REVES - Revista Relações Sociais, Vol. 05 N. 04 (2022)
https://periodicos.ufv.br/reves
eISSN: 2595-4490

Contribuições da LGPD para amenização dos efeitos dos mecanismos da Engenharia Social

LGPD'S Contributions to mitigate the effects of Social Engineering mechanisms

Bryan Felipe de Oliveira
ORCID: https://orcid.org/0000-0002-6866-903X
PPG Gestão da Informação – UFPR, Brasil
E-mail: bryan_f@ufpr.br
José Simão de Paula Pinto
ORCID: http://orcid.org/0000-0002-5023-437X
PPG Gestão da Informação – UFPR, Brasil
E-mail: simao@ufpr.br

Article Info:
Article history: Received 2022-05-21
Accepted 2022-07-25
Available online 2022-09-27
doi: 10.18540/revesvl5iss4pp14712-01e

Resumo. Esta pesquisa tem como objetivo central a análise das contribuições que a lei geral de proteção de dados pessoais (LGPD) pode trazer, para amenizar os efeitos dos mecanismos da Engenharia Social (ES). Utiliza da abordagem descritiva e qualitativa, através de revisão de literatura e documental. A relevância do estudo se relaciona ao enfoque de temas contemporâneos, de extrema importância no atual contexto social e tecnológico, referentes à privacidade de dados e segurança virtual. Foi possível, através da pesquisa desenvolvida, inferir que a LGPD possui em seu arcabouço aspectos e previsões que podem inibir ações dos agentes da ES. O estudo também traz contribuições às pesquisas futuras acerca dos temas que correlacionam seus principais tópicos.
Palavras-chave: LGPD; Engenharia Social; Segurança da Informação; Gestão de Dados.

Abstract. The main objective of this research is to analyze the contributions that the general law for the protection of personal data (LGPD) can bring, to mitigate the effects of the mechanisms of Social Engineering (SE). It uses a descriptive and qualitative approach, through literature and document review. The relevance of the study is related to the approach of contemporary themes, of extreme relevance in the current social and technological context, referring to data privacy and virtual security. It was possible, through the developed research, to infer that the LGPD has in its framework aspects and predictions that can inhibit actions of SE agents. The study also brings contributions to future research on the themes that correlate its main topics.
Keywords: LGPD; Social Engineering; Information Security; Data Management.

1 - Introdução

Desde a origem das primeiras organizações sociais é evidente, através da análise dos contextos históricos, que a informação é algo de extrema relevância para os indivíduos e aos grupos a que estes estão associados. É através da informação obtida sobre um grupo social ou mesmo a respeito de um indivíduo que se pode conhecer suas fragilidades, o que os torna vulneráveis ao detentor dessas informações. De acordo com a evolução das sociedades e a percepção desse enfoque, de valorização da informação, é que esta passou a ser cada vez mais protegida, com a finalidade de resguardar seus titulares e assim promover maior segurança e amenizar os riscos aos quais estariam sujeitos, pela vulnerabilidade dos seus dados.

A engenharia social (ES) pode ser entendida, de acordo com Mann (2018) como um complexo de mecanismos e técnicas de manipulação de indivíduos, a fim de coagi-los a executar ações, muitas vezes nocivas a si mesmos. Apesar de fortemente difundida na era da internet, por conta do crescimento do número de conexões que se estabeleceram, que gerou aumento exponencial no fluxo de dados transmitidos entre usuários, a *ES* pode ser identificada em ações de agentes mal-intencionados há muito tempo, antes mesmo do surgimento das tecnologias digitais, que atualmente permeiam nossa vida cotidiana.

Por conta do aumento das conexões, que proporcionam um vasto fluxo de dados, pela grande rede mundial, é que se tornou necessária a instituição de marcos legais, instrumentos de imposição ao grupo social e seus indivíduos, sobre as normativas gerais que visam garantir o resguardo à segurança dos dados dos cidadãos. Desde a década de 1970 em Hessen, na Alemanha, já se falava de privacidade e segurança da informação no âmbito jurídico e legal, o que veio evoluindo juntamente com as tecnologias digitais. No Brasil em 2018 foi sancionada a Lei 13.709, conhecida como LGPD, baseada nos marcos legais internacionais de mesmo teor, com o enfoque em estabelecer diretrizes para o tratamento de dados no país, sua proposta visa garantir a privacidade dos cidadãos e nesse contexto também pode trazer benefícios para amenizar os efeitos das ferramentas da ES.

2 – Referencial Teórico

2.1 – Gestão da Informação:

Sendo o surgimento da escrita um dos grandes marcos na história da informação, na linha do tempo da humanidade, este expressa grande relevância dos registros da existência humana, dos seus costumes, crenças, comportamentos, etc. Queiroz (2005) define como um dos principais aspectos norteadores para o estudo da história do homem e da informação, pois é através da escrita que o ser humano passou a expressar, de maneira mais clara e contida, a mensagem que se deseja transmitir. Antecedendo a escrita, muitos historiadores apontam que pinturas rupestres, identificadas como de períodos pré-históricos, já vinham esboçando esse mesmo sentido para as figuras registradas, como por exemplo da contagem dos períodos das luas, dos rebanhos de animais, as cheias de rios, chuvas, plantios e colheitas, etc. Serra (2007) define que a informação pode ser definida como o produto

da manipulação e organização dos dados, que gera conhecimento ao sistema responsável pelo seu processamento.

A fim de estabelecer parâmetros para ideal organização dos dados, no ambiente social, de maneira lógica e ordenada, a gestão da informação busca explorar a melhor forma de fazê-lo. Entendida como ciência na sociedade atual, expressa a necessidade dos indivíduos e dos seus coletivos, de organizar as informações a fim de obter resultados, Barbosa (2008). A maneira como os indivíduos interagem com o meio e com seus semelhantes gera a cada instante um grupo de dados e informações, que são o insumo para geração de novas atividades e interações. Choo (2003) entende que é da natureza humana a atividade exploratória e com isso se podem estabelecer diversas experiências, que registradas na forma de dados, terão utilidade para a continuação de sua história individual e coletiva, que se pode entender como geração de conhecimento.

Com a evolução do homem e suas tecnologias, o contexto de onde a informação é produzida e armazenada também sofreu diversas modificações. Das pinturas primitivas aos bits armazenados nas nuvens. Essa transformação evidencia o inestimável aumento desse fluxo, que há cerca de vinte anos Lyman (2001) já entendia como um agrupamento, que dobrava de volume a cada ciclo bienal. Para Morais *et al* o fenômeno big data pode ser percebido como produto da realidade tecnológica das sociedades atuais, onde o grande volume de dados gerado precisa ser administrado e armazenado a cada instante. A fim de estabelecer a melhor forma de gerir a informação, foram então concebidos e desenvolvidos os Sistemas de Informação (SI), que são ferramentas capazes de otimizar o fluxo dos dados, através de uma interface que gera comunicação entre usuários, recepcionando, transmitindo e armazenando informações, Audy (2007). A forma como são concebidos os *SI* estabelece onde, como e quando a informação estará disposta no meio digital. A arquitetura de informação, concebida por Wurman (1997) expressa a melhor maneira de se definir essa relação, fazendo analogia com a arquitetura de um edifício ou casa, que consiste em projetar e planejar uma construção, antecedendo sua execução, tornado possível a redução dos erros calculados em sua trajetória. Zachman (1987) destacou a definição de arquitetura informacional, relacionada à questão organizacional, estabelecendo como ponto primordial a concepção de um *framework*, ferramenta de base para a programação, que é tido como um modelo para as futuras aplicações, uma espécie de matriz do *SI,* para que os profissionais possam realizar o devido mapeamento dos dados. O *The Open Group Architeture*, baseado nos mesmos ideais de Zachman, também visava trazer a figura do *framework* do mundo acadêmico para as áreas profissionais, de Tecnologia da Informação (TI), porém seu enfoque principal era de reduzir custos aos usuários. Ambos os modelos expressam a idealização da arquitetura organizacional empresarial, que visa estabelecer e otimizar os princípios da segurança da informação dos usuários, desde a coleta até seu descarte.

As redes sociais podem ser entendidas como um ambiente onde os indivíduos realizam contato entre si. Na era digital, esses ambientes funcionam como um dos centros da comunicação entre os seres sociais, que realizam interações com experiências das mais diversificadas, sejam através do envio de mensagens de texto, voz, vídeos, imagens, tornando as experiências sensoriais mais ricas e envolventes, Souza (2008). Em se tratando de experiências sensoriais, Agra *et al* (2018) menciona a Internet das Coisas, termo difundido pelo pesquisador britânico Kevin Ashton nos anos 2000, para definir as conexões contidas em dispositivos, que podem transmitir e recepcionar dados através de uma rede local ou mais ampla, gerando interação entre indivíduo e dispositivo. Esse conceito vem se tornando fortemente difundido, por estar

cada dia mais presente na realidade das pessoas, do uso de s*martwatches* (relógios inteligentes), s*martphones* (telefones inteligentes), a uma infinidade dispositivos *IoT – Internet of Things,* que são entendidos como mecanismos de automação que tornam ações da rotina humana mais práticas.

Baars (2011) entende que a segurança da informação pode ser um conceito atual em sua definição, porém tem seu significado disposto há muito mais tempo, como por exemplo no antigo Egito, onde já eram utilizados hieróglifos codificados de maneiras não ordenadas, cujo conhecimento para sua leitura era restrito apenas aos indivíduos considerados mais importantes naquele contexto social, visando a proteção dos impérios e de suas riquezas. Quanto mais difundidas as ferramentas tecnológicas na era digital, maior a preocupação com o resguardo dos dados que por elas tramitam, tendo em vista os impactos que podem ser causados pela sua exposição. Barreto *et al* (2018) defende que o princípio norteador para segurança digital são as políticas de segurança da informação (PSI), que podem ser entendidas como um coletivo de diretrizes aos profissionais de TI, para que se desenvolvam novos SI e aprimoramento dos já existentes, com o objetivo central de se compor um ambiente virtual de segurança, por onde as informações possam trafegar de maneira protegida e que não haja quebra de protocolos. Russel (2017) cita uma das primeiras ocasiões em que o termo privacidade foi definido em mecanismos legais, relacionado à salvaguarda de informações, data de 1970, no então Regulamento de Hessen - Alemanha, onde foram definidos os primeiros passos sobre a proibição da violação da intimidade dos cidadãos, em marcos legais, entendida como a possível exposição das suas informações pessoais, que pudessem gerar desdobramentos acerca do seu uso para fins ilícitos, trazendo inclusive prejuízos aos seus titulares.

2.2 – Engenharia Social

Para Mitnick (2003) o termo engenharia social se popularizou na era da internet, após os anos 1990, porém seus mecanismos já eram utilizados em períodos anteriores ao surgimento da grande rede mundial. A arte de ludibriar um indivíduo, observando seu comportamento, com objetivo de definir suas principais fragilidades e atuar sobre elas, para obter para si algo de valor desse indivíduo ou mesmo alguma ação que possa ser prejudicial a ele.

McClure *et al* (2014) cita o termo *hacker* para definir um agente invasor, que utiliza suas habilidades práticas e conhecimentos de SI para burlar os protocolos de segurança. Já Barreto (2018) entende que um invasor pode assumir diferentes papéis, que são direcionados pela sua forma de atuação. Os c*rackers,* denominação oriunda do idioma inglês, da palavra "*crack*", que pode ser traduzida livremente como "quebra", são os principais responsáveis envolvidos na quebra dos protocolos de segurança e privacidade das informações, Tecmundo (2012). Voltado para esta temática, pode ser identificado como um agente da ES, definido popularmente como engenheiro social. Do outro lado desta cadeia estão as vítimas, que podem ser entendidos como usuários de sistemas, redes sociais digitais, funcionários e clientes de empresas, etc.

Peixoto (2006) aborda o tema evidenciando as possibilidades de atuação dos agentes ativos dessa cadeia, dando destaque a nomes conhecidos da história, que ganharam fama através da aplicação de golpes de grandes proporções, que geraram prejuízos a diversas empresas e pessoas. O primeiro deles foi Frank Abgnale W. Jr, que teve sua história conhecida por meio do filme "*Catch me if you can*", título traduzido ao português como "Prenda-me se for capaz", estrelado por Leonardo Di Caprio em 2002. Frank ficou conhecido pela dimensão dos golpes aplicados, desde a

sua adolescência na década de 1960 nos EUA, quando figurou diversos personagens, nos mais variados ambientes, se passando por médico, advogado, piloto de aeronaves, professor, engajando saques e farsas por uma série de locais. Frank trouxe prejuízo somado de alguns milhões de dólares às suas vítimas, bancos e empresas, quando finalmente foi capturado por agentes do FBI – *Federal Bureau Investigation*, passando a integrar, anos mais tarde, a equipe de inteligência responsável pela detecção de golpes e fraudes bancárias, tendo em vista sua longa trajetória e vasta experiência na prática dessas atividades.

Outro popular engenheiro social citado é Kevin Mitnick, figura emblemática entre os *hackers* dos anos 1990, por sua grande habilidade em burlar sistemas de segurança. Kevin atuou desde o início da sua adolescência, na aplicação de pequenos golpes junto à companhia de transportes da sua cidade, com a falsificação de bilhetes rodoviários, que lhe permitiam viajar por diversos trajetos de forma gratuita. Com o tempo suas habilidades foram se tornando mais precisas e os golpes aplicados das mais diversas naturezas, como em companhias telefônicas, grandes corporações e até mesmo entidades do governo norte-americano. Após uma série de episódios de fraudes, finalmente Kevin foi detido pelo serviço de inteligência norte-americano e hoje atua frente a uma grande empresa de segurança da informação. Mitnick (2003) destaca a importância da observação do funcionamento dos mecanismos tanto das organizações, como das rotinas de indivíduos, na busca de falhas ou fragilidades dos sistemas, estes envolvendo tecnologias digitais ou não. O enfoque principal é de identificar o ponto mais fraco e atuar sobre este na busca da obtenção de informações mais valiosas, que possam então, proporcionar vantagens.

Outro caso notório e mais recente, retratado pelo documentário da *Netflix* (2022) – "*O Golpista do Tinder*", relata a história do cidadão israelense Simon Leviev e uma série de aplicação de golpes de estelionato, protagonizados por ele contra diversas vítimas pela Europa. Os dados históricos são narrados pelas próprias vítimas, confrontados por informações de seus perfis em redes sociais, como troca de mensagens, *e-mails*, transações bancárias, bem como mensagens de teor mais íntimo, no aplicativo de relacionamentos *Tinder.* Simon atraía suas vítimas através de um perfil exuberante, onde exibia fotos de muita ostentação financeira. Quando conseguia o interesse delas, passava então ao envio de mensagens, com convites inusitados para eventos restritos, em hotéis caros, carros de luxo, etc. Após obter sua confiança, passava então para a aplicação das extorsões, fundamentadas por histórias criadas por ele, que circundam ameaças e perseguições. Através do coletivo de denúncias impetradas pelas vítimas, Simon foi identificado e posteriormente detido, embora tenha sido libertado meses após o episódio.

Topolniak *et al* (2021) cita que a ES não é um mecanismo exclusivo dos meios digitais, porém a tecnologia propicia a disseminação das informações de maneira mais rápida e abrangente, a cada instante. Grandes empresas são detentoras de patrimônios informacionais de seus clientes, que variam de dados básicos de identificação até como de suas preferências, o que sem dúvidas, pode gerar diversos impactos pela sua exposição. Estando as ferramentas da ES há muito tempo em utilização por diversos indivíduos no mundo, atualmente com a ascensão das tecnologias digitais, tornou-se possível delimitar e descrever algumas destas, conforme Quadro 1, com o objetivo de instruir os cidadãos afim de torná-los mais conscientes na identificação da aplicação de possíveis golpes e da vulnerabilidade de suas informações.

Quadro 1 – Tipos de Engenharia Social:

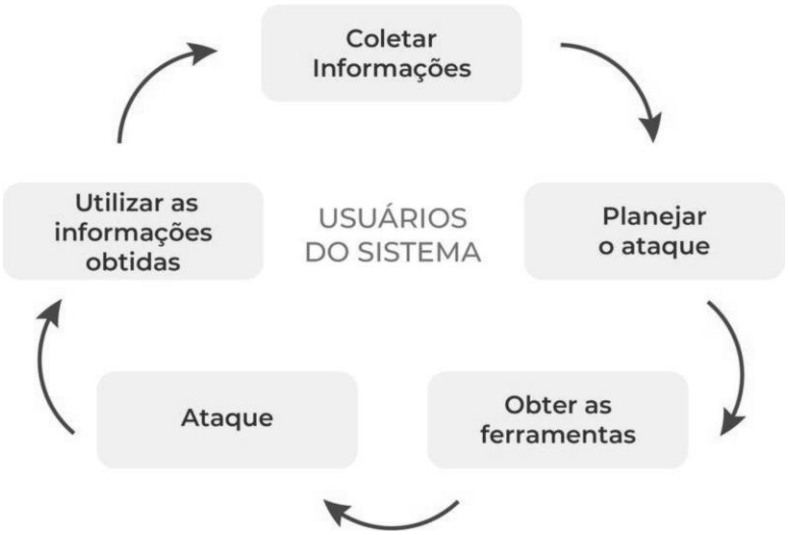
TIPOS	DESCRIÇÃO	AÇÕES	FERRAMENTAS	OBJETIVOS	ALVOS
DUMPSTER DIVING	Roubo de materiais descartados pelas vítimas, que possam conter informações de valor.	Vasculhar o lixo de pessoas ou empresas.	Lixeiras e descartes de materiais.	Obter dados pessoais da vítima ou da empresa a que está vinculada, para aplicação de outros golpes.	Pessoas Físicas, Empresas.
PHISHING	São encaminhados *links* falsos para o *e-mail* ou celular das vítimas, que direcionam para páginas *web* falsas, capazes de capturar os seus dados.	Endereços da *web* abreviados ou *links* errados, que direcionam para páginas falsas.	*E-mails* e *SMS*	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.	Ligações Telefônicas e *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 são instalados, em conjunto com programas baixados pela própria vítima.	*Download* de arquivos *e E-mails*.	Instalar *softwares* mal-intencionados nos dispositivos das vítimas, para roubo de dados pessoais.	Pessoas Físicas, Empresas.
SCAM	Envio de cartas 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* e *SMS*.	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 e 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.	*SMS*	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.	Ligações Telefônicas e *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 ou por 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.	Ligações Telefônicas.	Extorsão das vítimas através do medo.	Pessoas Físicas

Fonte: COMPUGRAF (2020).

De acordo com a análise do Quadro 1, se evidencia que o principal insumo para a ação dos agentes da ES é a informação, pois é através dela que os invasores poderão realizar suas atividades com maior precisão, estando cada vez mais próximos de suas vítimas. Essa relação sobre a necessidade da coleta de dados primários, para a realização de ações mais precisas, pode ser melhor entendida de acordo com a Figura 1.

Figura 1 – Ciclo da Engenharia Social



Fonte: COMPUGRAF (2020)

2.3 – Lei de Proteção de Dados:

Tendo em vista o aprimoramento das ferramentas tecnológicas digitais, nasceu então a preocupação com as informações que trafegam de maneira instantânea por esses meios. Desde o início das civilizações aos dias atuais, o valor dos dados pode estar representado pela capacidade de gerar informações/conhecimento e executar ações, que esse conjunto permitirá. Oliveira (2019) entende que esse ativo é imprescindível para o ideal funcionamento das organizações, sendo esse destaque necessário para fundamentar a importância desse bem e de sua salvaguarda. Rohling (2014) define a etimologia da palavra lei oriunda do latim “lex”, do verbo “legere” ou “lectum”, que pode ser compreendido como um sistema de regras que permeiam o ambiente social e seus agentes. Pereira (2010) cita que o meio social desenvolve as suas relações e, através destas é que podem ser concebidos as normativas, que permeiam essas relações, sendo as leis como um manual de regras sociais.

No ano de 2016 foi formalizado na União Europeia o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation – GDPR*), oriundo da atualização da diretiva de proteção de dados pessoais concebida em 1995 pela então comunidade europeia, que por sua vez foi representava um compilado de regulamentações relativas à proteção de dados, estabelecidas em diversos países do continente europeu, desde meados da década de 1970. Essa atualização surgiu pela necessidade de englobar os meios digitais utilizados na comunicação entre usuários, conectados à grande rede mundial.

Freitas (2021) define esse instrumento como um dos mais abrangentes de sua série, por elencar questões conceituais e bases de definições que permeiam todo o universo digital, atribuindo os devidos direitos e deveres, tanto dos usuários como dos agentes tratadores de dados. Suas regulações enfatizam o direito à privacidade do cidadão europeu, os quais devem possuir ciência sobre o tratamento e armazenamento de suas informações pessoais, podendo até mesmo se opor, a qualquer momento sobre essas atividades. Também há previsão para requisição de histórico sobre o tratamento de dados, importação de relatórios e solicitação de exclusão parcial e total das suas informações, contidas nos bancos de dados de

terceiros. Em sua estrutura regula uma série de definições, como a de “dados pessoais”, que podem ser entendidos como informações que permitem identificar um cidadão.

O termo “processamento” é utilizado para definir o ato de comercializar informações dos usuários, o que é proibido. Há previsão legal para a transferência de dados, desde que esta ocorra somente dentro do espaço econômico europeu. Há também previsão legal que visa punição às empresas que tenham seus bancos de dados violados e informações expostas, casos conhecidos como vazamentos de dados, NetApp (2021). Muitas normativas acerca da proteção de dados pessoais foram instituídas ou mesmo receberam atualizações, impulsionadas por meio da *GDPR*, pelo mundo todo.

A exemplo dessa regulação se baseia a *CCPA – California Consumer Privacy Act,* normativa de proteção de dados do Estado da Califórnia, nos EUA; A *POPIA – Protection of Personal Information Act*, na África do Sul; o *APPI – Act on the Protection Of Personal Information*, no Japão; A LPDP - Ley de Proteción de los Datos Personales, na Argentina; A *PIPL – Personal Information Protection Law*, na China; A LGPDP – *Ley General de Protección de Datos Personales*, no México, o PA – Privacy Act, na Nova Zelândia, etc.

No Brasil como nos demais países, regulamentações que visam defender um dos princípios já previstos anteriormente na Constituição Federal de 1988, relativo ao direito à privacidade e inviolabilidade da intimidade dos indivíduos, foram sendo instituídas e aprimoradas. Em 2011 foi sancionada a Lei 12.527, intitulada “Lei de Acesso à Informação”, que trata de viabilizar ao cidadão o direito de acesso à informação pública, propondo maior transparência e controle das ações do poder público. Esse instrumento diferencia principalmente o que é um dado público de um dado sigiloso, sendo o primeiro de acesso irrestrito à população e o outro, aquele que possa expor a segurança dos indivíduos ou instituições, Câmara (2022).

Em 2012, por pressão pública e grande repercussão midiática foi sancionada a lei 12.737, que ficou popularmente conhecida como “Lei Carolina Dieckmann”, título que faz referência à atriz, que protagonizou em sua vida real um conhecido episódio de violação de privacidade. Invasores quebraram os protocolos de segurança do computador pessoal da atriz, e obtiveram acesso a imagens da mesma em situação íntima, as quais foram divulgadas em perfis falsos em redes sociais, gerando grande polêmica e indignação pública sobre o assunto.

Nesse instrumento legal foram revisadas previsões já citadas no código penal brasileiro, definindo então normativas especificas para os crimes cometidos em meios cibernéticos. A lei também cita invasão de dispositivos digitais, interrupção, bloqueios ou imposição de dificuldades em serviços públicos de informação, uso indevido de cartões de crédito e débito ou mesmo de documentos pessoais de terceiros sem autorização, FMP (2021).

A Lei 12.965/14, conhecida como “Marco Civil da Internet”, tida como um presente aos brasileiros, citada por Leite (2014), foi a instituição de normativas específicas no âmbito digital. Suas previsões visam dar enfoque a liberdade de expressão, comunicação e manifestação do pensamento. A normativa propõe a mediação das relações nos ambientes virtuais, com objetivo de organizar este espaço, com definições dos direitos e deveres dos personagens atuantes nesse meio. Uma de suas principais garantias é do direito ao acesso à internet pelos cidadãos, como pleno exercício de sua cidadania, Gonçalves (2016). O direito ao anonimato visa a proteção da imagem e segurança dos indivíduos, tendo seus dados mantidos em sigilo, salvo por ordem judicial.

Então em 2018, A Lei Geral de Proteção de Dados Pessoais – LGPD foi sancionada no Brasil, fundamentada pela garantia do direito à privacidade dos cidadãos. NetApp (2021) cita que como as demais legislações para proteção de dados, identifica como “dado pessoal” a mesma definição trazida pela *GDPR*, com ramificações para os “dados sensíveis” que são aqueles que permitem identificar uma preferência do indivíduo, que possa estar relacionada à sua opinião política, crença religiosa ou filosófica, grupo ou etnia ao qual se identifica, gênero, associação partidária, etc. Esses dados tidos como sensíveis, são assim nomeados pois o seu mau uso pode trazer um grau de risco elevado à segurança do indivíduo, pela exposição. Suas prerrogativas visam enaltecer princípios constitucionais anteriormente estabelecidos, que em meio a era digital já se encontravam desfocados, como o direito à titularidade dos dados aos cidadãos.

As empresas e instituições públicas que realizam coleta, processamento e armazenamento de dados dos indivíduos são conhecidos como tratadores e tem o papel de resguardo desse bem, com a devida segurança. Para toda e qualquer coleta de informações, é necessário informar ao cidadão a sua necessidade, bem como solicitar o seu consentimento para fazê-lo. Nos termos da lei, as empresas precisam possuir políticas de segurança da informação sempre atualizadas e se manter atentas às vulnerabilidades sistêmicas, que possam gerar quaisquer tipos de invasão. Uma vez expostos os dados, seus titulares devem ser notificados quanto aos episódios e os tratadores precisam trabalhar para mitigação dos riscos gerados, sob o prenúncio de ter seus bancos de dados bloqueados, por tal descumprimento. Segundo a LGPD (2018) em seu art. 6º, o tratamento de dados deve ser norteado pelas suas finalidades, ou seja, a coleta deve ser restrita à necessidade informacional, para cada situação específica, sendo justificada a necessidade de obtenção de recursos maiores, de acordo com a atividade/serviço prestado.

O enfoque do consentimento do titular sobre o tratamento dado às suas informações pessoais é previsto no art. 7º, bem como da possibilidade de solicitar a exclusão destas, após o seu uso, do registro das empresas. Há previsão da instituição de autoridade nacional de proteção de dados – ANPD, no art. 48º, que visa mediar como agente controlador as atividades de tratamento de dados no país. No mesmo artigo está previsto a necessidade de comunicar a ANPD sobre os episódios de vazamentos, por parte dos tratadores, bem como da geração de relatórios sobre os possíveis impactos gerados aos titulares.

3 – Procedimentos Metodológicos

Para concepção do presente estudo, foi necessária a adoção dos métodos comuns às pesquisas científicas de cunho de investigação teórica, com base em revisão bibliográfica e documental:

I – Foi feito levantamento bibliográfico dos principais conceitos teóricos que fundamentam a pesquisa, tendo em vista a expressar as ideias mais atuais e aprimoradas dessas definições, enfatizando temas que a delineiam.

II – Também foi realizada pesquisa documental, nos principais marcos legais descritos, relativos à proteção de dados pessoais, objetivando evidenciar suas bases, bem como verificar a similaridades entre estes.

III - Outra pesquisa e análise documental foi realizada através de busca livre, sem delimitação de tempo ou espaço, em sites da web, blogs, jornais e revistas, que noticiaram episódios de vazamentos de dados de usuários, oriundos de diversas empresas, buscando evidenciar a dificuldade de se expressar esse aspecto sensível

das organizações, pois demanda exposição de suas fragilidades e que pode gerar impactos comerciais.
IV – Foram utilizados os dados estatísticos compilados pelos portais *GET – GDPR Enforcement Tracker* e da ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados, sobre as sanções já impostas às empresas após homologação da *GDPR*, na União Europeia e da LGPD no Brasil, respectivamente, com vistas a traçar um paralelo e comparação da prática dos regulamentos.

4 – Análise dos Resultados

Da pré-história à atualidade, o conceito do valor da informação teve seu destaque baseado no entendimento do que se pode obter com a posse dos dados. As informações que antigamente eram registradas de formas primitivas, como pinturas em paredes de cavernas, passando a pergaminhos, papéis, livros, chegaram aos registros em meios digitais e eletrônicos. Desde então, o fluxo informacional tem crescido de maneira exponencial, devendo-se ao fato da otimização da sua forma de registro. A informação pode ser processada, na forma de dados, gerando conhecimento, de acordo com os sistemas em que se inserem. O volume de dados existentes, requer tecnologias cada vez mais aprimoradas para seu devido processamento, necessitando também de inteligência capaz de estabelecer esse dimensionamento e protocolos otimizados.

As ferramentas de segurança da informação visam a geração de um ambiente de risco reduzido à navegação dos usuários, integrando dados de uma ponta a outra, disponibilizando os mesmos apenas aos agentes autorizados nesse meio. A arquitetura organizacional no âmbito da informação visa estabelecer boas práticas para os métodos de gestão de dados, com devido planejamento de ações, para redução de erros e riscos, nas etapas de processamento de informações.

A vulnerabilidade das informações de usuários há muito tempo se mostra como um risco à segurança de seus titulares, o que pode gerar uma série de impactos sociais, econômicos e financeiros. Os agentes que atuam na busca desse produto, muitas vezes “vazado”, ou mesmo rompem os obstáculos impostos pelos protocolos de segurança que permeiam os SI, para seu alcance, o fazem com o propósito de penetrar barreiras, físicas ou digitais, para obtenção de vantagens. Na história, muitos Engenheiros Sociais foram conhecidos por golpes aplicados, de formas diversas, o que se tornou mais evidente na era digital a qual vivenciados, pela possibilidade de acesso a um coletivo de dados cada vez maior e mais preciso.

A busca incessante pelas informações de usuários deixa algumas marcas na história de pessoas e empresas, estando estas preocupadas com a ocultação dessas informações, para preservar sua imagem, contratos comerciais, etc. São estabelecidos no Quadro 2 alguns episódios noticiados, dos casos de vazamentos de dados, que evidenciam essa preocupante situação.

De acordo com os dados, a maior parte dos casos remetem a empresas dos EUA e Brasil, não tendo sido sancionadas a condenações legais em sua maioria, por se tratarem de períodos que antecedem a instituição das normativas de proteção de dados, nos respectivos países. Há relevância no que diz respeito ao volume de dados vazados, observado pelo número de titulares envolvidos, que às vezes chega a um número próximo ao total da população do país, como no caso da empresa Serasa Experian, noticiado pela Carta Capital em 2020, que incluiu dados até mesmo de titulares já falecidos. Essas informações contemplam desde nomes completos e números de documentos cadastrais, como CPF, RG, CNH, até dados mais sensíveis como *scores* de crédito, negativações, dívidas, limites bancários, etc. A luz da LGPD

muitos desses casos estariam enquadrados como descumprimentos ao § 7º, Seção I – Das Sanções Administrativas, que prevê penalização pelo vazamento de dados.

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 o 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.			
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, bilhões
	G1 GLOBO	Estava envolvida a empresa *Cambridge Analytica*, que coletava e tratava dados do *Facebook*, a qual compartilhou indevidamente esses dados para manipular eleitores e influenciar a vitória de *Donald Trump* no governo dos EUA.			
UBER	2016	2018	EUA	57.000.000	US$ 148 milhões
	TECNOBLOG	A empresa sofreu um ciber ataque, que resultou na exposição de dados de seus usuários, como endereços de *e-mail*, número de celular, dados dos motoristas, como documentos de habilitação, etc.			
BANCO INTER	2017	2018	BR	19.000	R$ 1,5 milhões
	TECNOBLOG	Por mais de um ano estiveram expostos os dados cadastrais dos correntistas.			
NETSHOES	2018	2019	BR	2.000.000	R$ 500 mil
	G1 GLOBO	Vazamento de dados pessoais, de clientes cadastrados na plataforma de compras online, como CPF, data de nascimento, *e-mail*, histórico de compras, etc.			
C&A	2018	-	BR	2.000.000	0,00
	TECMUNDO	Através de invasão do sistema de geração de "cartões presente", comercializados pela empresa, *crackers* conseguiram ter acesso aos dados cadastrais dos usuários.			
GOOGLE	2018	2019	EUA	500.000	US$ 7,5 milhões
	TECNOBLOG	Empresa indenizou usuários, que tiveram seus dados de cadastro vazados, através da extinta rede social *Google*+.			
BRITSH AIRWAYS	2019	-	UK	500.000	£$ 183,39 milhões
	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.			

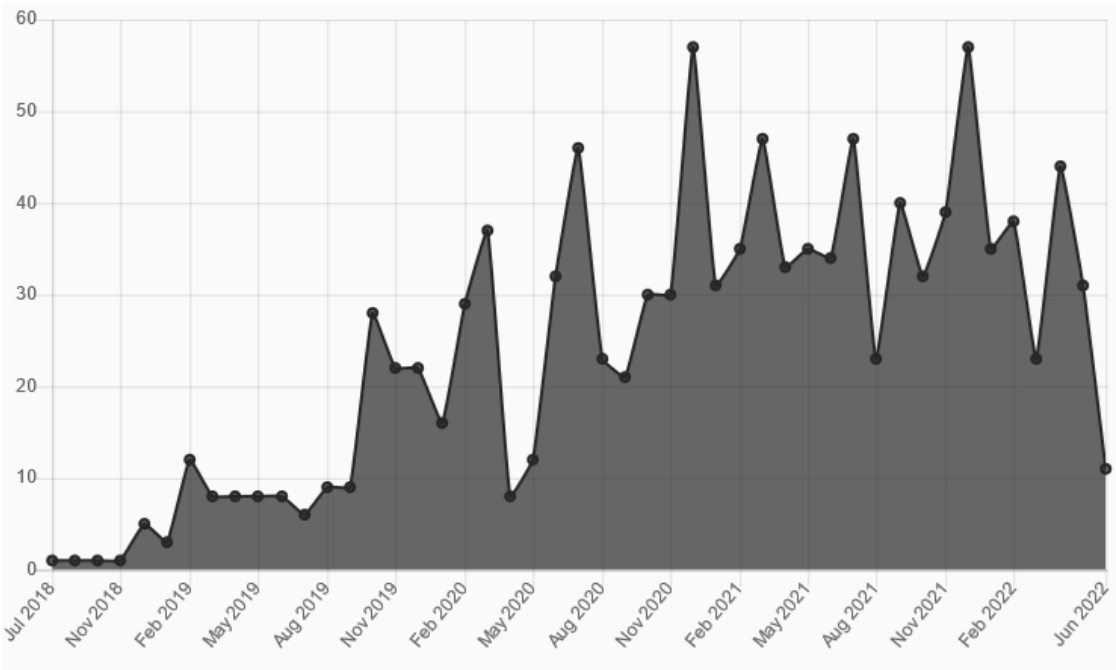
CLARO E VIVO	2019	2021	BR	2	R$ 20 mil
	CONVERGÊNCIA DIGITAL	Empresas de telefonia móvel foram condenadas a indenizar consumidores, cujos dados vazados resultaram no bloqueio de uso dos seus aparelhos celulares.			
BC CORP	2019	-	BR	Não divulgado	0,00
	THE HACK	Administradora de empresas especializadas 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 cópias de documentos pessoais.			
TWITTER	2019	-	BR	Não divulgado	0,00
	EXAME	Uma falha sistêmica expôs postagens marcadas como privadas, tornando-as 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 cadastros, pessoas físicas e jurídicas, sendo um dos maiores episódios na história, em número de usuários afetados. Além de dados de nº do 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.			
	2021	-	EUA	3.300.000	0,00

VOLKSWAGEN	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 tiveram seus dados vazados, após os servidores da empresa sofrerem ataques de invasores.			

Fontes: citações no quadro.

Realizando análise ao portal *GET – GDPR Enforcement Tracker,* uma plataforma virtual que documenta os casos de sanções já aplicadas, baseadas nas imposições legais da *GDPR* (Figura 2). Seu enfoque está em relatar aos usuários os impactos financeiros sofridos por empresas, pelo descumprimento das normativas, informando seu volume, agrupado por períodos mensais, ramos de atividade, entre outros.

Figura 2 – Número de multas mensais aplicadas através da GPDR (não cumulativo)

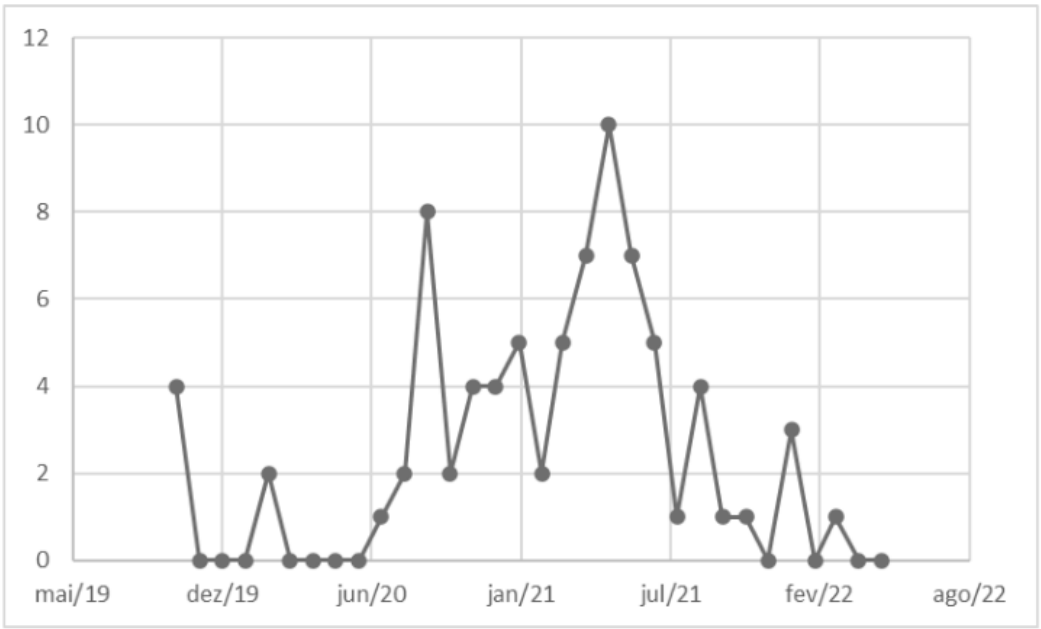


Fonte: *GDPR Enforcement Tracker* (2022).

Já foram registrados mais de 1.100 casos de julho de 2018 até o período atual, com perspectiva crescente das estatísticas apresentadas, tanto com relação ao número de multas, de uma média de cinco casos mensais no primeiro ano observado, para 33 nos últimos doze meses, também com relação ao valor que variou de uma média de € 4.4 milhões para € 54 milhões nos períodos respectivos.

No cenário brasileiro, não muito diferente do europeu, os dados agrupados pelo portal ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados, expressos na Figura 3, passam por uma perspectiva crescente, embora o pouco número de casos relatados, por se tratar da recente homologação da LGPD e da previsão da aplicação de multas. Dos quase 100 casos relatados, mais da metade tiveram sanções de multas, no somatório de cerca de R$ 2,7 milhões de reais. O maior número de descumprimentos refere-se ao art. 7º da lei, que abrange a regulamentação do tratamento de dados. Muitos descumprimentos são por parte de empresas da área financeira e bancos, com destaque para ocorrência de episódios de vazamentos não notificados à autoridade responsável, o que pode acarretar em fraudes bancárias, que geram prejuízos financeiros aos indivíduos, instituições e empresas.

Figura 3 – Número de multas mensais aplicadas através da LGPD (não cumulativo)



Fonte: ANPPD (2022).

5 – Considerações Finais

Para manutenção do direito constitucional, da privacidade e inviolabilidade da vida íntima dos cidadãos, foram estabelecidos uma série de instrumentos legais e seus detalhamentos que reforçam essas garantias. O principal objetivo do levantamento dessas normativas refere-se à atualização de suas regulamentações, de acordo com a transformação da realidade social, através da evolução que a tecnologia vem sofrendo com o passar dos anos. O fluxo de dados estando vulnerável a um invasor mal-intencionado, requer atenção dos responsáveis pela salvaguarda dessas informações, previsão legal instituída pelos marcos de proteção de dados.

A LGPD e demais instrumentos legais expressam a necessidade de se estabelecer critérios, cada vez mais detalhados, sobre as posturas éticas as quais as empresas e instituições precisam se ater, para com seus clientes e usuários, uma vez

que é comum a prática da comercialização informal de dados, que pode gerar sérios impactos a esses indivíduos. A Engenharia Social, independentemente da existência de medidas legais, consegue se alinhar à realidade estabelecida, buscando fragilidades dos mecanismos de defesa e proteção da privacidade, objetivando romper essas barreiras e alcançar o produto informacional, primordial para suas ações.

É possível então inferir que a principal contribuição da Lei Geral de Proteção de Dados Pessoais para mitigar os efeitos da engenharia social está associada à restrição quanto ao uso, comercialização, processamento e tratamento de dados dos cidadãos, uma vez que se regulam esses processos, se estabelecem medidas preventivas e ações punitivas de sanção ao seu descumprimento, as empresas e instituições passam a ter maior responsabilidade e zelo sobre esses processos, pelos possíveis impactos financeiros e comerciais a serem gerados.

Referências

AGRA, Andressa. D.; BARBOZA, Fabrício; Felipe. M. ***Segurança de Sistemas da Informação*** Editora Grupo A, 2019.

ANPPD – ***Associação Nacional dos Profissionais de Privacidade de Dados*** – Disponível em: < https://anppd.org/ > Acesso em 18/06/2022.

AUDY, Jorge Luis Nicolas; ANDRADE, Gilberto Keller.; CIDRAL, Alexandre **Fundamentos de Sistemas de Informação –** Editora Bookman, 2007.

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

BARBOSA, Ricardo Rodrigues ***Gestão Da Informação E Do Conhecimento: Origens, Polêmicas e Perspectivas*** *– Editora INF – Londrina, 2008.*

BARRETO, Jeanine dos Santos; ZANIN, Aline; MORAIS, Izabelly Soares; VETTORAZZO, Adriana ***Fundamentos de Segurança da Informação*** – Editora Grupo A, 2018.

BRASIL – ***Constituição Federal*** – Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/consti tuicao.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.

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.

CHOO, Chun Wei ***A Organização Do Conhecimento*** – Editora Senac, São Paulo, 2003.

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.

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.

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.

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.

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.

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 18/06/2022.

GONÇALVES, Victor Hugo P. ***Marco Civil da Internet Comentado*** – Editora Grupo GEN, 2016

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.

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.

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.

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.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George ***Hackers Expostos***. Editora Grupo A, 2014.

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.

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

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.

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, Bryan Felipe; PINTO, José Simão de Paula – ***LGPD, Privacidade e seus Impactos nos Prcessos de Engenharia Social*** – Disponível em: < https://acervodigital.ufpr.br/bitstream/handle/1884/76045/R%20-%20D%20-%20BRYAN%20FELIPE%20DE%20OLIVEIRA.pdf?sequence=1&isAllowed=y > Acesso em 01/06/2022.

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.

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

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

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.

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.

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

SERRA, João Paulo ***Manual de Teoria da Comunicação*** – Editora Covilhã: Livros Labcom, 2007.

SOUZA, Queila R; QUANDT, Carlos O ***Metodologia de Análise de Redes Sociais*** – Editora Perspectiva São Paulo, 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 – ***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.

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.

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 ***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.

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.

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.

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.