UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE CIÊNCIA DA COMPUTAÇÃO

DIEGO BARBOZA DE MEDEIROS

A proteção de dados nas redes sociais em tempos de pandemia: uma revisão de literatura

PATOS-PB

2022

DIEGO BARBOZA DE MEDEIROS

A proteção de dados nas redes sociais em tempos de pandemia: uma revisão de literatura

Trabalho de Conclusão de curso 2 apresentado ao Programa de Graduação em Bacharel em Ciência da Computação da Universidade Estadual da Paraíba.

Área de concentração: Redes de computadores

Orientador: MSc. Ingrid Morgane Medeiros de Lucena

PATOS-PB

2022

M488p Medeiros, Diego Barboza de.

A proteção de dados nas redes sociais em tempos de pandemia [manuscrito] : uma revisão de literatura / Diego Barboza de Medeiros. - 2022.

42 p. : il. colorido.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas , 2022.

"Orientação : Profa. Ma. Ingrid Morgane Medeiros de Lucena , Coordenação do Curso de Computação - CCEA."

1. Redes sociais. 2. Proteção de dados. 3. Internet - Segurança. 4. Pandemia da covid-19. I. Título

21. ed. CDD 004.678

Elaborada por Edson M. Almeida - CRB - CRB 15/743 BSC7/UEPB

DIEGO BARBOZA DE MEDEIROS

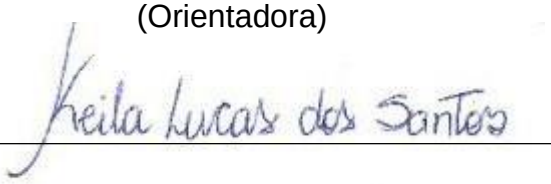
A proteção de dados nas redes sociais em tempos de pandemia: uma revisão de literatura

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Ciência da Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado em 03 de agosto de 2022

BANCA EXAMINADORA

Profª Me Ingrid Morgane Medeiros de Lucena
(Orientadora)



Profª Me Keila Lucas dos Santos
(Examinadora)

Profº Me Ferdinando de Oliveira Figueirêdo
(Examinador)

Dedico esse trabalho a Deus, pela força e coragem, e aos meus familiares por todo apoio e ajuda, e que contribuíram para a realização dessa conquista.

AGRADECIMENTOS

Em primeiro lugar, a Deus, que me proporcionou muita saúde, força, coragem, e fez com que meus objetivos fossem alcançados, durante todo esse período de estudos. Gostaria de agradecer ainda, aos meus pais/irmãs e familiares Doralice Barboza da Cruz Medeiros, João Batista de Medeiros, Luana Barboza de Medeiros, Mariana Barboza de Medeiros e Elane Garcia de Medeiros, por todo o apoio e pela ajuda, que muito contribuíram para a realização deste trabalho.

Agradeço, também, aos amigos, João Victor Souza Marques de Lira, Lincoln Rangel Nóbrega e Dennys Alves Angelim, que sempre estiveram ao meu lado, pela amizade incondicional e pelo apoio demonstrado durante todo esse período de tempo em que me dediquei na realização, não só desse trabalho, mas também em todos os momentos que contribuíram para a minha formação como pessoa.

À Mestre Ingrid Morgane Medeiros de Lucena, por ter sido minha orientadora e ter desempenhado tal função com dedicação e amizade. Gostaria de agradecer também, de forma geral aos professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso.

E, por fim, a todos que participaram de alguma forma, seja ela direta ou indiretamente, do meu desenvolvimento ao longo desses anos de curso, o que enriqueceram o meu processo de aprendizado, e que me incentivaram e certamente tiveram impacto na minha formação acadêmica.

O sucesso é a soma de pequenos esforços repetidos dia após dia.

(Robert Collier)

RESUMO

Com o início da pandemia, e consequentemente o isolamento social, as pessoas foram condicionadas a passar mais tempo em casa. Com isso, aumentou-se o número de procura à internet pelas ferramentas de entretenimento. A rede social é uma delas. Atrelado a isso, aumentaram-se os riscos de segurança digital para os usuários. Assim, este trabalho tem como objetivo geral identificar meios eficazes para manter a privacidade e a proteção dos dados das redes sociais durante a pandemia da COVID-19. Para isso, buscou-se respaldo teórico nas produções científicas de alguns autores, a exemplo de Miranda (2018), Monteiro (2020), Barbosa (2021), Brandão (2021), entre outros. Trata-se de uma pesquisa integrativa de revisão de literatura, caracterizada como método de sintetizar estudos anteriores da temática abordada neste trabalho, o que permite fazer uma análise de forma ordenada para um maior aprofundamento do tema. Esse trabalho se torna necessário para alertar as pessoas o quanto é perigoso uma exposição exacerbada em suas redes sociais, o que pode resultar em golpes virtuais que trarão sérias consequências para quem usa e as pessoas mais próximas.

Palavras-Chaves: Rede Social, Proteção dos Dados, Internet - Segurança, Pandemia da covid-19.

ABSTRACT

With the beginning of the pandemic, and consequently social isolation, people were conditioned to spend more time at home. As a result, the number of internet searches for entertainment tools has increased. The social network is one of them. Linked to this, digital security risks for users have increased. Thus, this work has the general objective of identifying effective ways to maintain privacy and data protection on social networks during the COVID-19 pandemic. For this, theoretical support was sought in the scientific productions of some authors, such as Miranda (2018), Monteiro (2020), Barbosa (2021), Brandão (2021), among others. This is an integrative literature review research, characterized as a method of synthesizing previous studies on the topic addressed in this work, which allows an orderly analysis to be carried out in order to deepen the topic. This work becomes necessary to warn people how dangerous an exacerbated exposure on their social networks is, which can result in virtual scams that will have serious consequences for those who use it and the people closest to them.

Keywords: Social Network, Data Protection, Internet - Security, Covid-19 Pandemic.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1. Introdução

Com o início da pandemia causada por um novo agente do Coronavírus (SARS-CoV-2), declarada em março de 2020 pela Organização Mundial de Saúde (OMS), e futuramente chamada de pandemia da COVID-19[1], as autoridades do mundo todo passaram a buscar medidas sanitárias para conter a dissipação do vírus, que avançava significativamente por diversos países, o que sobrecarregou os Sistemas de Saúde (HENRIQUES; PESSANHA; VASCONCELOS, 2020).

Desse modo, além dos cuidados de higiene das mãos, dos alimentos e uso de máscara, uma das medidas mais eficazes, encontrada em um primeiro momento, foi o isolamento social. Assim, as pessoas passaram a trabalhar, estudar e resolver suas demandas diárias em seu próprio lar. Se, antes, algumas pessoas acessavam exageradamente à *internet*, com a chegada da pandemia, esse acesso aumentou, pois, além de todas as necessidades já mencionadas, outras ferramentas digitais, como aplicativos de *Delivery* e entretenimento, se tornaram comuns no cotidiano da humanidade (COELHO, 2020).

Sobre a era digital, onde a maioria das pessoas tem acesso às tecnologias, as ferramentas tecnológicas se tornam essenciais no dia a dia, ainda mais no período da pandemia. Isso gera uma certa comodidade no homem, pelo fato de resolver diversas tarefas com um simples toque, através dos *smartphone* (CAVALCANTI, 2021). Nesse meio tecnológico, as redes sociais adquirem espaço como uma forma de entretenimento e também de empreendimento. Diversos usuários se transformam em grandes influenciadores, pelo simples fato de mostrar cada passo de suas vidas, no estilo *"reality show"*. Gravação de *stories,* publicações em *feeds, podcasts*, mensagens e ligações em tempo real por aplicativos de mensagens, por exemplo, são maneiras de como a sociedade avança continuamente ao tempo em que a tecnologia também progride e ambas se adaptam a esse progresso (SOUZA *et al.,* 2021).

[1] COVID-19: "Inicialmente chamada de 2019-n-CoV, a infecção provocada pelo novo coronavírus (o Sars-Cov-2) recebeu o nome oficial de COVID-19, em 11 de fevereiro de 2020: Significa "doença por coronavírus" em inglês" (FIOCRUZ, 2022).

Nessa perspectiva, através de tantos acessos e uso contínuo da rede mundial de computadores, o tráfego de dados aumentou, de modo que foram necessárias medidas de proteção dessas redes, com a manutenção da privacidade dos usuários (RODRIGUES, 2021).

Portanto, visto o aumento no número de tráfego de dados, assim como a demanda das pessoas nesse período pandêmico, faz-se necessário que a segurança dessas redes seja reorganizada ao ponto em que se aperfeiçoa para garantir a privacidade de acesso aos que utilizam essa ferramenta tecnológica (BARBOSA, 2021).

Assim, essa pesquisa pretende responder às seguintes questões:

- Como a proteção de dados se torna algo relevante para o cotidiano, sobretudo em tempos de pandemia?
- De que maneira a Lei Geral de Proteção de Dados influenciou na utilização dos dados nos meios digitais, em especial na pandemia do COVID-19?
- Como aplicar boas práticas de segurança para manusear as ferramentas que a era digital proporciona?

1.1. Objetivos

1.1.1. Objetivo geral

Identificar meios eficazes para manter a privacidade e a proteção dos dados das redes sociais durante a pandemia da COVID-19.

1.1.2. Objetivos específicos

- Pesquisar o contexto histórico da Quarta Revolução Industrial e seus efeitos para a criação da lei de proteção de dados no Brasil;
- Descrever os principais riscos encontrados na *internet,* bem como as boas práticas para a privacidade e proteção dos dados na rede;
- Registrar as redes sociais mais utilizadas durante a pandemia e as vulnerabilidades para uma invasão *cibernética.*

1.2. Justificativa

Com o início da pandemia, e consequentemente do isolamento social, as pessoas foram condicionadas a passar mais tempo em casa, devido ao avanço da infecção do novo coronavírus. Com isso, aumentou-se a procura à internet para uso de ferramentas de entretenimento, especialmente as redes sociais. Neste sentido, buscar a proteção dos dados de acesso a esses *softwares* é essencial para garantir maior tranquilidade de navegação na rede (RODRIGUES, 2021).

Assim, nota-se que ao passo em que a tecnologia transformasse o armazenamento e o processamento de dados pessoais em algo possível, a proteção da privacidade associou-se à própria proteção de dados pessoais, ou seja, a conservação e o tratamento dos dados pessoais devem ocorrer tanto nos meios digitais, quanto nos ambientes físicos (BASAN, 2021).

A segurança das redes sociais, ainda, enfrenta dificuldades no que diz respeito às legislações. Isso se dá porque a disseminação de informações se propaga em uma velocidade muito maior do que os processos jurídicos. Dessa forma, discorrer sobre a importância da privacidade e segurança na *internet* reafirma a urgente necessidade de uma prestação de serviço com eficácia para acesso à rede (BARBOSA, 2021).

A importância desse trabalho está atrelada ao fato de que muitas pessoas ainda não sabem como proteger suas redes sociais, ao ponto de estarem vulneráveis a *hackers* e outras pessoas mal-intencionadas que podem trazer grandes prejuízos, não só financeiros, mas também morais e psicológicos a suas vítimas.

Desse modo, essa proposta pretende esclarecer, para os usuários das redes sociais, os principais riscos de vulnerabilidade nos programas, bem como as boas práticas de fácil acesso para garantir a proteção de dados e privacidade ao utilizar as ferramentas tecnológicas, sobretudo aquelas em que possuem as informações pessoais.

2. Fundamentação Teórica

Neste capítulo, serão abordadas as seguintes temáticas: A história da Quarta Revolução Industrial e seus efeitos para a proteção de dados no Brasil, com a amostra da sua evolução ao longo dos anos; as boas práticas para o uso correto das redes sociais, bem como os riscos que essa rede traz; e as redes sociais mais utilizadas durante a pandemia da COVID-19 e suas vulnerabilidades para ataques cibernéticos.

2.1. Os processos de transições das Revoluções Industriais ao longo dos anos

Diante das constantes transformações ao longo dos anos, o período de 1760 a 1840 foi marcado pela Revolução Industrial, com início estabelecido pela transição para novos processos de manufatura, que envolviam outros métodos para produção de ferro, energia, produtos artesanais e máquinas, e que se torna um dos principais períodos da história da humanidade (CONTREIRAS, 2015).

Sem uma ruptura da primeira, surge a Segunda Revolução Industrial. Esse período, iniciado em 1850 e estendido até 1870, sob o olhar sócio tecnológico, trata-se de um aprimoramento das técnicas já criadas durante o período da Primeira Revolução Industrial. Nessa revolução, evidenciou-se a produção de aço da *Siemens* como o forno *Siemens-Martin* e do processo de *Bessemer*, – segundo Costa *et al.* (2007), esse método consiste em utilizar o ar para oxidar os materiais do ferro-gusa, para, assim, resultar no aço – ao tempo em que os custos da produção de aço foram reduzidos, o que aumentou a utilização pelos transportes rápidos, visto que, nessa época, a utilização de linhas de ferro e navios a vapor se tornou mais frequente (CONTREIRAS, 2015).

Por volta de 1940, surge a Terceira Revolução Industrial, também chamada de Revolução Técnico-Científica. Essa era foi marcada pelo uso de tecnologias no setor de sistema de produção industrial. Dentre os principais avanços desse período estão a robótica, a genética, a biotecnologia, entre outros. Essa revolução é marcada pela integração entre Ciência, Tecnologia e Produção. Além disso, essa era trouxe a utilização de recursos de informática nas produções, a globalização e a utilização de várias fontes de energia, a exemplo da eólica, nuclear e hidrelétrica (CONTREIRAS, 2015).

2.1.1. A Quarta Revolução Industrial: Os efeitos para a proteção de dados no Brasil

Nessa revolução, o foco não está apenas nos sistemas e nas máquinas inteligentes. Trata-se de novas descobertas simultâneas que envolvem o sequenciamento genético, a nanotecnologia, as energias renováveis, a computação quântica, entre outros. A Quarta Revolução Industrial se difere das anteriores pelo fato de integrar os aspectos físicos, digitais e biológicos com a fusão das tecnologias (SCHWAB, 2016).

A criação de *softwares* e máquinas inteligentes, a exemplo da: Inteligência Artificial e Robótica; a *Internet das Coisas*; Direção autônoma; Redes 5G; *Quantum* e Computação em Nuvem; Biotecnologia, *Deep Learning* e *Big Data*; Realidade Aumentada e Realidade Virtual. Os novos sistemas de geração e armazenamento de energia, partiram da Quarta Revolução Industrial (2011-atualmente) com caráter global para ampliar os recursos da *internet*. Trata-se da utilização de sensores menores, mais poderosos e com preços mais acessíveis (SCHWAB, 2016).

Dessa forma, a Quarta Revolução Industrial se destaca pela evolução da velocidade, a amplitude e a profundidade. Além disso, os programas passaram a se transformar nas organizações e indústrias (XU *et al.,* 2018).

Nos dias atuais, essa revolução se faz presente e obtém espaço no cotidiano das pessoas através da utilização de várias ferramentas tecnológicas, como, por exemplo, a *Internet das Coisas*, a realidade virtual e a impressão 3D e 4D. Nessa perspectiva, Cavazzini *et al.,* (2018) enfatiza que, a partir da Tecnologia da Informação, é que foi possível implementar a *Internet of Things* (IoT), a chamada *Internet das Coisas*.

A *Internet das Coisas* se trata de uma extensão da *internet* atual, que possibilita que objetos do dia a dia, com capacidade computacional e de comunicação, possam ser conectados à internet (SANTOS, 2016). Assim, o objetivo é que o *modus operandi* tenha uma maior flexibilidade, eficiência e sustentabilidade, e que pode elevar os padrões de qualidade e reduzir os custos.

Nesse sentido, com o desenvolvimento da tecnologia, fez-se necessário reforçar a importância em proteger os dados eletrônicos. As primeiras orientações a esse respeito surgiram a partir do processamento de

organizações, sejam elas privadas ou não, sobretudo no que diz respeito aos grandes bancos de dinheiro que utilizam uma maior quantidade de informações pessoais (LAZER, 2001).

Com receio do vazamento de informações fornecidas aos bancos e ao temer que as pessoas que os acessem os utilizem de forma inapropriada, fez-se necessário desenvolver um código de conduta para o uso correto da rede mundial de computadores (SANTOS e FAVACHO, 2021).

Assim, a Lei nº 12.965/2014 surge com o objetivo de garantir os direitos e as obrigações da internet no Brasil, estabelecendo princípios para um acesso com segurança, considerado como o marco civil da internet no país. Essa lei foi inspirada no Regulamento Geral de Proteção de Dados da União Europeia (BRASIL, 2014).

Anos depois, a Lei Geral de Proteção de Dados (LGPD), de nº 13.709, foi criada em 14 de agosto de 2018, com o intuito de garantir os direitos de liberdade e privacidade no que diz respeito aos meios digitais, sejam através de pessoas físicas ou jurídicas (BRASIL, 2018). Em suma, a LGPD busca assegurar, a todo e qualquer indivíduo, a titularidade de seus dados, e, assim, uma garantia prevista na constituição como direito à privacidade e à liberdade.

Porém, em muitos casos, os usuários se intimidam em compartilharem seus dados com algumas empresas, sejam elas comerciais ou sociais (MARRA, 2014). Para isso, a lei determina que, quando o usuário se dispõe a compartilhar seus dados, qualquer portabilidade que aconteça deve ser de forma a garantir a sua privacidade e segurança.

Nessa perspectiva, Miranda (2018, p. 49) afirma que:

> Resta inquestionável que a informação é importante tanto para o desenvolvimento pessoal como para o desenvolvimento econômico da pessoa e da sociedade, porém, a informação utilizada de forma exacerbada e como desvio de finalidade é uma afronta à privacidade que deve ser garantida, bem como empodera demasiadamente os detentores dessas informações.

Nesse sentido, o artigo 18 da LGPD estabelece que a portabilidade dos dados é direito do titular ou seu representante legal, o que impede o controlador dos dados cobrar alguma taxa pelo processo de portabilidade:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) V- portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e

> observados os segredos comercial e industrial de acordo com a regulamentação do órgão controlador, (BRASIL, 2018).

Logo, pode-se observar que a portabilidade deverá acontecer mediante requisição do titular dos dados. Isso deve acontecer da forma mais objetiva possível, sem gerar dificuldades ou empecilhos. Assim, Frazão (2022, p.15) define que “o direito à portabilidade, para atingir tais propósitos, deve ser fácil, gratuito e assegurado de modo a permitir a usabilidade dos dados com ciência e segurança”.

2.1.2. Segurança em sistemas IoT

Internet of Things (IoT) trata-se de um sistema capaz de medir parâmetros do cotidiano, como temperatura, frequência cardíaca e luminosidade, por exemplo, por meio de sensores conectados à internet (YANG *et al.,* 2017). Hoje, no mundo digital, são considerados como sistemas IoT os dispositivos autônomos e sistemas isolados, a exemplo dos *smartwatches, wearables*, telefones, entre outros (BUTUN *et al.,* 2020).

Por se tratar de um sistema diretamente ligado ao cotidiano das pessoas, as questões de segurança desses dispositivos precisam ser levadas em consideração. Para isso, Neshenko *et al.,* (2019) afirmam que a negligência na segurança desses sistemas pode resultar no vazamento de informações pessoais sensíveis, capaz de prejudicar o usuário.

Neste sentido, Frustaci *et al.,* (2017) abordam as principais camadas dos sistemas IoT, que são: Percepção, transporte ou rede e aplicação. A Figura 1 aborda as categorias fundamentais dos sistemas que utilizam a tecnologia *Internet of Things*.

Figura 1. Camadas dos sistemas IoT

Fonte: ResearchGate

Hassija *et al.,* (2019) classificam que a principal função da camada Percepção é o sensoriamento por meio dos sensores e atuadores, em que os primeiros detectam os fenômenos físicos e a ação dos atuadores é realizada de acordo com os dados que são lidos. Para Yang *et al.,* (2017), a Percepção se trata da coleta de dados. Assim, após a coleta dos dados, as informações são transferidas através da camada de Transporte, também conhecida como camada de Rede. Essa função é denominada como *network* (HASSIJA *et al.,* 2019). Ao final de todo o processo de coleta e transporte, mostra-se a camada de Aplicação, composta por um conjunto de protocolos que permite a comunicação dos dados através de *softwares.* São exemplos de dados mostrados por esta camada a temperatura, umidade de ar, entre outros (FRUSTACI *et al.,* 2017; NESHENKO *et al.,* 2019).

Desse modo, a Figura 1, ilustra as camadas essenciais dos sistemas IoT definidas segundo Frustaci *et al.* (2017), Neshenko *et al.* (2019) e Hassija *et al.* (2019). Além da definição de cada camada, são enunciados exemplos de cada uma, bem como a sua importância.

2.2. A Cartilha de Segurança para Internet

A Cartilha de Segurança para Internet foi produzida pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.BR), no ano de 2012, em São Paulo. O documento traz os principais riscos causados pela utilização das redes sociais: as conexões com pessoas mal-intencionadas, a identidade furtada, a invasão de privacidade e as mensagens maliciosas.

De acordo com a cartilha, alguns cuidados precisam ser seguidos em relação às mídias sociais. As principais orientações estão voltadas acerca da privacidade do usuário, os cuidados com a localização, a privacidade alheia, a proteção contra códigos maliciosos e a proteção do perfil e imagem profissional.

Os conceitos que serão apresentados a seguir correspondem às orientações da Cartilha do CERT.BR (2012), com respaldo teórico, também, de alguns autores que abordam sobre a segurança das redes.

2.2.1. Os principais riscos de ataques virtuais

Os vírus são pequenos agentes infecciosos, à exemplo, o coronavírus (SARS-CoV-2) que contaminou – e ainda contamina – diversas pessoas, com a infecção dos sistemas respiratórios, e que pode se multiplicar rapidamente e sofrer diversas mutações.

De fato, o vírus digital segue basicamente as mesmas características do vírus biológico, quando se trata da rede mundial de computadores, onde os agentes, são programas, que estão contaminados com algum tipo *malware* (SANTOS e FAVACHO, 2021).

Ainda segundo Santos e Favacho (2021), o vírus digital trata-se de um programa mal-intencionado, que tem como objetivo prejudicar o sistema computacional, com a criação de autocópias e a sua propagação em outros aparelhos que utilizam da mesma rede, já que o maior alvo desse tipo de vírus é a rede local.

Os principais tipos de vírus digitais são: *Blended Threats, Keylogger, Ransomware, Spyware, Trojan Horse, Worms*. O *Blended Threats*, por exemplo, se dá por meio de e-mails falsos, e que se torna uma mistura de ameaças em um só local. No que se refere aos roubos de informações bancárias, o vírus responsável é o *Ransomware*, capaz de assumir o controle dos dados (RAMAKRISHNAN e TANDON, 2018).

Com relação às conexões com pessoas “mal-intencionadas”, infelizmente, muitos usuários ainda se submetem a ações de perfis falsos. E, com isso, indivíduos com má conduta conseguem dinheiro e informações pessoais dos usuários, a fim de furtar a identidade desses, o que ocasiona a perca da conta na rede social ou o seu total controle. Com o controle da rede social do usuário, os indivíduos mal intencionados podem aplicar golpes em familiares da vítima ao assumir a identidade do outro. Desse modo, quanto mais informação os invasores obtiverem, mais fácil será a apropriação do perfil.

Vários exemplos de ataques virtuais estão presentes no cotidiano, como a fraude por antecipação *(Advance Fee Fraud),* que consiste no repasse de valores antes mesmo da aquisição de determinados produtos ou serviços; o *Phishing,* que consiste em terceiros se passarem pela assessoria oficial de empresas ou sites populares; os golpes voltados à *sites* fraudulentos de

comércio, compra ou leilão; os boatos *(Hoax)*, que são mensagens alarmantes e falsas que induzem o indivíduo a acessar sites maliciosos (CERT, 2012).

Sobre o *Phishing*, o próprio nome já se associa ao roubo de informações pessoais. *Phishing* é oriundo do inglês, que significa pescar, responsável por "fisgar" informações como: Nome completo, documentos de identidade, dados bancários. Esse tipo de ataque pode ser apresentado em vários tipos, cujo os principais são: *Blind Phishing*, *Smishing*, *Scam*, *Clone Phishing*, *Spear Phishing*, *Whaling*, *Vishing*, *Pharming* (PEREIRA, 2012).

No que se refere a invasão de privacidade, a cartilha aborda que, quanto maior o número de contatos que o usuário cria em sua rede social, maior serão as chances de que as informações pessoais serão repassadas para terceiros de maneira indevida.

A cartilha aborda, ainda, os principais ataques realizados por meio de varreduras em redes *(scan),* que consiste em realizar uma busca minuciosa em aparelhos ativos, com a identificação das vulnerabilidades e, consequentemente, a concretização de invasão.

Além disso, estão também, nas orientações apresentadas no documento, o cuidado com o *e-mails spoofing,* uma técnica bastante utilizada, que altera o cabeçalho dos e-mails a fim de se assemelharem ao máximo com os das contas oficiais de sites ou empresas; a Interceptação de Tráfego *[Sniffing],* que pode ser realizada de forma legítima pelos administradores da rede ou maliciosa por atacantes, com o intuito de coletar informações importantes, a exemplo de senhas, número de cartões e outras informações pessoais; a Força Bruta *[Brute force],* que consiste em adivinhar, por tentativas e erros, o acesso, a possíveis senhas e usuários.

A cartilha também discorre sobre a desfiguração de página (*Defacement*), a fim de explorar as vulnerabilidades do servidor ou furtar senhas e acessos. A negação de serviço (*DoS e DDoS*) não tem como foco o roubo de senhas ou acesso, mas, sim, causar uma indisponibilidade nos sistemas do alvo.

Ainda nessa perspectiva, a cartilha apresenta os riscos que as mensagens maliciosas fornecem por meio de códigos ou links, a exemplo de *vírus, worm, bot* e *botnet, spyware, backdo*or, cavalo de troia e *rootkit*. Além do *spam*, há os chamados e-mails não solicitados, mas que são enviados para um grande número de pessoas.

Por fim, são elencados outros riscos, como os *cookies*, os códigos móveis, as janelas de *pop-up*, os links patrocinados, os *banners* de propaganda e os programas de distribuição de arquivos *Peer-to-Peer* (P2P).

2.2.2. As boas práticas para privacidade e proteção de dados

Em meio as tecnologias vivenciadas nos diversos setores da sociedade, surge a necessidade de se criar estratégias de segurança para as informações. Assim, a segurança da informação tem como objetivo fornecer proteção para as informações, sejam elas de um indivíduo ou de um determinado grupo (DURBANO, 2019).

Desse modo, Queiroz e Rosa (2019) abordam que, para garantir segurança da informação, é necessário que sejam levados em considerações alguns fatores, como: o ambiente, o usuário e sua estrutura digital, bem como as pessoas mal-intencionadas que buscam danificar ou alterar os dados. É de suma importância que haja uma política de segurança explícita aos usuários, de maneira que garanta a proteção da informação e que os usuários sigam as normas de segurança que foram determinadas (SÊMOLA, 2003).

O primeiro aspecto que deve ser levado em consideração é que, apesar de se tratar de um meio virtual, os acontecimentos que ocorrem na internet não devem ser distanciados do conhecimento humano, sobretudo por se tratar de pessoas, organizações e dados que estão integrados dentro e fora da rede de computadores (PARISER, 2012). Faz-se necessário que as pessoas, ao acessarem as redes sociais, por exemplo, devem manter os mesmos cuidados que assumem em seu dia a dia. Desse modo, da mesma forma que precisam estar atentos aos lugares que frequentam, no não fornecimento de informações a estranhos ou no impedimento de transmissão de dados para empresas ou organizações suspeitas, devem adotar cuidados específicos ao acessar a internet.

Segundo Hernandez (2011) as diferentes mídias sociais caracterizam-se como um ambiente para expressar opiniões, registrar momentos e compartilhar informações. Dentre elas destacam-se alguns formatos, como os sites de relacionamentos, os *blogs, e-mails* e *scrapbooks.*

Atualmente, algumas mídias sociais estão em alta, se tornam um ambiente de interação e multimídias, a exemplo de fotos, vídeos e músicas. As principais mídias utilizadas pelo mundo são: O *Facebook,* o *Instagram*, o *Linkedin*, o *Twitter*, o *Tiktok* e o *Youtube* (CRUZ, 2020).

No que se refere à privacidade, a cartilha orienta que é essencial que o usuário mantenha seus dados bloqueados para *sites* desconhecidos. Além disso, deve-se levar em consideração a cautela pessoal ao aceitar conexões com outros usuários, especialmente em evitar interações entre usuários indesejados.

É necessário, ainda, que se tenha certa cautela ao postar nas redes sociais sua localização em tempo real. A recomendação adequada é que seja postado apenas ao sair do local em questão, como uma forma de evitar roubos ou outras formas de atentado à integridade física. Da mesma forma, ao realizar planos de itinerários de viagens, esse não deve ser postado publicamente antes da sua execução.

Ao abordar sobre a privacidade alheia, a cartilha alerta sobre publicações específicas que envolvem terceiros sem autorização, de modo que se deve evitar expressar sobre a rotina e hábitos dessas pessoas.

No que diz respeito a proteção contra códigos maliciosos, é orientado que o usuário mantenha seu computador seguro, com a atualização dos *softwares* de segurança e *firewall*, além de uma atenção fundamental com mensagens recebidas de pessoas próximas, sobretudo com compartilhamento de dados, pois as redes desses indivíduos também podem ser afetadas pela invasão.

A cartilha recomenda ainda que o perfil do usuário seja cuidadoso ao criar suas senhas de seguranças, a fim de não facilitar o acesso para possíveis invasores. Para isso, é recomendado que as senhas possuam 6 dígitos, no mínimo, sendo utilizados letras (maiúsculas e minúsculas), números e caracteres. Além disso, não é recomendado a inserção do nome do usuário na senha (ROCCIA, 2021). A notificação de acesso ao *login* deve sempre estar ativada, de modo que o usuário seja avisado nos momentos que alguém tentar acesso a sua conta (SOUSA, 2021).

Por fim, vale ressaltar a importância de que o usuário seja seletivo quanto às postagens que envolvam sua imagem profissional nas redes sociais. Em

ciência do que deve ser diferenciado do conteúdo pessoal e profissional nas redes sociais (SANTOS e FAVACHO, 2021).

2.3. Segurança em camadas nos servidores da WEB.

Em meio aos ataques cibernéticos, os dados pessoais são os mais afetados, e é na contemporaneidade que existe o principal alvo dos *crackers*[2]. Esses dados envolvem desde as informações mais simples, como nomes de escolas, datas de nascimento, como também as mais complexas, que envolvem fotografias, números de CPF (Cadastro de Pessoa Física) ou RG (Registro Geral) (SANTOS, 2016). Para garantir a segurança dos dados citados, a Segurança da Informação prioriza os três pilares como essenciais: Integridade, Disponibilidade e Confidencialidade.

Segundo Galvão (2015), a integridade busca garantir a veracidade das informações, isto é, que não são afetadas por nenhum tipo de modificação. A autora afirma a importância de preservar a integridade dos dados, de modo que os *softwares* executem as suas rotinas sem falhas. A integridade dos dados não permite que sejam alterados os dados no percurso da mensagem, de maneira que esse envio seja intencional ou não (GALVÃO, 2015).

De acordo com Código de Prática para a Gestão de Segurança da Informação NBR ISO/IEC[3] 27002 (2005), a disponibilidade garante que a informação esteja livre, uma vez que a pessoa autorizada deseje acessá-la. Já a confidencialidade diz respeito à privacidade dos dados, de forma que estejam disponíveis apenas para as pessoas autorizadas.

Para amenizar esses ataques, criou-se um Protocolo de Transferência de Hipertexto Seguro (HTTPS), que protege a transferência de dados entre o computador do usuário e o site, por meio da criptografia (ROCHA JR, 2013). Entende-se por criptografia o processo matemático que faz com que a mensagem enviada ou recebida não seja lida por terceiros. Ou seja, é a garantia

[2] Termo utilizado para denominar o responsável pelo ataque de um sistema computacional. Diferentemente dos *crackers*, os *hackers* invadem os sistemas para buscarem autoconhecimento sem a intenção de prejudicar usuários.

[3] A ISO é uma organização internacional não governamental independente, criada em meados de 1946 com o intuito de desenvolver Normas Internacionais, de forma voluntaria.

de que somente quem a enviou e quem a recebeu terá acesso (SURVEILLANCE SELF-DEFENSE, 2018).

A criptografia, segundo Stallings (2014), diz respeito à codificação e decodificação dos dados, o que impede as ameaças de pessoas mal-intencionadas. Neste sentido, é criado um protocolo para a efetiva troca de dados entre os usuários e o conjunto de páginas da internet, e essa troca de informações entre o computador do usuário e o servidor que hospeda um determinado website é denominado de *Hypertext transfer protoco* (HTTP). Esse protocolo é o responsável por permitir que uma página seja visualizada na web (ROVEDA, 2018). O HTTPS é uma versão mais segura do que HTTP.

Desse modo, para garantir a implementação do HTTPS, o usuário precisa adquirir certificados de segurança confiáveis, através de uma Autoridade de Certificação, do inglês *Certification Authority* (CA), que irá analisar se, de fato, o endereço da *web* pertence à organização; usa redirecionamentos permanentes à páginas ou recursos HTTPS; verifica se o *Google* consegue rastrear as páginas HTTPS; e utiliza de conteúdos compatíveis com o *Strict Transport Security* (HSTS), criado com intuito de assegurar a proteção aos navegadores (IZUMI e TOMAZETI, 2019).

A diferença entre HTTP e HTTPS é que o segundo está acrescido de criptografia dos dados. Essa criptografia se faz presente neste protocolo a partir do certificado *Secure Sockets Layer (SSL)*. Assim, as informações pessoais cedidas por um determinado *site* são protegidas pelo HTTPS (ROVEDA, 2018).

O certificado SSL, ou certificado digital, funciona como uma camada de segurança sobre uma página com o objetivo de isolar as informações. Essa camada permite, ainda, atestar a identidade de um site para que o usuário permaneça assegurado no acesso de eventuais páginas falsas (ROVEDA, 2018).

De maneira semelhante, o certificado *Transport Layer Security* (TLS) protege os dados, com algumas melhorias sobre os protocolos de segurança, em relação ao seu antecessor o SSL. Com isso, os certificados SSL não são mais usados com tanta frequência (HOSTINGER, 2019).

2.4. Redes sociais e a pandemia: a vulnerabilidade para ataques cibernéticos

O espaço criado através da rede mundial de computadores, com o intuito de promover a interação humana através dos recursos tecnológicos, recebe o nome de *cibernético* (APDSI, 2005). Além de serem constituídos de sistemas de informações automatizados, os espaços *cibernéticos* apresentam uma rede de comunicação de dados a fim de fornecer informações sejam a usuários ou a clientes (VIANNA e FERNADES, 2015).

Desse modo, ISO/IEC 27032 (2012) caracteriza o espaço *cibernético* como "um ambiente complexo resultante da interação de pessoas, *software* e serviços existentes na *internet*, conectados entre si por meio de dispositivos de tecnologia e redes, o qual não existe como forma física".

Assim, Wallier Vianna, (apud BARBOSA *et. al,* 2021) traz as principais situações em que podem ocasionar riscos de ataques *cibernéticos*. Dentre elas, destacam-se os programas indesejados, a exemplo de vírus, cavalos de troia ou *spywares*; utilização de funções não recomendadas nos programas operacionais; inserção de comandos não documentados, que cede a terceiros o poder de alterar as operações do sistema e disponibilização de acesso por meio de senhas a pessoas não autorizadas, e que possam promover o ataque ou modificação de *hardware.*

Com o início da pandemia e, consequentemente, o isolamento social, as pessoas ficaram mais tempo em seus lares. Em muitos casos, a internet se tornou a alternativa mais eficaz para o entretenimento e ocupação desse tempo que permaneceram isoladas em suas residências. É importante destacar que a pandemia provocou um maior tráfego de dados na rede, o que aumentou o contato virtual com outras pessoas e, por conseguinte, provocou uma elevação no número de vítimas que sofrem ataques de crimes (ROCHA, 2020).

Em uma pesquisa realizada no ano de 2021 pela empresa de cibersegurança Norton, revelou que nos 12 meses anteriores à pesquisa, 35% das pessoas com acesso à internet no mundo sofreram ataques cibernéticos. Segundo a Associação de empresas e profissionais da informação, no ano de 2021, mais especificamente no primeiro semestre, o Brasil sofreu mais de 16,2 bilhões de tentativas de ataques cibernéticos. No ano de 2020, foi informado ao

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) um total de 665.079 ataques à população brasileira.

De acordo com o correio Braziliense (2020), houve um aumento significativo dos ataques *cibernéticos,* principalmente pelo fato de as pessoas aderirem, neste período pandêmico, às compras realizadas pela *internet.* Segundo a Polícia Civil do Distrito Federal, entre março e junho de 2020, os crimes de estelionato aumentaram 198,95%. Já em relação aos roubos mediante a fraude subiu cerca de 310,97%. Nesse sentido, o jornal “Daqui de Minas” (2020) aponta que, nos meses de janeiro a maio, registrou-se mais de 3 mil casos de crimes *cibernéticos*, um número que chega a ser aproximadamente 600 a mais que em 2019.

Segundo Gatefy (2020), as campanhas de *phishing* e *spam* são utilizadas para infectar *softwares,* com o objetivo de extorquir dinheiro e dados pessoais, principalmente na venda de equipamentos de proteção individual falsificados, e teve como proveito o atual cenário. Além desses ataques, a agência afirma que, nesse período, houve um aumento da criação de sites falsos e ataques contra crianças e adolescentes, sobretudo na elevação do número de exploração sexual infantil.

Ao longo dessas seções, foram apresentas os processos de transições das Revoluções Industriais ao longo dos anos, bem como o marco de cada revolução e sua influência para a criação da Lei Geral de Proteção de Dados. Evidenciou-se a importância da Cartilha de Segurança para Internet, criada em 2012, pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil, documento esse que aborda os principais riscos de ataques virtuais, assim como as boas práticas para a privacidade e proteção de dados na utilização dos meios digitais.

Outro fator significativo, é uso de segurança em camadas nos servidores Web, destacando o Código de Prática para a Gestão de Segurança da Informação NBR ISO/IEC 27002, tal como a aplicação de criptografia no Protocolo de Transferência de Hipertexto Seguro, do inglês *Hyper Text Transfer Protocol Secure* (HTTPS). Por fim, as vulnerabilidades para ataques nas redes sociais durante a pandemia, exibindo as principais técnicas utilizadas nesses ataques cibernéticos, como a elevação do número de vítimas que sofreram com esses crimes ao longo da pandemia.

3. METODOLOGIA

Este estudo se trata de uma pesquisa integrativa de revisão de literatura com uma abordagem qualitativa, caracterizada como método de sintetizar estudos anteriores da temática abordada neste trabalho, o que permite fazer uma análise de forma ordenada para um maior aprofundamento do tema (SOUSA et al., 2017).

E, para definir a abordagem qualitativa, Prodanov e Freitas (2013) discorrem que “o ambiente natural é fonte direta para coleta de dados, interpretação de fenômenos e atribuição de significados”. Essa definição está inserida na coleta de artigos, dissertações, teses, monografias, livros e outras fontes que foram utilizadas para a fundamentação desta pesquisa.

A questão norteadora para essa pesquisa é: Quais os meios eficazes para manter a privacidade e a proteção dos dados das redes sociais durante a pandemia da COVID-19?

Os critérios de inclusão estabelecidos foram: trabalhos completos online nacionais na íntegra na forma de artigos científicos, com acesso gratuito, nos idiomas português e inglês, publicados entre os anos de 2020 a 2022 e que atendam ao objetivo proposto, e que apresentam, em sua discussão, questões relacionadas à proteção dos dados durante o período de pandemia da COVID-19.

As palavras chaves utilizadas na busca foram: Privacidade; Proteção de Dados; Pandemia; Redes Sociais.

Com o uso do título deste trabalho como busca no *Google Acadêmico*, obteve-se um resultado de dezesseis mil publicações. Após um segundo filtro no mesmo repositório, agora sendo utilizado as palavras chaves na barra de pesquisa, obteve-se um resultado de quinhentos e sessenta e cinco publicações.

Com isso, foi feito um terceiro filtro, em vista do alcance dos objetivos deste trabalho, nessa última seleção, após uma averiguação minuciosa dos títulos das publicações encontradas, foram eliminados os artigos que não possuíam relação com a temática abordada, e assim obteve-se um resultado de seis artigos. Por conseguinte, foram priorizados os trabalhos que expusesse em seu conteúdo a proteção de dados nas redes sociais em tempos de pandemia, servido como base para a atual revisão de literatura.

4. RESULTADOS E DISCUSSÃO

Quadro 1. Perspectiva dos autores acerca da proteção de dados nas redes sociais em tempos de pandemia

Autor	Título	TRATAMENTO DE DADOS EM UMA PERSPECTIVA DA LEI GERAL DE PROTEÇÃO DE DADOS DURANTE A PANDEMIA DE COVID-19
VIEIRA e VECCHIO (2021)	Delineamento	Revisão bibliográfica por meio de doutrinas nacionais e internacionais.
	Objetivos	Analisar situações de urgência que suprimiram direitos individuais durante esse grave período, e de também perseguir as experiências de outros países que reconheceram a sensibilidade dos dados relacionados à saúde dos cidadãos.
	Principais Resultados	A Lei Geral de Proteção de Dados entrou em vigor no período pandêmico, portanto, é normal que apareçam conflitos de interesses e ameaças de violações a direitos. Outra face, a presença de um ente regulador independente - como a Agência Nacional de Proteção de Dados - seria de extrema importância diante desse cenário mundial, pois somente um órgão autônomo e imparcial seria capaz de fiscalizar o uso correto de dados, visando soluções definitivas.
	Conclusões	O tratamento de dados pessoais deve assegurar a proteção de direitos garantidos constitucionalmente, não devendo ser colocado em conflito com a privacidade de seus titulares, com a tutela da vida ou até mesmo com a saúde coletiva.

Autor	Título	COVID-19: A NECESSIDADE DE DISCIPLINA ADEQUADA À PROTEÇÃO DE DADOS SENSÍVEIS NO BRASIL
CORRÊA; PAULA e BELLINTANI (2020)	Objetivos	Analisar dois pontos essenciais da disciplina legal de dados sensíveis da Lei Geral de Proteção de Dados, a categoria de dados biométricos e o consentimento como principal base legal para o tratamento de dados, explicitando a divergência entre os regimes europeu e brasileiro, bem como os desafios decorrentes do caminho traçado pelo legislador nacional.
	Delineamento	Trata-se de uma revisão bibliográfica
	Principais Resultados	Medidas de enfrentamento à pandemia do Covid-19 têm se utilizado de diversas tecnologias digitais com finalidades de monitoramento e controle de propagação da doença, como o *contact tracing.*
	Conclusões	Os exemplos relativos ao tratamento de dados biométricos – especialmente quanto ao uso de imagens digitais de pessoais e à definição do consentimento exigido para o tratamento de dados pessoais sensíveis – demonstram a relevante margem interpretativa dos dispositivos da LGPD, como a ausência do conceito de dados biométricos e quando eles são dados sensíveis ou as exatas características do consentimento qualificado, e os problemas práticos que essa incerteza gera.

Autor	Título	PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DOS EFEITOS DA PANDEMIA DA COVID-19 NA PROTEÇÃO DOS DADOS
MONTEIRO (2020)	Objetivos	Analisar se o cenário de pandemia pode se tornar pretexto para que o direito de proteção de dados seja inutilizado.
	Delineamento	Revisão bibliográfica sobre a Lei Brasileira Geral de Proteção de Dados, o Regulamento Geral Europeu sobre a Proteção de Dados, estudos empíricos sobre o comportamento dos usuários no ambiente digital, investigações sobre a efetividade da anonimização de dados e o usufruto de dados de localização para a contenção de epidemias.
	Principais Resultados	O marco normativo da Lei Geral de Proteção de Dados ao garantir que o consentimento seja uma manifestação livre, informada, inequívoca e com vistas a uma finalidade específica, procura garantir que haja usufruto substancial do consentimento, posto que as pessoas ao anuírem pelo fornecimento dos seus dados, saberiam o porquê e quais os procedimentos que serão utilizados para tratar suas informações.
	Conclusões	A carência sobre entendimento de segurança digital se verifica reconhecível quando os indivíduos confrontados por ofertas econômicas estão mais suscetíveis a anuírem pelos seus dados, ao passo que, no momento em que alcançam a compreensão da magnitude de previsões que podem ser realizadas, a partir desses mesmos dados, sobre a vida privada, recuam dessa anuência.

Autor	Título	A proteção de dados e segurança da informação na pandemia Covid-19: contexto nacional
BARBOSA *et al.,* (2021)	Objetivos	Apresentar a lei geral de proteção de dados, segurança da informação e os ataques cibernéticos durante a pandemia Covid-19 e refletir o impacto social dos ataques medidas na sociedade e nas organizações.
	Delineamento	Trata-se de uma pesquisa qualitativa, baseada em uma revisão exploratória.
	Principais Resultados	As tecnologias digitais exercem papel crucial nesses tempos de pandemia, tendo um aumento no acesso, bem como o aceleramento no uso de algumas ferramentas a Inteligência Artificial, a qual está sendo bastante aplicada na área da saúde, seja no monitoramento de pacientes infectados, na busca de desenvolver vacinas, para citar alguns.
	Conclusões	Transformações provocadas no uso das tecnologias digitais trazem imensos desafios seja no campo ético na regulação de uso, na área de segurança e proteção dos dados, respeito aos direitos fundamentais de privacidade, na era pós-Covid-19.

Autor	Título	Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global
ALMEIDA *et al.,* (2020)	Objetivos	Enfatizar a importância da proteção de dados pessoais durante a pandemia.
	Delineamento	Trata-se de uma pesquisa qualitativa, baseada em uma revisão exploratória.
	Principais Resultados	Aspectos relacionados ao direito à privacidade, direito à proteção de dados pessoais e direitos de grupos não inviabilizam o uso de dados pessoais e a possibilidade de seu uso para responder à pandemia.
	Conclusões	A legitimidade de coleta, processamento, compartilhamento e uso de dados pessoais não advém do acesso aos dados, mas da confiança em quem os detém, tratando-os com transparência e dentro dos parâmetros legais.

Autor	Título	ALÉM DA TRANSPARÊNCIA: a Lei Geral de Proteção de Dados Pessoais e a *Accountability* como mecanismo de controle e proteção de dados
SILVA (2020)	Objetivos	Analisar a natureza jurídica e as limitações da responsabilidade civil dos mecanismos institucionais e seus agentes de proteção de dados no Brasil definidos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).
	Delineamento	Trata-se de estudo de natureza exploratória, analítica e descritiva, utilizando-se do procedimento de pesquisa bibliográfica e documental com analise de doutrinas, documentos, legislações em uma abordagem qualitativa.
	Principais Resultados	Devido as mudanças advindas da inovação e contínuo desenvolvimento tecnológico, o cenário nacional, quando comparado a outros países demonstrou uma certa fragilidade de legislação na proteção de dados, levando a necessidade de desenvolver uma regulamentação especifica para monitorar o processamento de dados em meio digital.
	Conclusões	É vantajoso uma articulação da lei com as várias instâncias que instrumentalizam os mecanismos de *accountability*, cujo foco é a visibilidade e transparência das atividades a serem realizadas para garantir que a sociedade e as entidades associadas possuam um livre acesso às informações. Isso porque não há dúvida que a transparência é requisito básico para promoção da *accountability*.

Os estudos de Vieira e Vecchio (2021) apontam que, durante a pandemia, a Lei Geral de Proteção de Dados não foi uma prioridade para os usuários da saúde. De início, algumas medidas já permitiram identificar certas falhas no que se refere à privacidade, a exemplo da geolocalização dos aparelhos celulares, com o intuito de controlar a circulação da “rota do vírus” da COVID-19. Medidas como essas, apesar de se apresentarem como perigosas e necessárias para a população, mostraram-se inconstitucionais e violadoras da legislação.

Neste sentido, Monteiro (2020) destaca que pequenos atos de coleta de informações invadem a privacidade das pessoas, sem que elas percebam que

são violadas, o que se tornam um instrumento poderoso que pode influenciar ou moldar comportamentos.

Sobre a LGPD, os autores Corrêa, Paula e Bellintani (2020) enfatizam a sensibilidade dos dados pessoais, ao realizar o reconhecimento facial, a verificação digital e reconhecimento de voz. Porém, apesar da LGPD caracterizar essas ações, através dos dados biométricos, como sensíveis, não define o termo em sua natureza, o que falta esclarecer o que são considerados dados pessoais somente aqueles que identificam o indivíduo. Essa falta de informação resulta em uma má interpretação nos indivíduos, o que compromete a importância da lei de proteção previstas nos documentos oficiais. Em seus estudos, Monteiro (2020) mostra a importância de se ter uma linguagem clara e mais transparente para as empresas utilizarem, a fim de que os cidadãos estejam conscientes acerca dos seus dados compartilhados.

No contexto pandêmico em que se situa esta pesquisa, Barbosa *et al.,* (2021) enfatizam a vulnerabilidade aos ataques cibernéticos, sobretudo porque as pessoas estão mais conectadas, o que traz desafios éticos quanto à regulação de uso na área de segurança. Segundo Brandão (2021), as redes sociais são uma mina de ouro para ataques cibernéticos, pois se utilizam da engenharia social, com o objetivo de coletar informações sigilosas de pessoas, além do usufruto do poder de persuasão, para atingir os usuários por meio das plataformas sociais.

Neste sentido, com intuito de que os dados dos usuários sejam tratados de forma lícita e responsável, faz-se necessário haver mais tecnologias para que, consequentemente, obtenha-se uma conformidade da lei de proteção de dados (ALMEIDA *et al.,* 2020). Ainda segundo os autores Almeida *et al.,* (2020), alguns países possuem centros especializados para processar e prover acesso aos dados anonimizados, uma vez que esses dados não são considerados dados pessoais, pois não possuem identidade dos indivíduos.

Dessa forma, Silva (2020) ressalta a necessidade de uma maior efetivação nas leis relacionadas à proteção de dados no Brasil. Há uma fragilidade no que se refere à essa legislação, pois é preciso que contenha uma regulamentação mais direcionada para o monitoramento dos dados de forma digital.

Desse modo, essa pesquisa tem como propósito solucionar as três questões norteadoras. Em primeiro lugar responder “Como a proteção de dados se torna algo relevante para o cotidiano, sobretudo em tempos de pandemia?”. Com isso, percebeu-se que com no início da pandemia houve um aumento na utilização dos meios digitais, para que essa navegação ocorra de forma segura, é recomendado a utilização das boas práticas para privacidade e proteção de dados, presentes na Cartilha de Segurança para Internet.

O segundo questionamento “De que maneira a Lei Geral de Proteção de Dados influenciou na utilização dos dados nos meios digitais, em especial na pandemia do COVID-19?”. A Lei Geral de Proteção de Dados, influenciou de maneira positiva na vida em sociedade, sendo uma garantia para os usuários dos meios digitais que seus dados serão utilizados e armazenados de forma segura, e caso isso não ocorra, essa má utilização dos dados pessoais poderá ser constituída como crime, previsto na constituição brasileira.

Por fim, a interrogativa “Como aplicar boas práticas de segurança para manusear as ferramentas que a era digital proporciona?”. Desse modo, foram descritas as principais práticas de segurança para a utilização dos meios digitais, essas condutas estão descritas na Cartilha de Segurança para Internet, desenvolvida pelo (CERT.BR) no ano de 2012, em São Paulo. Um exemplo de boa prática, é a utilização de senhas com no mínimo seis dígitos, e dentre os dígitos, possuam letras maiúscula e minúsculas, números e caracteres especiais.

5. CONCLUSÃO

O objetivo geral, de identificar meios eficazes para manter a privacidade e a proteção dos dados das redes sociais durante a pandemia da COVID-19, desse trabalho foi atingido, ao mostrar vários métodos eficientes, através de dicas de segurança, para a proteção das redes sociais nesse período de pandemia em que as pessoas se encontram mais conectadas à internet e também mais vulneráveis a ataques cibernéticos.

Tornou-se evidente o aumento nas conexões virtuais por meio da internet durante a pandemia da COVID-19. Assim, quanto mais as pessoas se conectam através de suas redes sociais com as outras pessoas, mais chances têm de serem vítimas de ataques cibernéticos. Nesse sentido, foram apresentadas algumas recomendações acerca dos cuidados que usuários deverão conter, por meio da cartilha de segurança de São Paulo, ao abordar os principais golpes virtuais, como: *Blended Threats, Keylogger, Ransomware, Spyware, Trojan Horse, Worms.*

A partir disso, foram apontadas algumas medidas de segurança, para que, as pessoas que estão em suas casas, saibam como agir em uma tentativa de ataque cibernético. Mostrou-se, ainda, que as principais recomendações estão relacionadas ao cuidado que os usuários precisam ter com suas senhas, para não facilitar os ataques cibernéticos.

Este trabalho, ademais, destaca a importância da segurança em camadas dos servidores da *web*, e que prioriza os três pilares essenciais para de preservação dos dados pessoais: Integridade, Disponibilidade e Confidencialidade. Dessa forma, com esses pilares, é possível evitar ataques frequentes dos *crackers*.

Apesar do avanço das tecnologias, e, principalmente, do aprimoramento das informações, evidenciou-se que muitas pessoas ainda não são totalmente cientes da Lei Geral de Proteção de Dados, criada no Brasil desde de 2018, mas que só entrou em vigor no ano de 2020. Esse problema faz com que esses usuários acreditem em informações falsas, apresentadas nas redes de comunicação, o que pode colocar em risco a credibilidade de legislação de privacidade dos dados no Brasil.

Esse trabalho se torna necessário para alertar as pessoas sobre o quanto é perigoso uma exposição acima dos limites em suas redes sociais, o que possibilita a ocorrência de golpes virtuais que trarão sérias consequências para quem usa e também para pessoas de seu convívio.

Ao longo do desenvolvimento deste estudo identificaram-se algumas limitações, se tratando da busca de embasamento teórico, embora que haja muito material voltado para a segurança dos dados, foi difícil encontrar autores que discutissem da temática abordada, durante o período pandêmico. Outro fator limitante foi que muito dos trabalhos pesquisados estavam em línguas estrangeiras e com os seus acessos bloqueados, devido exigir a assinatura dos repositórios para poder ter acesso às pesquisas.

Com relação aos trabalhos futuros, seria interessante de se pesquisar a relação dos ataques cibernéticos, durante o período da pandemia e o seu período antecessor. Outro viés de estudos, poderia estar relacionado às questões sociais da população, ou seja, um estudo voltado para identificar os indivíduos que são mais suscetíveis a esses tipos de ataques virtuais.

REFERÊNCIAS

ALMEIDA, Bethania de Araujo. **Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global.** 2020. Disponível em: <https://www.scielo.br/j/csc/a/T6rwdhnTNzp5vYr84w9xthB/?lang=pt#>. Acesso em: 03 jul 2022.

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (APDSI). (2005). **Glossário da Sociedade da Informação.** Portugal: APDSI.

ASSOCIAÇÃO DE EMPRESAS E PROFISSIONAIS DA INFORMAÇÃO. Brasil sofre mais de 16,2 bilhões de tentativas de ataques cibernéticos na primeira metade de 2021. 2021. Disponível em: <https://abeinfobrasil.com.br/brasil-sofre-mais-de-162-bilhoes-de-tentativas-de-ataques-ciberneticos-na-primeirametade-de-2021/>. Acesso em: 17 abr 2022.

BARBOSA, Juliana Souza et al. **A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional**. Research, Society andDevelopment, v. 10, n. 2, p. e40510212557-e40510212557, 2021.

BASAN, Arthur Pinheiro. **Publicidade digital e proteção de dados pessoais: o direito ao sossego**. Indaiatuba, SP: Editora Foco, 2021.

BRANDÃO, Guilherme Henrique Freitas. **Segurança da Informação nas Redes Sociais: Um Estudo Teórico e Experimental Sobre as Redes Sociais**. (2021). Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2775>. Acesso em: 17 abr 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. (2014, 23 de abril)**. Diário Oficial da União. Recuperado em 31 de julho de 2014: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 03 fev 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 (LGL\2018\7222).** Diário Oficial da União**.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 fev 2022.

BUTUN, I.; ÖSTERBERG, P.; SONG, H. **Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures**. IEEE Communications Surveys & Tutorials, v. 22, n. 1, p. 616-644, novembro 2020. DOI: 10.1109/COMST.2019.2953364. Disponível em: <https://ieeexplore.ieee.org/document/8897627>. Acesso em: 01 jun 2022.

CAVALCANTI, Henrique Tagliari. **O ciberespaço e os direitos fundamentais na era digital da deep web**. Intertem@ s ISSN 1677-1281, v. 42, n. 42, 2021.

CAVAZZINI, L. S., CAVALCANTI, L. de L., MACHADO, A. R., DENNY, D. M. T. & SALEME, E. R. (2018). **Aplicabilidade da indústria 4.0 na cadeia produtiva agroindustrial: sonho ou realidade**. VIII Congresso Brasileiro de Engenharia de Produção.
CERT.br. **Cartilha de Segurança para Internet**. São Paulo: CERT.br. SP. Brasil. 2012. Disponível em: <http://cartilha.cert.br>. Acesso em: 17 abr 2022.

COELHO, Akeni Lobo et al. **A utilização de tecnologias da informação em saúde para o enfrentamento da pandemia do Covid-19 no Brasil.** Cadernos Ibero-Americanos de Direito Sanitário, v. 9, n. 3, p. 183-199, 2020.

CONTREIRAS, Pedro Augusto Rodrigues. **A quarta revolução industrial: um estudo de caso realizado na empresa Lix de Tecnologia**. Revista Gestão, Inovação e Negócios, v. 1, n. 1, p. 79-97, 2015. Disponível em: <http://revistas2.unievangelica.edu.br/index.php/administracao/article/view/1307>. Acesso em: 17 abr 2022.

CORRÊA, I.; DE PAULA, F.; BELLINTANI, B. COVID-19: a necessidade de disciplina adequada à proteção de dados sensíveis no Brasil. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 14, n. 1, p. 179–206, 2020. DOI: 10.30899/dfj.v0i0.1007. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1007>. Acesso em: 03 jul 2022.

CORREIO BRAZILIENSE. (2020). **Registros de golpes na internet crescem 310% no DF durante a pandemia.** Disponível em: <https://www.correiobraziliense.com.br/cidades-df/2020/08/4868977-mais-Golpes na-pandemia.html>. Acesso em: 01 fev 2022.

COSTA, Verlaine Lia; ESCORSIM, Sérgio; COSTA, Deneive Leonor. **Processo produtivo e produção de aço: a inserção do Grupo Gerdau S.A. no cenário mundial.** Congresso Internacional de Administração, 2007. Disponível em: < http://ri.uepg.br/riuepg/bitstream/handle/123456789/778/EVENTO_Processo%20produtivo%20e%20produ%c3%a7%c3%a3o%20de%20a%c3%a7o%20a%20inser%c3%a7%c3%a3o%20do%20Grupo%20Gerdau.pdf?sequence=1>. Acesso em: 16 jul 2022.

CRUZ, Maria do Socorro Corrêa da. **Redes Sociais Virtuais: Percepção, finalidade e a influência no comportamento dos acadêmicos**. Brazilian Journal of Development, v. 6, n. 3, p. 12433-12446, 2020. Disponível em: <https://www.brazilianjournals.com/ojs/index.php/BRJD/article/view/7681>. Acesso em: 17 abr 2022.

DURBANO, Vinicius. **Cartilha de Segurança da informação: Como aumentar sua proteção**. [S. l.], 2019. Disponível em: <https://blog.ecoit.com.br/cartilha-deseguranca-da-informacao/>. Acesso em: 08 fev 2022.

FIOCRUZ. **Informações sobre o SARS-CoV-2 e a COVID-19. 2022**. Disponível em: <https://www.bio.fiocruz.br/index.php/br/sua-saude/informacoes-sobre-doencas/informacoes-coronavirus>. Acesso em: 17 jul 2022.

FRAZAO, Ana. **Nova LGPD: direito à portabilidade.** 2018. Disponível em: < https://www.jota.info/opiniaoe-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direito-a-portabilidade-07112018>. Acesso em: 16 fev 2022.

FRUSTACI, M.; PACE, P.; ALOI, G.; FORTINO, G. **Evaluating Critical Security Issues of the IoT World: Present and Future Challenges**. IEEE Internet of Things Journal, v. 5, n. 4, p. 2483-2495, agosto 2018. DOI: 10.1109/JIOT.2017.2767291. Disponível em: <https://ieeexplore.ieee.org/document/8086136>. Acesso em: 31 mai 2022.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Person Education do Brasil, 2015.

GATEFY. **Como a Covid-19 impactou os crimes cibernéticos, segundo a Europol**. (2020). Disponível em: <https://gatefy.com/pt-br/blog/covid19-crimes-ciberneticos-relatorio-europol/>. Acesso em: 01 fev 2022.

GUSMAO, Gabriel; BRITO, Parcilene. **MODELO DE INTERNET DAS COISAS PARA O PARQUE ESTADUAL DO CANTÃO**. (2015). Disponível em: <https://www.researchgate.net/figure/Figura-6-Arquitetura-de-tres-camadas-A-Camada-de-Percepcao-e-o-nivel-mais-proximo-ao_fig2_315600552>. Acesso em: 24 jul 2022.

HASSIJA, V.; CHAMOLA, V.; SAXENA, V.; D. Jain, D.; GOYAL, P.; SIKDAR, B. **A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures**. IEEE Access, v. 7, p. 82721-82743, 2019, junho 2019 DOI: 10.1109/ACCESS.2019.2924045. Disponível em: <https://ieeexplore.ieee.org/document/8742551>. Acesso em: 31 mai 2022.

HENRIQUES, Cláudio; PESSANHA, Maierovitch; VASCONCELOS, Wagner. **Crises dentro da crise: respostas, incertezas e desencontros no combate à pandemia da Covid-19 no Brasil**. Estudos avançados, v. 34, p. 25-44, 2020.

HERNANDEZ, R. **Qual é a diferença entre Redes Sociais e Mídias Sociais?** 2011. Disponível em: <https://pt-br.facebook.com/notes/consumidor-moderno/ qual é a diferença entre redes sociais e mídias sociais?>. Acesso em: 09 fev de 2022.

HOSTINGER. **O que é SSL e TLS.** 2019. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-ssl-tls-https>. Acesso em: 22 mar 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2012). **ISO/IEC 27032:** Informationtechnology: Security techniques: Guidelines for cybersecurity. Geneva:ISO/IEC. Disponível em: < https://www.iso.org/home.html>. Acesso em: 24 jun 2022.

IZUMI, Paulo Teruo; TOMAZETI, Daiane Mastrangelo. **Segurança e Privacidade: Proteção e tratamento de dados nos aplicativos de redes sociais**. 2019. Disponível em: <

https://hto.ifsp.edu.br/portal/images/thumbnails/images/IFSP/Cursos/Coord_ADS/Arquivos/TCCs/2019/TCC_PauloTeruoIzumi.pdf>. Acesso em: 03 mar 2022.

JORNAL DAQUI. (2020). **Crimes Cibernéticos Crescem Durante a Pandemia da Covid-19.** <https://www.daquibh.com.br/crimes-ciberneticos-crescem-durante-a-pandemia-da-covid-19/>. Acesso em: 26 mai 2022.

LAZER, David; MAYER-SCHONBERGER, Viktor. **Governing networks:**telecommunicationderegulation in Europeandthe United States. **Brook. J. Int'l L.**, v. 27, p. 819, 2001. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/bjil27&div=33&id=&page=>. Acesso em: 10 abr 2022.

MARRA, Gabriel Artur et al. Facebook: negociação de identidades e o medo da violência. **Arquivos Brasileiros de Psicologia**, v. 66, n. 1, p. 18-32, 2014.

MIRANDA, Leandro Alvarenga. **A proteção de dados pessoais e o paradigma da privacidade**. São Paulo: All Print Editora, 2018.

MONTEIRO, Guilherme Ornelas. **Proteção de Dados Pessoais: uma análise dos efeitos da pandemia da COVID-19 na proteção dos dados**. Revista Caderno Virtual, p. 446- 473, 2020. Disponível em: <https://portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/4849>. Acesso em: 13 jul 2022.

NESHENKO, N.; BOU-HARB, E.; CRICHIGNO, J.; KADDOUM, G.; GHANI, N. **Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations**. IEEE Communications Surveys & Tutorials, Singapore, v. 21, n. 3, p. 2702-2733, abril 2019. DOI: 10.1109/COMST.2019.2910750. Disponível em: <https://ieeexplore.ieee.org/document/8688434>. Acesso em: 02 jun. 2022

PARISER, Eli. **O filtro invisível: o que a internet está escondendo de você**. Editora Schwarcz-Companhia das Letras, 2012.

PEREIRA, Cleber Guedes. **Phishing: Conceitos e ações preventivas aplicadas à empresa**. 2012. Disponível em: <https://repositorio.uniceub.br/jspui/handle/235/8136>. Acesso em: 10 abr 2022.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar. **Metodologia do trabalho científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico**. 2. ed., Novo Hamburgo: Feevale, 2013. Disponível em: <www.feevale.br/editora>. Acesso em: 17 jul 2022.

QUEIROZ, Mariana Pessoa De; ROSA, Nícolas Domingues. **Phishing e redes sociais: um estudo de caso**. São Paulo, p. 1-88, 2019. Disponível em: <http://ric.cps.sp.gov.br/handle/123456789/3780>. Acesso em: 20 mai 2022.

RAMAKRISHNAN, Ullas P.; TANDON, J. K. The evolving landscape of cyber threats. **Vidwat**, v. 11, n. 1, p. 31-35, 2018. Disponível em:

<https://www.proquest.com/openview/61f5c620a5cd1b8d34f1a690eb6b1a15/1?pq-origsite=gscholar&cbl=936333>. Acesso em: 17 abr 2022.

ROCCIA, Rubens Douglas. **Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas**. 2021. Disponível em: <https://bcc.ime.usp.br/tccs/2020/rubensd/Monografia.pdf>. Acesso em: 20 mai 2022.

ROCHA, A. A. S. *et al*. **Tecnologias, acesso à Internet e impactos da Pandemia para alunos (as) do Ensino Médio da 13ª URE/Breves**. 2020. Tese de Doutorado. Universidade Federal do Pará. Disponível em: < https://campusbreves.ufpa.br/images/documentos_institucionais/05.-Relatrio-EM---Tecnologias-acesso--Internet-e-a-Pandemia-para-alunosas-do-EM.pdf>. Acesso em: 29 mai 2022.

ROCHA JR, Valdemar C. **Segurança de Rede**. Revista de Tecnologia da Informação e Comunicação, v. 3, n. 1, p. 14-21, 2013. Disponível em: <http://rtic.com.br/index.php/rtic/article/view/34>. Acesso em: 20 mai 2022.

RODRIGUES, Rosália. **O papel da Comunicação Interna em tempos de pandemia: uma resposta à crise da Covid-19**. Revista Aprender, p. 42-49, 2021. Disponível em: <http://aprender.esep.pt/index.php/aprender/article/view/141>. Acesso em: 20 mai 2022.

ROVEDA, Ugo. **HTTPS: o que é, como funciona e por que é importante. 2018.** Disponível em: <https://kenzie.com.br/blog/https/>. Acessado em: 22 Mar 2022.

SANTOS, João Lucas Oliveira dos, FAVACHO, Kaio Eduardo Gama. **"Privacidade e proteção de dados pessoais durante a pandemia da covid-19."** (2021).

SANTOS, B. P., SILVA, L. A., CELES, C. S., BORGES NETO, J. B., PERES, B. S., VIEIRA, M. A. M., ... & LOUREIRO, A. A. (2016). **Internet das coisas: da teoria à prática**. Disponível em: <https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf>. Acesso em: 29 jun 2022.

SCHWAB, Klaus. **A QUARTA REVOLUÇÃO INDUSTRIAL**. Brasil, Edipro, 2016. Disponível em: < https://edisciplinas.usp.br/pluginfile.php/4212041/mod_folder/content/0/Schwab%20%282016%29%20A%20quarta%20revolucao%20industrial.pdf?forcedownload=1>. Acesso em: 07 fev 2022.

SEMOLA, M. **Gestão da Segurança da Informação**. Rio de Janeiro: Elsevier.RJ. Brasil, 2003. Disponível em: <http://ric-cps.eastus2.cloudapp.azure.com/handle/123456789/1079>. Acesso em: 26 jun 2022.

SILVA, Pamela De Oliveira Leal da. **ALÉM DA TRANSPARÊNCIA: a Lei Geral de Proteção de Dados Pessoais e a Accountability como mecanismo de controle e proteção de dados.** 2020. Disponível em: < https://repositorio.uniceub.br/jspui/handle/prefix/14663>. Acesso em: 04 jul 2022.

SOUSA, Angélica Silva de; OLIVEIRA, Guilherme Saramago de; ALVES, Laís Hilário. **A pesquisa bibliográfica: princípios e fundamentos.** Cadernos da FUCAMP, v. 20, n. 43, 2021. Disponível em: < https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2336>. Acesso em: 22 mar 2022.

SOUZA, Gabriela Alves Resende Rocha et al. **A cultura do cancelamento nas redes sociais: impactos e práticas em tempo de pandemia e suas consequências.** ScientiaGeneralis, v. 2, n. Supl. 1, p. 147-147, 2021. Disponível em: < http://scientiageneralis.com.br/index.php/SG/article/view/365>. Acesso em: 20 jul 2022.

SOUZA, J. B. DE; MENEGOLLA, G. C. S.; MENEGHEL, D.; PASQUETTI, D.; BARBOSA, S. DOS S. P.; GEREMIA, D. S.; MAESTRI, E. **Consulta de Enfermagem: relato de experiência sobre promoção da saúde de pessoas com Diabetes Mellitus**. Ciência, Cuidado e Saúde, v. 19, 21 jul. 2020. Disponível em: < https://periodicos.uem.br/ojs/index.php/CiencCuidSaude/article/view/48498>. Acesso em: 05 jul 2022.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas**. 6° ed.: São Paulo: Pearson Education do Brasil Ltda., 2014. ISBN 978-85-430-1450-0.

SURVEILLANCE SELF-DEFENSE**. O que eu deveria saber sobre criptografia?** Disponível em: <https://ssd.eff.org/pt-br/module/o-que-%C3%A9-criptografia>. Acesso em: 15 mar 2022.

VIANNA, E. W. & FERNANDES, J. H. (2015). C. **O Gestor da Segurança da Informação no Espaço Cibernético Governamental:** Grandes Desafios, Novos Perfis e Procedimentos. Disponível em: <https://revistas.marilia.unesp.br/index.php/bjis/article/view/5216>. Acesso em: 20 mai 2022.

VIEIRA, Débora Manke; VECCHIO, Fabrizio Bom. **Tratamento de dados em uma perspectiva da lei geral de proteção de dados durante a pandemia de Covid-19.** 2021. Disponível em: < https://iiacompliance.org/wp-content/uploads/2021/05/s4kK8ne99Zu1-447-463.pdf>. Acesso em: 02 jul 2022.

XU, M. et al. **The Fourth Industrial Revolution: Opportunities and Challenges**. International Journal of Financial Research, v. 9, n. 2, 2018. Disponível em: <http://creo.sc-celje.si/pluginfile.php/2387/mod_resource/content/1/4.1.4_01_The%20fourth%20industrial%20revolution.pdf>. Acesso em: 17 abr 2022.

YANG, Y.; WU, L.; YIN, G.; LI, L.; ZHAO, H. **A Survey on Security and Privacy Issues in Internet-of-Things**. IEEE Internet of Things Journal, v. 4, n. 5, p. 1250-1258, outubro 2017. DOI: 10.1109/JIOT.2017.2694844. Disponível em: <https://ieeexplore.ieee.org/document/7902207>. Acesso em: 02 jun 2022.