco que se especifique na LGPD sobre a forma direta como esses dados serão coletados e armazenados, e também sobre o seu compartilhamento. Nas designações a respeito do consentimento da captação e armazenagem das informações é que se entende a possível regulação desses meios, o que tem por objetivo inibir a comercialização desses dados.

A segurança informacional, dentro do ciclo de vida dos dados, delineado através da LGPD, pode ser melhor direcionada a fim de cumprir essas imposições legais, tendo em vista a revisão dos seus protocolos, ressaltando a importância do que é coletado e armazenado, bem como a forma que os dados são tratados e até mesmo a forma mais segura de garantir sua exclusão sem ferir os princípios de privacidade.

Numa proposta de arquitetura informacional organizacional, estabelecidas as estruturas de redes, alocação dos itens sistêmicos e ainda mais detalhadas como seus modelos específicos, conforme *Zachman* ou mesmo *TOGAF*, a sua principal função seria a de análise quanto às propostas já fixadas e seguidas pela empresa antes e após a homologação da LGPD, uma vez que essa reestruturação traz consigo a possibilidade de revisão de itens críticos inerentes à segurança do banco de dados da organização.

As ferramentas da Engenharia Social vêm sendo aperfeiçoadas de acordo com as características das transações sociais. Conforme a maior adesão aos meios eletrônicos para negociações financeiras e comerciais, os invasores têm se adequado a esses moldes, na tentativa de garantir a continuidade de suas práticas, muitas vezes profissionais. Hoje em dia já existem métodos tecnológicos capazes de identificar semelhança de assinaturas, que trazem maior segurança na emissão de documentos. Mecanismos simples capacitados a identificar a veracidade de cheques, notas de dinheiro em papel moeda. Existem também sistemas competentes para apontar compras potencialmente suspeitas, utilizados principalmente pelas redes bancárias, que analisam através do perfil de consumo de seus clientes uma possível fraude, quando um ponto fora da curva é identificado em seu histórico.

Para Engenheiros Sociais que construíram sua fama baseada em corromper barreiras de sistemas de alta segurança, como Mitnick, Abignale ou Leviev, os instrumentos legais de proteção de dados não indicam nem mesmo um pequeno obstáculo, apenas mera formalidade para constar ao cidadão a sensação de proteção à sua privacidade, pois esse grupo de indivíduos poderá continuar agindo silenciosamente, encontrando formas de driblar qualquer nova barreira sistêmica. Já para as empresas que realizam aquisição, de bases de dados, de clientes de outras empresas, de maneira informal, pode significar um indicativo de alerta para deixar essa prática de lado, bem como a comercialização de sua própria base de dados, uma

vez que isso a enquadra como descumpridora da lei. Alguns desses fatores contribuem para que o cerco se feche em torno dos engenheiros sociais, trazendo mais dificuldade em suas ações contra os usuários. Entretanto, esse universo ainda não apresenta um viés de equilíbrio diante de tantos casos que se destacam na mídia, com relação aos ataques sofridos por grandes empresas ou mesmo pessoas físicas.

Com a LGPD, na teoria, por se tratar de uma normativa que visa a garantia do direito à privacidade dos cidadãos, entende-se que seus instrumentos serão efetivos na busca do estabelecimento desta garantia. Os principais pontos observados no estudo deste marco regulatório, estão relacionados à segurança de dados, pois é através deste aspecto que se pode definir de que forma poderão ser diminuídos os efeitos de ações de Engenharia Social. Buscam frisar a importância do cumprimento das medidas legais, na Seção III do CAP. VI, onde se destaca a responsabilidade pelo ressarcimento de danos aos titulares, pelo vazamento e exposição de seus dados, bem como na Seção I do Cap. VIII onde são previstas as sanções administrativas aplicáveis pela ANPD, que incluem até mesmo o bloqueio do banco de dados empresariais. Também destacado no seu Art. 7º, sobre a necessidade de consentimento dos titulares para o tratamento dos dados, bem como no Art. 48º sobre a responsabilidade de notificação à ANPD sobre os episódios de exposição dos dados pessoais, contidos pelas empresas.

Também de acordo com as definições da LGPD (2018) as pessoas físicas ou jurídicas, de direito público ou privado, deverão sinalizar de forma oficial o seu objetivo em utilizar os dados pessoais, solicitando consentimento de seus portadores. Em seu Art. 5º pode-se entender que o ciclo de vida dos dados se inicia a partir de sua coleta, junto aos detentores (titular), posteriormente eles serão processados, via sistemas e então analisados, para que caso sejam compartilhados com outras entidades empresariais, estejam anonimizados. Na próxima etapa, se estabelece o armazenamento, cujo objetivo principal é a reutilização desses dados, para finalidades previstas e informadas previamente à sua coleta. A última fase desse ciclo é a de eliminação, onde os dados que já não são mais necessários às empresas sejam excluídos. Todas essas etapas ocorrem dentro da organização são de sua inteira responsabilidade e visam garantir a segurança e principalmente a privacidade das informações fornecidas pelos usuários. Alves (2022).

Assim sendo, a Lei Geral de Proteção de Dados Pessoais, após entrar em vigor no Brasil em agosto de 2020, já pode estar sendo considerada como ferramenta de punição às empresas, cujos dados de clientes e usuários se deixar exposto ou de maneira vulnerável a ataques. As multas chegam a 2% do faturamento, no limite de R$ 50 milhões. De acordo com as punições propostas nos demais países, que já aderiram instrumentos legais para proteção de dados, se espera nesse contexto de que o comportamento possa ser semelhante no Brasil.

## 5 CONCLUSÃO E CONSIDERAÇÕES FINAIS

Desde o surgimento das civilizações e seus registros históricos, o homem tem se tornado capaz de contar sua própria história. Os registros antigos demonstram a importância, para os seres sociais, de arquivar suas memórias. O valor informacional vem sofrendo ajustes desde então, de acordo com a percepção do que se pode obter através de sua posse, uma vez que, quanto mais precisa é a informação ela pode tornar seu titular mais vulnerável. Com a ascensão das tecnologias de informação, tornou-se necessário o estabelecimento de controles e ferramentas para a proteção dos dados. Entendendo o direito à privacidade como garantia fundamental para os cidadãos, muitas nações vêm definindo ao longo dos anos, regulamentações e normativas que visam tornar esse direito cada vez mais efetivo.

A LGPD bem como os demais marcos legais similares, com a finalidade de proteger a privacidade dos cidadãos pelo mundo, trazem em seus referenciais uma série de previsões acerca da forma como as informações pessoais desses indivíduos devem ser coletadas, tratadas, armazenadas e extintas dentro do ambiente informacional e social. Também trazem reforços sobre as definições de privacidade e sua contextualização, de acordo com os avanços tecnológicos. Essas previsões buscam a melhor maneira para evitar a exposição de informações, que possam auxiliar a identificação singular dos seres sociais. Uma vez expostos e identificados, os cidadãos passam a ser possíveis alvos para aplicação de golpes. Esse ciclo infinito, desde a obtenção de dados básicos até a subtração de bens maiores e valores configura a cadeia da Engenharia Social. Presente na história dos homens há muitos anos e estabelecida de forma conceitual recentemente, a ES possui diversas ferramentas e definições técnicas, agrupadas de acordo com seus modos de operação. Os agentes dessa cadeia relacionam-se entre si geralmente no contato vítima e golpista, onde a vítima é o foco da aplicação dos estratagemas do golpista, de acordo com as informações que este possui previamente.

Desta forma, entende-se que o objeto principal do estudo, que se trata da informação pessoal, requer constante atenção dos agentes governamentais para garantir a efetividade de sua proteção, uma vez que a sua ruptura pode acarretar numa série de situações de violação e que colocam em risco até mesmo a segurança do indivíduo. Em se tratando de leis que visam esse cumprimento, muitas delas

detalham a obrigatoriedade dos agentes tratadores de dados sobre sua responsabilidade em administrá-los, da origem ao descarte, mantendo sempre informados os titulares sobre esses processos. A importância da revisão dos métodos de coleta de dados, tanto com relação a sua operacionalização como o teor do que é levantado, visando análise sobre a necessidade de tais informações e de que forma podem ser tratadas e armazenadas também tem seu enfoque nos regulamentos. Conforme previsto na LGPD, também é importante informar aos titulares sobre quaisquer situações de exposição as quais os dados podem ter sofrido, bem como a criação de um agente regulador em âmbito nacional para assegurar os cidadãos do seu devido cumprimento. Todas essas medidas são direcionadas ao foco de proteger a privacidade do indivíduo e também tem suas sanções aplicáveis no caso do descumprimento, que geralmente acarretam em multas e até mesmo penalizações, como o bloqueio do seu banco de dados informacionais.

Através da imposição legal, dessas sanções que acarretam o prejuízo financeiro, às empresas que descumprirem as normativas, previstas nos instrumentos legais de proteção de dados de usuários, pode-se enxergar uma perspectiva positiva com relação às inibições das ações de agentes que compõe a cadeia dos mecanismos da Engenharia Social. Como visto no cenário Europeu, de acordo com os relatos do portal *GET*, houve um crescimento exponencial dos casos de multas aplicadas aos transgressores, emitindo um cenário de alerta às empresas que utilizam de maneira informal, dados compilados de usuários, comercializados livremente. Por outro lado, os crackers e invasores, menos profissionais, que atuam no lado mais obscuro desse canal, podem não ser atingidos, por trabalharem de maneira informal nesta prática. Em comparação com a *GDPR*, no sentindo da aplicação de sanções, a LGPD ainda caminha de forma suave com relação a estas penalizações, por se tratar de período mais curto de vigência, o que impacta de certa forma na institucionalização de suas ferramentas, uma vez que em meio à pandemia do COVID-19 e demais situações de crise vivenciadas no país, pode ter havido dificuldade de sua implementação. Além desses fatores, é importante ressaltar que a legislação de proteção de dados europeia abrange uma grande fatia territorial, o que contribui para sua regulação. No Brasil o ente governamental responsável por promover essa regulação (ANPD), ainda se encontra em fase de estruturação e definição de políticas, por ter sido recentemente instituída.

No que tange o cumprimento dos objetivos da realização dessa pesquisa, foi possível através do método de revisão bibliográfica, com pesquisa documental e bibliográfica estabelecer a definição da Lei Geral de Proteção de Dados Pessoais no Brasil, bem como realizar um breve levantamento histórico e social que impulsionou a sua concepção. Também foi possível através desse levantamento encontrar e descrever as similaridades entre a LGPD e os demais marcos legais de proteção de dados pelo mundo, ressaltando seus conceitos básicos, atendendo aos objetivos específicos “A” e “B”. Com o uso dos relatos de casos importantes da história, dignos de se tornarem livros, documentários e até mesmo filmes de grandes produções e com as definições conceituais referentes ao tema da Engenharia Social, bem como a explanação de suas ferramentas atuais, cumpriu-se com os objetivos específicos “C” e “D”. Para análise dos incidentes aplicáveis à LGPD, relativos ao objetivo específico “E”, foi necessária a busca em web sites de revistas e jornais digitais dos relatos da mídia sobre os casos de vazamentos de dados, o que resultou no Quadro 2, bem como da discussão que se segue a respeito do tema, podendo assim satisfazer a intenção do trabalho. Uma das dificuldades encontradas nesse processo foi tornar essa pesquisa tão ampla quanto possível, em função da dispersão das fontes. Ressalta-se que a pesquisa não foi exaustiva e nem todos os episódios podem ser documentados, pois para as empresas não é estratégico ter esse tipo de exposição na mídia, tendo em vista os impactos comerciais que elas podem sofrer, então não há um tipo de consulta pública para essas situações. A pesquisa na mídia foi escolhida como melhor forma de alcançar esses objetivos, pois existem também questões de sigilo acerca da Segurança da Informação, que impediria a coleta de dados diretamente com empresas envolvidas, através de entrevistas, por exemplo, pois poderia invalidar essa pesquisa.

Por fim, para que se atenda ao objetivo geral da pesquisa, relativo à análise dos meios legais capazes de mitigar os efeitos da Engenharia Social, os mesmos dizem respeito principalmente à normalização da forma como se operacionaliza a coleta, tratamento e armazenagem de dados, visando estabelecer a garantia do princípio fundamental da privacidade, tanto para a LGPD como para as leis de mesmo teor do cenário global, que possuem delineamentos acerca do tema. Então, é possível inferir que a LGPD pode ser um fator de inibição aos mecanismos da Engenharia Social, uma vez que seu objetivo principal é garantir a privacidade dos dados dos

cidadãos, mantendo as empresas detentoras desses dados, tanto públicas como privadas, alertas ao seu ônus em caso de não cumprimento e estabelecimento de medidas de segurança da informação. Concluindo, a realização desta pesquisa colabora para a melhor compreensão do tema, e pode-se também inferir que a aplicação dos mecanismos regulatórios da LGPD, a exemplo do que ocorre hoje na Europa (na qual já foram, desde 2019, aplicados mais de 1,6 bilhão de Euros em multas), poderá contribuir para mitigar alguns dos mecanismos levantados.

## 6 REFERÊNCIAS BIBLIOGRÁFICAS:


- AGRA, Andressa. D.; BARBOZA, Fabrício. Felipe. M. ***Segurança de sistemas da informação*** < Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595027084/ > Acesso em: 09/11/2021.

- ALVES, Gervânia – ***Ciclo de Vida dos Dados e LGPD*** – Disponível em: < https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd >. Acesso em 12/01/2022.

*- ANDRADE, Nélio -* ***Lei de Proteção de dados traz desafios a empresas, cidadãos e governo*** *– Disponível em: < http://agenciabrasil.ebc.com.br/geral/noticia/2019-08/lei-de-protecao-de-dados-traz-desafios-empresas-cidadaos-e-governo* > Acesso em 01/03/2020.

- ANDRADE, Vitor Morais de; HENRIQUE, Lygia Maria M. Molina - ***Vazamento de dados: uma preocupação da Lei Geral de Proteção de Dados*** **- Disponível** em: < https://www.migalhas.com.br/depeso/298452/vazamento-de-dados--uma-preocupacao-da-lei-geral-de-protecao-de-dados > Acesso em 17/07/2021.

- ANPPD – ***Associação Nacional dos Profissionais de Privacidade de Dados*** – Disponível em: < https://anppd.org/ > Acesso em 16/05/2022.

- ARAMUNI, João Paulo, MAIA, Luiz Cláudio - ***O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa***. Disponível em: < http://dx.doi.org/10.5380/atoz.v7i1.64640 > AtoZ: novas práticas em informação e conhecimento, 2018.

- Assis e Mendes Advogados – **Direito Digital, Empresarial e Proteção de Dados** – Disponível em: < https://assisemendes.com.br/historico-protecao-de-dados/ > Acesso em 10/11/2021.

- AUDY, Jorge Luis Nicolas; ANDRADE, Gilberto Keller.; CIDRAL, Alexandre - **Fundamentos de Sistemas de Informação** – Editora Bookman, 2007. Disponível em: < https://integrada.minhabiblioteca.com.br/#/books/9788577801305/ > Acesso em 25/03/2022.

- BARBOSA, Ricardo Rodrigues - ***Gestão Da Informação E Do Conhecimento: Origens, Polêmicas e Perspectivas*** *– INF – LONDRINA – 2008.*
- BARRETO, Aldo Albuquerque – ***A Questão da informação -*** São Paulo em Perspectiva, Fundação Seade, v.8, n.4, 1994.

- BARRETO, Aldo Albuquerque – ***Uma Quase História da Ciência da Informação*** – Disponível em: < https://ridi.ibict.br/bitstream/123456789/162/1/Barreto%205.pdf > Acesso em 25/03/2022.

- BARRETO, Jeanine dos Santos; ZANIN, Aline; MORAIS, Izabelly Soares; VETTORAZZO, Adriana - ***Fundamentos de Segurança da Informação*** - Disponível

em: https://integrada.minhabiblioteca.com.br/#/books/9788595025875/ > Acesso em 09/11/2021.

- BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André – ***Fundamentos da Segurança da Informação Com base na ISSO 27001 e na ISSO 27002*** – Brasport – São Paulo – 2011.

- BELLOQUIM, Atila - ***Frameworks de Arquitetura*** – Disponível em: < https://arquiteturacorporativa.com.br/2010/09/frameworks-de-arquitetura-parte-2-togaf/ >. Acesso em 12/02/2022.

- BLOM, José Roberto Opice – ***China aprova Lei de Proteção de Dados Pessoais semelhante à LGPD e ao GDPR*** – Disponível em: < https://opiceblum.com.br/china-aprova-lei-de-protecao-de-dados-pessoais-semelhante-a-lgpd-e-ao-gdpr/ > Acesso em 25/03/2022.

- BOTTINO, Celina. Perrone, Christian. Carneiro, Giovana. Heringer, Leonardo. Viola, Mário. - **Lei Geral de Proteção de Dados e Resolução de Conflitos: Experiências Nacionais e Internacionais** – Disponível em: < https://itsrio.org/wp-content/uploads/2020/04/Relatorio_LGPDResolucaoConflitos.pdf > Acesso em 25/03/2022.

- BRASIL – ***Constituição Federal*** – Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm > Acesso em 28/02/2021.

- BRASIL – ***Lei Geral de Proteção de Dados Pessoais 13.709/2018*** – Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm > Acesso em 10/09/2021.

- CÂMARA DOS DEPUTADOS - ***Acesso à Informação*** – Disponível em: < https://www2.camara.leg.br/transparencia/acesso-a-informacao > Acesso em 31/03/2022.

- CAMARGO, Liriane Soares; GREGÓRIO, Silvana Aparecida - ***Arquitetura da Informação - Uma Abordagem Prática*** - Disponível em: < https://integrada.minhabiblioteca.com.br/#/books/978-85-216-2094-5/.> Acesso em 11/11/2021.

- CANALTECH - Banco de dados expôs 235 milhões de usuários do TikTok, YouTube e Instagram – Disponível em: < https://canaltech.com.br/seguranca/banco-de-dados-expos-235-milhoes-de-usuarios-do-tiktok-youtube-e-instagram-170220/ > Acesso em 01/09/2021.

- CANALTECH - ***Relembre os maiores vazamentos de informação de 2013*** - Disponível em: < https://canaltech.com.br/seguranca/relembre-os-maiores-vazamentos-de-informacao-de-2013-17910/> Acesso em 01/09/2021.

- CANALTECH - ***Volkswagen culpa fornecedor por vazamento dos dados de 3,3 milhões de clientes*** – Disponível em: <

https://canaltech.com.br/seguranca/volkswagen-culpa-fornecedor-por-vazamento-dos-dados-de-33-milhoes-de-clientes-187129/ > Acesso em 01/09/2021.

- CARTA CAPITAL - ***Expostos: a falta de proteção e os mega vazamentos de dados no Brasil*** – Disponível: < https://www.cartacapital.com.br/tecnologia/expostos-a-falta-de-protecao-e-os-megavazamentos-de-dados-no-brasil/ > Acesso em 01/09/2021.

- CESAR JÚNIOR, Roberto Marcondes - ***Do mundo aos dados e dos dados ao conhecimento***. In: HEY, Tony; TANSLEY, Stewart; TOLLE, Kristin (Org.). O quarto paradigma: descobertas científicas na era da e Science. São Paulo: Oficina do Texto, 2011.

- CHOO, Chun Wei - ***A Organização Do Conhecimento*** - São Paulo: Senac, 2003.
- COELHO, Cristiano Farias. RASMA, Eliane Tourinho. Morales, Gaudélia - ***ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO*** – Disponível em: < https://ojs3.perspectivasonline.com.br/exatas_e_engenharia/article/view/87/59 > Acesso em 01/04/2022.

- COINTELEGRAPH - ***Embraer confirma invasão de hackers e vazamento de dados; empresa diz que não pagou criptomoedas de resgate*** – Disponível em: https://cointelegraph.com.br/news/embraer-confirms-hacker-invasion-and-data-leak-company-says-it-didnt-pay-ransom-cryptocurrencies > Acesso em 01/09/2021.

- COMPUGRAF – ***Quais os principais tipos de ataques de Engenharia Social*** - Disponível em: < https://www.compugraf.com.br/quais-os-principais-tipos-de-ataque-de-engenharia-social/ > Acesso em 03/09/2021.

- CONVERGÊNCIA DIGITAL - ***Claro e Vivo são condenadas por vazamento de dados*** – Disponível em: < https://www.convergenciadigital.com.br/Telecom/Claro-e-Vivo-sao-condenadas-por-vazamento-de-dados-57434.html?UserActiveTemplate=mobile > Acesso em 01/09/2021.

- DICIONÁRIO MICHAELIS ONLINE - ***Segurança*** - Disponível em: < http://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/seguran%C3%A7a/. > Acesso em 28/02/20.

- DIEB, Daniel - ***Coração, diabetes e mais: como apps revolucionam nosso cuidado com a saúde*** - Disponível em: < https://www.uol.com.br/tilt/noticias/redacao/2020/01/06/da-diabetes-a-terapia-apps-ajudam-medicos-e-pacientes-no-cuidado-a-saude.htm > Acesso em 09/11/2021.

- DURBANO, Vinícius - ***Leis de Proteção de Dados pelo Mundo: como aplicar a devida prioridade e importância dos dados pessoais*** – Disponível em: < https://blog.ecoit.com.br/leis-de-protecao-de-dados-pelo-mundo-como-aplicar-a-devida-prioridade-e-importancia-dos-dados-pessoais/ > Acesso em 25/03/2022.

- EXAME - ***Twitter expôs dados de usuários de smartphones Android*** – Disponível em: < https://exame.com/tecnologia/twitter-expos-dados-de-usuarios-de-smartphones-android/ > Acesso em 01/09/2021.

- EXAME - ***Vazamento de Site da BB Previdência Expõe Dados de 153 mil Clientes*** – Disponível em: < https://exame.com/negocios/vazamento-de-site-da-bb-previdencia-expoe-dados-de-153-mil-clientes/ > Acesso em 01/09/2021.

- FMP, FUNDAÇÃO ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO - ***Lei Carolina Dieckmann: Você Sabe O Que Essa Lei Representa?*** – Disponível em: < https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/ > Acesso em 30/03/2022.

- FERNANDES, Gustavo - ***Captura de perfis dinâmicos de usuários a partir da análise de mensagens em redes sociais*** – Disponível em: < http://www.repositorio-bc.unirio.br:8080/xmlui/bitstream/handle/unirio/12531/MI201317.pdf?sequence=1 > Acesso em 09/11/2021.

- FREITAS, Guilherme Farage - ***A Lei Geral de Proteção de Dados nas Relações de Consumo: O Impacto no Desenvolvimento da Atividade de E-Commerce*** - Disponível em: < https://repositorio.animaeducacao.com.br/handle/ANIMA/14267 > Acesso em 18/07/2021.

- GAZETA REGIONAL - ***Prefeitura de Poá deixa vazar dados de 2,7 mil funcionários*** – Disponível em: < https://www.leiaogazeta.com.br/prefeitura-de-poa-deixa-vazar-dados-de-27-mil-funcionarios/ > Acesso em 01/09/2021.

- GET – ***GDPR ENFORCEMENT TRACKER*** - Disponível em: < https://www.enforcementtracker.com/ > Acesso em 31/03/2022.

- GONÇALVES, Victor Hugo P. - ***Marco Civil da Internet Comentado*** - Grupo GEN, 2016. Disponível em: < https://integrada.minhabiblioteca.com.br/#/books/9788597009514/. >. Acesso em 12/02/2022.

- GRADIM, Luca Cisneiros - ***Análise Comparada da Lei Geral de Proteção de Dados com o Regulamento Europeu sobre a Proteção de Dados e a Proteção de Dados nos Estados Unidos*** - Disponível em: < https://repositorio.uniceub.br/jspui/bitstream/prefix/14892/1/Luca%20Gradim.pdf > Acesso em 17/07/2021.

- G1 GLOBO, ***Ataque de hackers ao Citibank afetou 360 mil contas de clientes*** - **Disponível** em: < http://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-ao-citibank-afetou-360-mil-contas-de-clientes-do-banco.html > Acesso em 01/09/2021.

- G1 GLOBO – ***Facebook pagará multa recorde de US$ 5 bilhões por violação de privacidade*** - Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/2019/07/24/facebook-pagara-multa-de-us-5-bilhoes-por-violacao-de-privacidade.ghtml > Acesso em 01/09/2021.

- G1 GLOBO - ***Netshoes Terá de Pagar R$ 500 Mil por Vazamento de Dados de 2 Milhões de Clientes*** - Disponível em: < https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml > Acesso em 01/09/2021.

- ISTO É - **Clientes do Latam Pass têm Dados vazados Após Ataque à Empresa de TI** – Disponível em: < https://www.istoedinheiro.com.br/clientes-do-latam-pass-tem-dados-vazados-apos-ataque-a-empresa-de-ti/ > Acesso em 01/09/2021.

- ISTO É – ***Uber pagará US$ 148 milhões por vazamento de dados*** - Disponível em: < https://www.istoedinheiro.com.br/uber-pagara-us-148-milhoes-por-vazamento-de-dados/ > Acesso em 01/09/2021.

- JORNAL DO CARRO - ***Detran deixa vazar dados de 70 milhões de brasileiros com CNH*** – Disponível em: < https://jornaldocarro.estadao.com.br/carros/detran-vaza-dados-70-milhoes-brasileiros/ > Acesso em 01/09/2021.

- LOZADA, Gisele; NUNES, Karina da Silva - ***Metodologia Científica*** - Grupo A, 2019. < Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595029576/ > Acesso em 29/11/2021.

- LYMAN, Peter; VARIAN, Hal R. (2003) - ***How Much Information*** – Disponível em:

< https://groups.ischool.berkeley.edu/archive/how-much-info-2003/ > Acesso em: 22/03/2022.

- MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George - ***Hackers Expostos***. Grupo A, 2014. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601426/. Acesso em: 12/02/2022.

- MAGNO, Carlos; ROSAL, Bispo - ***Auditoria de Segurança da Informação em Sistemas e Aplicações -*** Disponível em: < https://repositorio.unb.br/handle/10482/25258 >. Acesso em 12/02/2022.

- MANN, Ian. ***Engenharia Social***. Série Prevenção de Fraudes. Editora Edgar Blücher, 2018.

- MARINHO, Fernando – ***Os Dez Mandamentos da LGPD* (*Como Implementar a Lei Geral de Proteção de Dados em 14 Passos)*** – Editora Atlas, São Paulo, 2020.

- MATOS, Tiago Farina. ***Comércio de dados, privacidade e internet*** - Disponível em: < https://ambitojuridico.com.br/edicoes/revista-18/comercio-de-dados-privacidade-e-internet/ > Acesso em 15/09/2021.

- MITNICK, Kevin. ***A Arte de Enganar.*** Editora Pearson Education, 2003.

- MORAIS, Izabelly Soares. GONÇALVES, Priscila de Freitas. LEDUR, Cleverson L. - ***Introdução a Big Data e Internet das Coisas (IoT)*** – Ed. Sagah Educação, Porto Alegre, 2018.

- NASCIMENTO, Luiz Paulo - ***Elaboração de projetos de pesquisa: Monografia, dissertação, tese e estudo de caso, com base em metodologia científica.*** - Cengage Learning Brasil, 2016.

- NETAPP - ***Worldwide Data Privacy Regulations Compared*** – Disponível em: < https://www.portosrio.gov.br/sites/default/files/inline-files/Worldwide%20Data%20Privacy%20Regulations%20Compared.pdf.pdf > Acesso em 01/12/2021.

- NUNES, Natália Martins – ***Os requisitos para tratamento de dados pessoais no Brasil*** – Disponível em: < https://ndmadvogados.jusbrasil.com.br/artigos/620879223/os-requisitos-para-tratamento-de-dados-pessoais-no-brasil > Acesso em 29/02/2020.

- OLHAR DIGITAL - ***Ali babá é hackeado; 1 bilhão de dados de clientes foram roubados*** – Disponível em: < https://olhardigital.com.br/2021/06/16/seguranca/alibaba-hackeado-1-bilhao-de-dados-roubados/ > Acesso em 01/9/2021.

- OLIVEIRA, D. M.; RODRIGUES, L. A. S.; FROGERI, R. F.; PORTUGAL JUNIOR, P. S. - ***Habilidades e competências do profissional da informação. Encontro Nacional de Pesquisa em Ciência da Informação***, n. XX ENANCIB, 2019. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/122364>. Acesso em 29/02/2020.

- O GLOBO - ***Facebook pagará multa recorde de US$ 5 bilhões por violação de privacidade*** - Disponível em: < https://oglobo.globo.com/economia/vazamento-de-152-milhoes-de-contas-de-usuario-da-adobe-pode-ter-sido-maior-da-historia-10725973 > Acesso em 01/09/2021.

- PAES, Eneida Bastos. - ***A construção da Lei de Acesso à Informação Pública no Brasil: desafios na implementação de seus princípios*** – Disponível em: < https://revista.enap.gov.br/index.php/RSP/article/view/80 > Acesso em 01/04/2022.

- PAIXÃO, Pedro – ***Proteção de Dados na América Latina*** – Disponível em: < https://itforum.com.br/noticias/protecao-de-dados-na-america-latina/ > Acesso em 25/03/2022.

- PASSARELI, Vinícius – ***LGPD: Entenda o que é Lei Geral de Proteção de Dados Pessoais*** - Disponível em: < https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/ > Acesso em 01/03/20.

- PEIXOTO, Mário César Pintaudi - ***Engenharia Social & Segurança da Informação na Gestão Corporativa***. Brasport: Rio de Janeiro, 2006.

- PEREIRA, Luiz Carlos Bresser - **Notas para o curso de Teoria do Estado, do Mestrado Profissional em Gestão Pública** – EAESP, 2010.

- POPPER, Karl - *The* ***Open Society and Its Enemies*** - Princeton, New Jersey: Princeton University Press, 1971.

- QUEIROZ, Rita de Cássia Ribeiro – A Crítica Textual e a Recuperação da História – Disponível em: <

http://www.filologia.org.br/scripta_philologica/01/A_Cr%C3%ADtica_Textual_e_a_Recupera%C3%A7%C3%A3o_da_Hist%C3%B3ria.pdf > Acesso em 22/03/2022.

- ROBERTSON, Adi - ***Netflix documentary The Great Hack turns the Cambridge Analytica scandal into high drama –*** Disponível em: < https://www.theverge.com/2019/1/30/18200049/the-great-hack-cambridge-analytica-netflix-documentary-film-review-sundance-2019 > Acesso em 28/02/2020.

- ROCHA, Carin Cunha; PINTO, Virgínia Bentes; DAVID, Priscila Barros - ***Arquitetura da informação: revisão integrativa em bases de dados de ciência da informação*** – Disponível em: < https://www.uel.br/revistas/uel/index.php/informacao/article/view/38061/pdf > Acesso em 09/11/2021.

- *ROHLING, Marcos* - ***O conceito de lei, lei legítima e desobediência civil na teoria da justiça como equidade de John Rawls.Synesis*** - Disponível em: < http://seer.ucp.br/seer/index.php?journal=synesis&page=article&op=view&path%5B%5D=580 > Acesso em: 28/02/2020.

- ROSA, Natalie. - ***Crítica O Golpista do Tinder | Quando um conto de fadas acaba em pesad***elo – Disponível em: < https://canaltech.com.br/entretenimento/critica-o-golpista-do-tinder-netflix-208287/ > Acesso em 01/04/2022.

- ROTHER, Edna Terezinha – ***Revisão Sistemática X Revisão Narrativa*** – Disponível em: < https://doi.org/10.1590/S0103-21002007000200001 >Acesso em 01/12/2021.

- RUSSEL, Chad; FULLER, Shane. - ***GDPR For Dummies*** - MetaCompliance Special Edition. West Sussex : John Wiley & Sons, 2017.

- SAYÃO, L. F.; SALES, L. F. - ***Curadoria digital: um novo patamar para preservação de dados digitais de pesquisa -*** Informação e Sociedade, p. 179–191, 2012.

- SERRA, João Paulo - ***Manual de Teoria da Comunicação*** - Covilhã: Livros Labcom. p. 93-101, 2007.

- SILBERSCHATZ, Abraham - ***Sistema de Banco de Dados*** - Grupo Editorial Nacional, Rio de Janeiro, 2020.

- SOUZA, Queila R. QUANDT, Carlos O. ***Metodologia de Análise de Redes Sociais***. In: F. Duarte; C. Quandt; Q. Souza. (Org.). O Tempo das Redes. São Paulo: Perspectiva, 2008.

- TECHTUDO - ***Nintendo confirma vazamento de dados de 160 mil contas; saiba o que fazer*** – Disponível em: < https://www.techtudo.com.br/noticias/2020/04/nintendo-confirma-vazamento-de-dados-de-160-mil-contas-saiba-o-que-fazer.ghtml > Acesso em 01/09/2021.

- TECHTUDO - ***Vazamento de dados da Microsoft expõe 250 milhões de registros de usuários*** – Disponível em: < https://www.techtudo.com.br/noticias/2020/01/vazamento-de-dados-da-microsoft-expoe-250-milhoes-de-registros-de-usuarios.ghtml > Acesso em 01/09/2021.

- TECMUNDO - ***British Airways é multada em r$ 900 milhões por vazamento de dados*** – Disponível em: < https://www.tecmundo.com.br/seguranca/143529-british-airways-multada-r-900-milhoes-vazamento-dados.htm > Acesso em 01/09/2021.

- TECMUNDO - ***C&A é hackeada e vazam dados pessoais de clientes*** - Disponível em: < https://www.tecmundo.com.br/seguranca/133753-c-hackeada-vazam-dados-pessoais-clientes.htm > Acesso em 01/09/2021.

- TECMUNDO – ***O que é Cracker?*** - Disponível em: < https://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm > Acesso em 16/05/2022.

- TECNOBLOG - ***Banco Inter paga R$ 1,5 milhão e encerra processo sobre vazamento de dados*** - Disponível em: < https://tecnoblog.net/272056/banco-inter-acordo-mpdft/ > Acesso em 01/09/2021.

- TECNOBLOG - ***Uber pagará multa de US$ 148 milhões após encobrir vazamento de dados*** - Disponível em: < https://tecnoblog.net/261648/uber-multa-encobrir-vazamento/ > Acesso em 01/09/2021.

- TECNOBLOG - ***Google recebe multa de 50 milhões de euros na França por violar GDPR*** - Disponível em: < https://tecnoblog.net/275817/google-multa-gdpr-franca/ > Acesso em 01/09/2021.

- TECNOBLOG - ***MP investiga Banco Pan após vazamento de 250 GB em dados de clientes*** – Disponível em: < https://tecnoblog.net/306130/mp-investiga-banco-pan-dados-clientes/ > Acesso em 01/09/2021.

- THE HACK - ***Dados de 4.5 milhões de clientes da Air Índia são vazados em ataque a associação gestora de transporte aéreo*** – Disponível em: < https://thehack.com.br/dados-de-4-5-milhoes-de-clientes-da-air-india-sao-vazados-em-ataque-a-associacao-gestora-de-transporte-aereo/ > Acesso em 01/09/2021.

- THE HACK - ***Exclusivo: empresa deixa vazar 33 mil exames médicos de funcionários da Vale, Prosegur e outras*** – Disponível em: < https://thehack.com.br/exclusivo-empresa-deixa-vazar-33-mil-exames-medicos-de-funcionarios-da-vale-prosegur-e-outras/ > Acesso em 01/09/2021.

-THE HACK - ***McDonald's sofre ataque cibernético e tem dados internos comprometidos*** – Disponível em: < https://thehack.com.br/mcdonalds-sofre-ataque-cibernetico-e-tem-dados-internos-comprometidos/ > Acesso em 01/09/2021.

- TOPOLNIAK, Luciano; FEDERICE, Anderson; TAVARES, Ricardo Ribeiro; INÁCIO, Sandra Regina da Luz - ***Desenvolvimento prático de projetos de segurança da informação no Instituto Federal de Educação de Rondônia*** – Disponível em: <

https://www.brazilianjournals.com/index.php/BRJD/article/view/44122/pdf >. Acesso em 12/02/2022.

- UOL – ***LinkedIn é alvo de nova denúncia de vazamento de dados*** - Disponível em: < https://www.uol.com.br/tilt/noticias/redacao/2021/06/29/vazamento-no-linkedin-expoe-dados-de-mais-de-90-dos-usuarios-o-que-fazer.htm > Acesso em 01/09/2021.

- VALENTIM, Marta Lígia - ***Gestão Da Informação E Gestão Do Conhecimento: Especificidades E Convergências*** - Londrina: Infohome, 2004. Disponível em: < https://www.brapci.inf.br/_repositorio/2010/01/pdf_ea77bd91aa_0007779.pdf >. Acesso em 22/03/2022.

- WURMAN, Richard Saul - **Information Architects**. 2. Ed. Lakewood: Watson-Guptill Pubns, 1997.

- ZACHMAN, Jonh. A. – ***A Framekwork for Information Systems Architeture*** – IBM Systems Journal, vol. 26, nº 3, 1987 – Los Angeles, 1987.