INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA

E TECNOLOGIA DO AMAPÁ – IFAP

CÂMPUS MACAPÁ

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

JOÃO LUCAS OLIVEIRA DOS SANTOS

KAIO EDUARDO GAMA FAVACHO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DURANTE A PANDEMIA DA COVID-19

MACAPÁ – AP

2021

JOÃO LUCAS OLIVEIRA DOS SANTOS

KAIO EDUARDO GAMA FAVACHO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DURANTE A PANDEMIA DA COVID-19

Trabalho de conclusão de curso apresentado ao curso superior de tecnologia em redes de computadores, do Instituto de Educação, Ciência e Tecnologia do Amapá – Ifap, como requisito avaliativo para obtenção de título de tecnólogo em redes de computadores. Orientador: Prof. Dr. Klenilmar Lopes Dias.

MACAPÁ – AP

2021

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

S237p Santos, João Lucas Oliveira dos
Privacidade e proteção de dados pessoais durante a pandemia da COVID-19 / João Lucas Oliveira dos Santos, Kaio Eduardo Gama Favacho. - Macapá, 2021.
64 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2021.

Orientador: Dr. Klenilmar Lopes Dias.

1. Proteção de dados pessoais. 2. Privacidade. 3. Pandemia da COVID-19. I. Favacho, Kaio Eduardo Gama. I. Dias, Dr. Klenilmar Lopes, orient. II. Título.

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

JOÃO LUCAS OLIVEIRA DOS SANTOS

KAIO EDUARDO GAMA FAVACHO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DURANTE A PANDEMIA DA COVID-19

Trabalho de conclusão de curso apresentado ao curso superior de tecnologia em redes de computadores, do Instituto de Educação, Ciência e Tecnologia do Amapá – Ifap, como requisito avaliativo para obtenção de título de tecnólogo em redes de computadores. Orientador: Prof. Dr. Klenilmar Lopes Dias.

BANCA EXAMINADORA

Prof.Dr. Klenilmar Lopes Dias

Prof.Me. Klessis Lopes Dias

Prof.Esp. Eonay Barbosa Gurjão

Aprovada(o) em: 25/06/2021

Nota: 10

Eu João Lucas Oliveira dos Santos dedico aos meus pais: João Batista Oliveira dos Santos e Irismar Cardoso de Oliveira.

Eu Kaio Eduardo Gama Favacho dedico aos meus pais: Keilo Favacho e Rubenita Gama.

RESUMO

O trabalho apresentado é uma pesquisa sobre a Privacidade e Proteção de Dados Pessoais Durante a Pandemia Da Covid-19, irá apresentar um referencial teórico que estará dividido em três tópicos abstratos, no primeiro, a base introdutória sobre estruturas civis na internet; no segundo a legislação; e no terceiro, meios de proteção. Este trabalho de conclusão utilizará como modo de pesquisa qualitativa, usufruindo de obras publicadas de autores e doutrinadores da área. Tem por objetivo pesquisar, meios de prevenção dos dados pessoais, no período pandêmico evitando o uso indevido, ou de forma criminosa por terceiros, levando em consideração, o alto uso da rede mundial de computadores. E trará os resultados e a discussão e conclusão de todo o levantamento bibliográfico.

Palavras-chave: Privacidade. Proteção. Dados. Pandemia.

ABSTRACT

The work presented is a research on the Privacy and Protection of Personal Data During the Covid-19 Pandemic, it will present a theoretical framework that will be divided into three abstract topics in the first introductory basis on civil structures on the internet; in the second, legilation; and in the third means of protection. This conclusion work will use as a way of qualitative research, taking advantage of published works by authors and doctrines of the area. It aims to search, means of prevention of personal data, in the pandemic period avoiding the misuse, or in a criminal way by third parties, taking into account, the high use of the world wide web. And it will bring the results and the discussion and conclusion of the entire bibliographic survey.

Keywords: Privacy. Protection. Data. Pandemic.

SUMÁRIO

1 INTRODUÇÃO

No final do ano de 2019, no mês de dezembro, no dia 31, foi descoberto por um cientista chinês, um novo agente do Coronavírus (SARS-CoV-2), que causou a COVID-19 ou popularmente chamado de Coronavírus, que por questões sanitárias e a contaminação em massa, se fez necessário adotar algumas medidas, a principal delas adotadas pelos governantes das nações foi o isolamento social. Esse isolamento, afeta diretamente nosso dia a dia, temos que adaptar nossa vida pessoal, social e profissional à vida digital, remotamente. Desta forma, levou a população a fazer mais uso da internet; passamos a trabalhar e estudar através da internet, a consumir mais entretenimento, deliverys de alimentação, e outros modais.

Com o surgimento desse vírus que para alguns é letal e para outros passa despercebido, levou-se a população mundial a fazer uso continuo e com mais frequência das redes de internet, fazendo com que o tráfego de dados fosse ainda maior, e a exposição também. Fazendo-se necessário buscar meios e medidas, que possa a vir a coibir o uso indevido desses dados e a manutenção da privacidade desses usuários.

A era tecnológica, que vive o homem, o levou a um patamar, que iniciou com uma imensa maquina, e que hoje cabe na palma da mão e lhe traz a comodidade, de ter um cartão de credito ou até grandes negociações envolvendo milhões. E pelo momento vivenciado, as pessoas voluntariamente cedem seus dados a rede, fazendo uso de seus dispositivos que estão conectados à internet, sujeitando-se ao uso por pessoas públicas, ou estatais, como por pessoas desconhecidas.

Para tanto tem que ser pesquisados, quais os meios desenvolvidos, pelos responsáveis da área para se evitar, essa invasão de privacidade e manutenção em segurança dos dados dos usuários da rede.

2 JUSTIFICATIVA

A segurança do seu computador pessoal pode ser um problema com o qual você tem lidado há muito tempo. Se você atualizar seu software antivírus, criar senhas fortes para contas online e fizer alterações regulares, poderá atender a maioria dos requisitos de segurança recomendados. Além disso, é importante lembrar que, diante da crise da Covid-19, o uso de trabalho remoto pode trazer uma série de riscos de segurança cibernética para as empresas menos compreendidas. “O CoronavÍrus não apenas mantém a saúde das pessoas sob controle, mas também é usado como isca por ciber criminosos para espalhar malwares”.

A importância deste trabalho reside no fato de que a World Wide Web ocupa uma posição de extremo destaque no cenário global e é a "casa" das empresas mais valiosas do planeta, sendo um elemento básico no dia a dia de trabalho da maioria dos residentes. O país promove a revolução democrática e é responsável pela globalização e disseminação da informação.

Entretanto, o ordenamento jurídico ainda demonstra dificuldades em lidar com as peculiaridades do mundo digital, principalmente porque o processo caótico, difundido e global da rede acarreta em transformações com muito mais velocidade do que o processo ordenado, concentrado e local da criação de normas. Sendo assim, discorrer sobre o direito fundamental à privacidade na internet não é apenas pertinente, mas é essencial para que a tutela jurisdicional seja prestada da melhor forma possível.

A Lei Geral de Proteção de Dados, por sua vez, impõe normas que irão modificar as relações entre os provedores de aplicativos da internet (como Facebook e Google) e os usuários destes serviços ou consumidores desses produtos, de forma que a análise desta legislação é de suma importância para qualquer pessoa que tenha acesso à rede. Ademais, para os provedores de aplicação de internet, há a necessidade de adaptação com relação às novas regras, que na maioria dos casos são diferentes das práticas adotadas antes da entrada em vigor da Lei Geral de Proteção de Dados. Portanto, o cumprimento da nova agência é essencial para manter o fornecimento de serviços ou produtos na rede mundial de computadores, utilizadas no período anterior à vigência da Lei Geral de Proteção de Dados, de forma que o fato de estar em conformidade com os novos institutos é essencial para

a manutenção da prestação de serviço ou fornecimento de produto no âmbito da Rede Mundial de Computadores.

3 OBJETIVOS

3.1 Geral:

Pesquisar meios para tentar se manter a privacidade e a proteção aos dados pessoais, durante a pandemia da COVID -19.

3.2 Específicos:

Tem como objetivos específicos:

- Pesquisar a historicidade da base introdutória sobre estruturas civis na internet.
- Analisar a legislação vigente.
- Apontar meios e recursos que possa manter a privacidade e a proteção dos dados pessoais do cidadão.

4 REVISÃO LITERARIA

Neste capítulo iremos ver um levantamento literário acerca do que há de atual sobre o tema em questão, com a perspectiva de um olhar atualizado sobre a problemática da pesquisa, para isso veremos primeiro o contexto histórico sobre o tema; como se iniciou o processo de criação da rede mundial de Internet, e das primeiras máquinas computacionais da história global. Em seguida faremos um apanhado geral sobre as principais leis a proteção de dados pessoais existentes e em vigor na nossa legislação brasileira, tanto como era antes da pandemia da COVID-19, assim como a mesma se encontra atualmente.

Por fim, veremos uma breve abordagem sobre as principais normas e padrões, acerca da segurança da informação, serão elas: ISO, ABNT e NBR. Tratando juntamente sobre a importância da segurança da informação para a privacidade e proteção dos dados pessoais, destrinchando seus pilares: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade.

4.1 Contexto histórico

Era 1957, quando a União Soviética lançou o primeiro satélite artificial "Sputnik" Artificial. Os americanos ficaram chocados com a notícia. A guerra fria estava chegando em seu apogeu, os Estados Unidos e a União Soviética se viam como inimigos, com a União Soviética capaz de lançar satélites para o espaço, também sendo possível lançar um míssil apontado para a América do Norte.

O presidente Dwight D. Eisenhower fundou a Agência de Projetos Avançados de Defesa (ARPA), em 1958 como uma resposta direta ao lançamento de satélites artificiais. O objetivo do ARPA é que dê aos Estados Unidos uma vantagem tecnológica sobre os outros países, que teve como parte importante de sua missão o uso da ciência da computação. Tyson acredita que o objetivo do ARPA era mudar aquela situação. A agência pediu ajuda a Bolt, Beranek e Newman (BBN) para criar uma rede de computadores.

> A rede tinha de conectar quatro computadores, cada qual acionado por um sistema operacional diferente, “localizado em pontos estratégicos, coligados por meio de redes de telecomunicações geográficas, denominadas Internet ou Inter Networking, que sobrevivesse a ataques inimigos, com a missão de

> garantir a comunicação entre as remanescentes cidades coligadas, na hipótese de uma delas vir a ser destruída por um ataque nuclear" (PAESANI, 2006, p.25)

A rede resultante deste trabalho é denominada ARPANET. A Internet não funcionava como hoje em dia e era muito diferente. E poderia nem existir. Embora existiam outros grupos trabalhando na criação de uma rede de computadores, a ARPANET era a que estava mais próxima de ser estabelecida e era a mais parecida com a Internet que temos hoje. Além disso, se não houvesse a criação da ARPANET, poderia demorar mais para a existência de uma rede de computadores, dessa forma, o objetivo era que alguém pudesse encontrar uma maneira de conectar à rede de área a um sistema mais amplo.

Na década de 1950, os computadores eram dispositivos enormes, ocupando salas inteiras, tendo apenas um pequeno poder de processamento das máquinas modernas, se comparados as da atualidade. Muitos computadores daquela época só podiam ler fitas ou cartões perfurados, e não tinha como fazer o computador funcionar na rede.

Mas foi em meados da década de 1970, mais precisamente em 1973, onde a Internet cresceu rapidamente nos EUA, que engenheiros começam a encontrar uma maneira de fazer com que a ARPANET se conecte à rede de pacotes sem fio (PRNET). A rede de pacotes de rádio passa pelo transmissor e Receptor de rádio. O computador não enviava dados pela linha telefônica, mas enviava dados pelas ondas de rádios usadas pelas linhas telefônicas. Com isso após três anos de pesquisa e testes, os engenheiros obtiveram o sucesso tão esperado.

Cada um dos primeiros quatros computadores ARPANET usavam um sistema operativo. Os designers de sistema desenvolveram um conjunto de regras gerais para que os computadores se comunicassem entre si, seguindo a rede sem degradar o sistema. Essas regras são chamadas de acordos (Protocolos), o conjunto de protocolos é denominado Protocolo de Controle de Rede (NCP). Então, em 1976, os engenheiros conseguiram conectar as duas redes com sucesso através da utilização de protocolos. No entanto, o crescimento explosivo da Internet ocorreu durante o período de pico, quando os preços da Internet começaram a se tornarem mais baratos e acessíveis. Ao longo do século 20, milhares de pessoas por décadas em diante iriam aproveitar este benefício da Internet, como forma de comunicação entre si, para trabalho, para estudos e muitos outros afins. Mas o elemento mais

importante é permitir que a Internet se torne uma ferramenta de comunicação em massa, o mundo é a World Wide Web (WWW, ou mesmo W3, ou simplesmente chamada de Web) que foi criada naquela época em 1989, sob o comando de T. Berners-Lee e R. Cailliau, no European Physics Laboratory High Energy, com sede em Genebra, que visou simplificar a forma de navegar na internet e popularizar o seu uso.

O elemento WWW compõe-se de hipertextos, ou seja, documentos cujo texto, imagem e sons são evidenciados de forma particular e podem ser relacionados com outros documentos. (PAESANI, 2006).

Sendo assim logo, algumas pessoas começaram a reconhecer que a Internet é igual à web, a Internet de Computadores e o WWW são uma forma de navegar em uma grande rede. A década de 1990 se tornou uma época de expansão da Internet. Com sua facilidade de navegar, através da Internet surgiram vários navegadores (browser), como o Internet Microsoft Explorer e Netscape Navigator. Nove anos após a criação da Key Elements (WWW), em novembro de 1998, o Pentium III era lançado, com capacidade de execução de mais de 400 milhões de operações por segundos, com mais de 9,5 milhões de transistores e velocidade acima de 500 MHz (CORRÊA,2000, p.01).

A maioria dos primeiros usuários da Internet eram funcionários do governo, membros das forças armadas, estudantes de graduação e cientistas da computação. Como era utilizada a World Wide Web, a Internet se tornou mais acessível. As universidades logo começaram a se conectar à Internet e as empresas logo em seguida também aderiram ao seu uso. Assim em 1994, o uso comercial da Internet foi realizado.

O surgimento acelerado de ISPs e portais de serviços online contribuiu para esse crescimento. A Internet estava começando a ser usada por vários segmentos de mercado social, os alunos começaram a buscar informações para pesquisas escolares; e os jovens usavam sites de jogos exclusivamente para entretenimento; as salas de chat tornaram-se o foco, para a realização de uma reunião a qualquer momento para um bate-papo virtual; o desempregado poderia encontrar uma vaga no site da agência de empregos ou enviar seu currículo por e-mail; as empresas descobriram uma maneira maravilhosa de aumentar os lucros através da Internet; o

aumento nas vendas online transformou a Internet em um verdadeiro shopping center Virtual.

Portanto, do ponto de vista técnico, em breve teremos o conceito de Internet, a saber a Internet é uma grande rede com um grande número de computadores conectados em toda a rede do planeta, cancelou todas as distâncias de tempo e lugar. Esses links vêm de lugares diferentes e podem ser de várias formas: rede telefônica, cabo e satélite. Sua proliferação é um tanto semelhante à proliferação da Internet, no entanto se dá através das redes de computadores e redes telefônicas. Assim cada computador pode conter e fornecer mediante solicitação do usuário, informações ilimitadas difíceis de obter pelo telefone por exemplo. Os computadores surgiram quando estourou a Segunda Guerra Mundial, mas foi limitado ao uso do governo, chegando assim aos tempos atuais como conhecemos e utilizamos os computadores em nossas vidas, como forma de nos conectarmos a internet, de forma social em nossos dia-a-dia.

Para resolver um tema específico, é essencial fornecer um pano de fundo histórico para melhor compreender e analisar o tema em discussão. Sua visão original e suas mudanças ao longo do tempo. Não há dúvida de que o surgimento da sociedade da informação foi o surgimento dos computadores em meados de 1939 como relata (PEREIRA, 2014):

> Para sermos mais precisos em relação a nosso objeto é possível datar a emergência dos computadores como os conhecemos hoje na década de 1950 e no contexto da guerra fria. Os primeiros computadores, fabricados como armas de inteligência a serem utilizados na guerra, eram muito grandes, posto que funcionavam por meio de válvulas. O primeiro passo em direção à miniaturização foi o desenvolvimento dos transistores, condutores de impulsos que dariam origem aos chips. Até a década de 1970 os computadores mantiveram-se restritos a governos e universidades e tinham o perfil de Mainframes. Foi neste período que começou a difusão do conceito de PC (Personal Computer), aparelhos compactos a serem usados por pessoas físicas ou empresas para executar tarefas. A partir da década de 1980 os PCs se popularizam, marcados pela queda do preço e pelo aumento de capacidade de processamento, que se amplia de forma vertiginosa até hoje. (PERERIRA, 2014)

Vale ressaltar que, no Brasil, não existe uma lei especial para trazer os direitos e obrigações dos usuários para uma época mais distante. Por meio do Código Civil Brasileiro, do Código do Consumidor e demais regulamentações disponíveis à época, as questões levantadas pelas autoridades judiciais foram tratadas de forma comum.

Barros e Flain (2016) mencionaram que o Marco Civil estabeleceu uma série de direitos no que diz respeito à proteção da privacidade e manutenção de registros de conexão, e o direito de acesso a aplicativos e dados pessoais, incluindo os direitos que os provedores devem manter. Está claramente definido no contrato como lidar com esses dados.

Lei nº 12 de dezembro de 2014, denominada Marco Civil (Constituição Brasileira da Internet) na Internet, traz inovações na área comercial em termos de ambiente tecnológico, com o objetivo de aumentar essas empresas no meio digital e estabelecer "regras" na Internet ou melhor dizer, utilizar a Internet no país, pois com o desenvolvimento da tecnologia, os padrões de proteção existentes também devem ser aprimorados. Como está na redação oficial:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede.
> [..] (BRASIL, 2014)

O Marco Civil não antecedeu todas as disputas envolvendo internet e tecnologia no Brasil. Antes dele, o judiciário havia considerado diversos casos de responsabilidade civil na internet (JESUS, 2014). Para uma melhor análise do tema em discussão, é necessário ter um panorama histórico para um melhor entendimento, tanto para definir algumas definições quanto para elencar os pontos principais.

4.2 Leis gerais sobre a proteção de dados

Hoje, a característica da sociedade é uma nova forma de organização, em que a informação é essencial para o desenvolvimento das relações sociais. Com o avanço da tecnologia, as informações são processadas e transmitidas em uma grande quantidade e velocidade, então as relações sociais são afetadas pelo fluxo de informações que supera obstáculos corpo e distância, liberdade pessoal, privacidade das pessoas, política, mercados, etc. Neste caso, a informação

desempenha um papel central na sociedade, que reorganize seus novos elementos, assim como a terra em uma sociedade agrícola, o vapor e a eletricidade da sociedade industrial e os serviços da sociedade pós-industrial.

Durante a pandemia da COVID-19, observou-se que vários países estão fazendo o uso de dados pessoais para combater a doença e buscar garantir através do acompanhamento e tratamento de pessoas infectadas, e que elas cumpram medidas de distanciamento social e restrições ao acúmulo populacional, alguns desses dados são utilizados para identificar pessoas que estiveram em contato com pessoas infectadas, assim também para fazer um gerenciamento de risco do contágio do vírus, através de testes de diagnósticos em comunidades e regiões onde se tem uma maior taxa de infecção, assim o diagnóstico é realizado e priorizado.

No Brasil, a cidade do Rio de Janeiro-RJ utiliza dados fornecidos por operadoras de telefonia para monitorar o movimento das pessoas para que a velocidade do movimento possa ser medida e comparada a movimentação de pessoas em cada área da cidade. Da mesma forma, o estado de São Paulo utiliza os dados de células, para também controlar o movimento, a medição, a cada dia, a taxa de isolamento social da população.

Pode-se verificar que o tratamento de dados pessoais é muito útil e necessário para proteger a segurança de vidas e bens. A população é “saudável”, especialmente durante a pandemia em relação a esses dados. No entanto, se não houver parâmetros e restrições, processamento de dados pode causar danos às pessoas, especialmente danos aos direitos pessoais, como personalidade, privacidade, honra, igualdade, liberdade e identidade pessoal.

Embora o LGPD não tenha entrado em vigor, o princípio que adota é, sem dúvida, o sistema jurídico brasileiro decorre da necessidade de proteger os direitos fundamentais do cidadão. Portanto, esses princípios podem e devem ser aplicados desde o início. Uma vez que os direitos fundamentais têm efeito jurídico, eles são os parâmetros para a realização dos direitos fundamentais de qualquer processamento de dados visando a manutenção da vida e saúde da população para garantir que evite ferir o direito da personalidade pessoal das pessoas em sociedade. Por isso, veremos a seguir o aparato legislativo sobre as leis de proteção de dados.

4.2.1 Regulamentação e responsabilidade civil para cidadãos digitais

O marco civil aprovado em 23 de abril de 2013, pela ex-presidente Dilma Roussef, e também a decisão em 12 de dezembro de 2014 na reunião do NET mundial realizada em São Paulo, aproveitando esta oportunidade para proteger a Internet e as questões técnicas lançam os alicerces, proporcionando assim um certo grau de segurança jurídica a essas relações. Na verdade, estamos caminhando para a globalização. O fato é que se nem todas as relações de consumo e de contrato atuais forem estabelecidas em ambientes virtuais, então haverá seus efeitos, inclusive a falta de privacidade que fará com que pessoas se tornem vulneráveis diante de cenários virtuais.

A cidadania digital é conceituada como o uso responsável do ambiente tecnológico, ou seja, diante de um ambiente virtual, o cidadão físico tem seu cidadão virtual, o que inclui direitos como o cidadão físico e deve ser tratado de forma adequada. Na Lei nº 12.965 / 14. Os artigos 3º da lei estipulam as disposições relativas à proteção da privacidade, à inviolabilidade do sigilo da informação, à privacidade pessoal dos cidadãos e à garantia da liberdade de expressão. Disposto:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Portanto, é impossível dizer que não existem regras definidas de manejo no ambiente tecnológico, como muitas pessoas geralmente chamam de “terra sem lei”, porque atualmente existe toda essa informação que rege direitos, regras e restrições. A responsabilidade civil pela troca, independentemente de a informação ser sigilosa ou não, para isso falamos em privacidade.

Os novos meios tecnológicos, a intensidade de vida e o adensamento populacional têm aproximado cada vez mais as pessoas, e cada vez mais estreita a relação entre as pessoas, o que tem gerado mais conflitos de direitos e consumo de interesses, o que tem causado divisões sociais. A resposta ao comportamento nocivo levou ao desenvolvimento de um código de conduta para o uso responsável da Internet, conforme mostrado a seguir. Deve-se observar aqui que se um terceiro usar o serviço fornecido pelo provedor do aplicativo para fins maliciosos e a vítima solicitar legalmente o fornecimento de informações após o tempo de retenção especificado pela lei, o provedor pode explicar que ele não possui mais os dados, mas não se recusou a fornecer responsabilidade civil.

4.2.2 Padrões regulamentares para uso da internet

A Lei nº 12.965 / 2014 estabeleceu os princípios, garantias, direitos e obrigações da Internet em nosso país, e apontou os direcionamentos à União, aos estados, ao Distrito Federal e aos municípios quanto ao uso da Internet no Brasil. A Internet é definida como "uma rede internacional de computadores interligados", que é "um meio de comunicação que pode trocar várias informações à escala global com um nível de interatividade sem precedentes".

As leis relevantes trouxeram-nos princípios e garantias para proteger a liberdade de expressão e comunicação; proteger a privacidade pessoal, segurança e funções de rede de forma a não entrar em conflito com outros princípios estabelecidos na lei. Atos considerados violadores de terceiros, bem como atos que resultem na divulgação de dados pessoais sem consentimento, devem ser compensados, com o objetivo de proteger a honra das pessoas neste sentido.

O acesso à Internet passou a ser uma condição dos cidadãos. Esse mandamento deve exigir que os poderes públicos e até mesmo instituições privadas com essa agenda proponham uma série de ações com responsabilidades sociais claras ” (JESUS, 2014).

A Internet, as leis digitais ou eletrônicas ainda estão em processo de formação, assim como qualquer ciência relacionada às grandes redes e à Internet. O termo direito digital é utilizado pela especialista Patrícia Peck Pinheiro, que ensinou:

O direito digital inclui a evolução do próprio direito, abrangendo todos os princípios básicos e institutos que têm sido válidos e aplicados até hoje, e introduzindo novos institutos e elementos para o pensamento jurídico em todos os campos (PINHEIRO, 2008).

Como disse Schreiber (2015, p. 4), essa visão do direito digital visa eliminar a "ideia romântica de que a Internet deve ser um espaço livre de quaisquer normas formais". O desenvolvimento será pautado pelas normas legais, pois somente em um ambiente padronizado o exercício livre pode ocorrer sem medo de abusos.

Embora a Internet tenha contribuído para as relações de trabalho, pessoais e de aprendizagem, vale ressaltar o que disse Anderson Schreiber: extremismo e radicalismo, características do individualismo em constante evolução nesses novos ambientes no fruto da comunicação, as pessoas muitas vezes caem em ataques verbais, calúnias e incitação ao ódio, que se espalharão na Internet, infringindo assim o direito da personalidade (SCHREIBER, 2015).

Nessa perspectiva, os direitos da personalidade são um "conceito inacabado" que deve ser "treinado", principalmente diante das fontes de dados geradas pelas pessoas na sociedade da informação. Sob essa premissa, será possível encontrar novas variantes dessa categoria jurídica para se adequar à proteção de dados pessoais (BIONI, 2019).

4.2.3 Lei de proteção de dados

A Lei n. º 13709/18 da Lei da Proteção Civil e Civil de 2014, nomeadamente a Lei Geral da Proteção de Dados Pessoais (LGPD), foi alterada para regulamentar a concessão e utilização de dados em ambientes virtuais. Nas últimas décadas, avanços tecnológicos extraordinários trouxeram um dos desafios mais sensíveis a aprovação da Lei Geral de Proteção de Dados Pessoais (Finalmente fez do Brasil um dos países que possuem instrumentos que protegem os direitos básicos de privacidade). Além disso, as regulamentações europeias têm forte influência neste assunto nº 13.709 / 2018. Os dados pessoais são definidos de forma ampla, tal como "informação relativa a uma pessoa singular identificada ou identificável" (SCHREIBER, 2020, p. 207), pelo que a Internet é o espaço mais livre e não

perturbado devido à falta de geografia. A fundação está sob o controle de regulamentos ou do governo, que promove a disseminação de novas formas de opressão e ódio até certo ponto.

4.2.4 Da proteção da privacidade à proteção dos dados pessoais

Hoje, é inimaginável imaginar a ideia de proteger dados pessoais não relacionados à Internet. Seu ciclo violento ocorre imediatamente através da rede e dos meios de comunicação. Além das inúmeras facilidades, esse fenômeno também faz com que as pessoas desconheçam como gerenciar esses dados, como capturá-los, como salvá-los, quem os armazena, para que uso e quando ainda podem ser acessados. Essas evidências tornam as pessoas mais necessitadas de reconhecer e fazer cumprir o direito de proteger os dados pessoais.

No entanto, antes de discutir a proteção dos dados pessoais em si, serão apresentados os princípios básicos da privacidade. (KUJAWSKI; THOMAZ, 2014, p. 677-694). Segundo Leonard (2012, p.47), o conceito de "privacidade" no ordenamento jurídico nacional é extremamente amplo, o que o torna uma "palavra" - chameleon ", capaz de manter significados diversos, esta abertura não favorecerá a implementação de políticas públicas e a resolução de certos casos concretos, pois as interpretações são muito diversas, principalmente no caso de outra norma-regra ou princípio jurídico.

A amplitude de significado pode ser atribuída ao conceito de privacidade, embora tenham encontrado algumas dificuldades na implementação de políticas públicas e na resolução de casos concretos, mostrou-se muito importante porque pode ser usado como um motivo para proteger diferentes situações - mas, no contexto comum, não encontraram proteção especial no ordenamento jurídico ativo.

4.2.5 Uma visão geral da legislação brasileira sobre a proteção de informação pessoal

O motivo pelo qual o controlador assumido presta serviços eficazes (públicos ou privados) e garante a segurança do país, da sociedade e dos cidadãos justifica a

utilização de dados pessoais. A tecnologia torna as informações pessoais mais relevantes: ajuda a torná-las úteis e reduz o custo de sua aquisição e transporte. Comparado com a vida privada, o grau de avanço tecnológico é tão grande que levou as pessoas a perceberem claramente as "deficiências do dogma tradicional" para controlar o fluxo intensivo de informações. (DONEDA, 2006, páginas 22-34).

GEDIEL e CORRÊA (2008, p.145) insistem que “a proteção dos dados pessoais é afetada por dois principais meios de pressão, característica típica da sociedade contemporânea, em que a informação constitui o elemento central do controle social e da produção de riqueza”. Estes meios de comunicação estão relacionados com o desempenho do Estado e do mercado e procuram “aumentar a quantidade e a qualidade da informação sobre os cidadãos para proteger a segurança e a saúde pública”. O mercado, portanto, atua onde esta informação tem valor econômico.

Além das questões sociopolíticas já mencionadas, há uma controvérsia de ordem prática a respeito dos instrumentos jurídicos existentes no ordenamento jurídico brasileiro que podem proteger efetivamente os dados pessoais. Quando se pensa em proteger esses dados, não é para impedir sua circulação ou seu uso, pois como afirma DONEDA (2006, p.13): o problema não é utilizá-los, mas perder completamente o controle dos dados e o objetivo de usá-los.

Portanto, é necessário enfrentar os aspectos práticos desse debate. No contexto da legislação brasileira, é necessário um esforço maior para encontrar um instrumento jurídico conducente à proteção de dados pessoais, pois o país não possui legislação específica sobre o assunto. Diante disso, a relação entre privacidade e proteção de dados pessoais é potencialmente fortalecida, pois esta é a principal forma de buscar argumentos jurídicos que possam proteger o uso irrestrito de tais dados.

4.2.6 Pioneira na proteção de marcos civis na internet

“Marco Civil da Internet (MCI) ”, lei número: 12 de dezembro de 2014, estabeleceu os princípios, garantias, direitos e obrigações dos internautas. Ao longo do processo de redação, houve intensas discussões em torno da proteção da privacidade e dos dados pessoais. Isso se deve fundamentalmente ao

esclarecimento de Edward Snowden sobre a prática de vigilância em larga escala do governo dos Estados Unidos por meio da rede mundial de computadores. A partir dessas revelações, foram confirmados os espiões do governo brasileiro e do Presidente da República, e Ronaldo Lemos (2014, p. 03) apontou isso. Tornou-se o principal motivo de distanciamento e aceleração do processo legislativo.

A criação da MCI é marcada pelas suas características inovadoras e democráticas, pois o seu design meticuloso possui uma plataforma digital que permite a cooperação de todo e qualquer cidadão interessado. Além disso, são coletadas informações geradas em determinadas redes sociais. LEMOS (2014, p. 05) acredita que o principal objetivo é “promover a liberdade de expressão, privacidade, neutralidade da rede e acesso para a Internet, a limitação da responsabilidade dos intermediários e a defesa da abertura da Internet são cruciais para a inovação. ”

4.2.7 Leis gerais sobre a proteção de dados pessoais antes da pandemia da covid-19

A pandemia é considerada uma epidemia universal. A Organização Mundial da Saúde (OMS) anunciou em 30 de janeiro de 2020 que o surto da doença causado pelo novo coronavírus (COVID-19) constitui uma emergência de saúde pública de importância internacional. Em 11 de março de 2020, a OMS listou COVID-19 como uma pandemia.

Na verdade, na pandemia, não só o Brasil, mas o mundo inteiro está mudando, seja na forma de atuação da empresa, seja no dia a dia de todos, porque antes não havia acontecido outra coisa deste tipo com um impacto tão grande globalmente. Portanto, é necessário analisar as formas como as informações pessoais são expostas. Vale ressaltar que devido à situação de pandemia no país, tanto as relações pessoais quanto de trabalho são alcançadas por meio de um ambiente tecnológico, portanto, a relação à distância com o tempo e o espaço é mais conveniente, pois não física. No entanto, todas essas tecnologias e instalações poderão reduzir a proteção dos direitos individuais até certo ponto, como direitos de imagem, direitos de privacidade e direitos de intimidade.

Diante da situação acima, as medidas Provisórias nº 959/20 adiaram os principais pontos da Lei Geral de Proteção de Dados até 13 de maio de 2021 (13.709 / 18). Entre as propostas de medidas provisórias, a única parte da lei geral de proteção de dados que ainda está em vigor diz respeito à criação da Agência Nacional de Proteção de Dados, que fiscalizará o cumprimento da lei, que entrou em vigor em 2018. Vale ressaltar que, no início de abril do ano de 2019, o Senado aprovou um projeto de lei que prorroga sua vigência até janeiro de 2021. O projeto de lei (PL 1179/20) prevê o sistema jurídico de emergência e de transição (RJET) das relações jurídicas de direito privado durante a pandemia do coronavírus (Covid-19).

Esta lei fornece regras temporárias e urgentes para a supervisão das relações jurídicas de direito privado durante a pandemia do coronavírus (Covid-19). Parágrafo único. Para os fins desta lei, a data de emissão de 20 de março de 2020 (Decreto nº 6) é considerada o prazo inicial para eventos originados da pandemia do coronavírus (Covid-19). Pessoas coletivas de direito privado a que se referem os artigos I a IV. O artigo 44 da Lei Civil estipula que, durante o período de cumprimento desta lei, devem ser observadas as restrições à realização de reuniões e encontros presenciais e observadas as normas sanitárias das autoridades locais.

A legitimidade da Lei 1179/20 é uma consequência grave da pandemia do coronavírus (Covid-19) que a economia e a sociedade brasileiras já sentiram. Em mais de cem países, a situação é a seguinte:

> O presente Projeto de Lei insere-se nesse conjunto de iniciativas que os Parlamentos estão convertendo em regras jurídicas nos últimos dias. O projeto baseia-se em alguns princípios: (1) manter a separação entre relações paritéticas (de Direito Civil e de Direito Comercial) e relações assimétricas (de Direito do Consumidor e das Locações Prediais Urbanas); (2) não alterar as leis vigentes, dado o caráter emergencial da crise gerada pela pandemia, mas apenas criar regras transitórias que, em alguns casos, suspendam temporariamente a aplicação de dispositivos dos códigos e leis extravagantes; (3) limitar-se a matérias preponderantemente privadas, deixando questões tributárias e administrativas para outros projetos; (4) as matérias de natureza falimentar e recuperacional foram deixadas no âmbito de projetos já em tramitação no Congresso Nacional (SENADO FEDERAL, PL 1179/20).

Em geral, o projeto decidiu adiar a Lei Geral de Proteção de dados por mais 18 meses para evitar onerar a empresa diante das enormes dificuldades técnicas e econômicas causadas pela pandemia. Como o parlamento tem a responsabilidade de atuar como protagonista na garantia da segurança jurídica e na proteção dos

direitos fundamentais deve entregar aos indivíduos uma lei que esclareça as regras aplicáveis a essas relações de direito privado nesta fase especial, especialmente depois que a legislação entrou em vigor e não é uma medida para tais situações sob medida (SENADO FEDERAL, PL 1179/20).

A interpretação das normas de proteção de dados é complicada, pois também de acordo com a Constituição Federal de 1988, é possível proteger dados pessoais com base na proteção de dados pessoais, ou seja, com base na proteção da privacidade pessoal e da privacidade pessoal concedida no artigo quinto, que foi confirmado no mesmo art. O artigo 21 do Código Civil garante sua inviolabilidade e a possibilidade de ação cautelar quando necessário (JUNIOR, 2020). Ainda fora da consideração de Junior (2020), é obviamente necessário fazer com que a necessária proteção de dados pessoais sensíveis (como informações relacionadas à saúde das pessoas) conflitem com o interesse público sob a premissa de responder ao interesse público. Porém, na perspectiva da coexistência de direitos, é importante proteger os interesses coletivos, e não excluir a necessária proteção das pessoas físicas.

4.3 Normas e padrões

Uma gestão da informação feita de forma eficiente em uma empresa, assegura qualidades e benefícios, como a importante proteção dos dados, assim como adquirir novos negócios de forma estratégica. Para que a empresa possa fazer uso dos benefícios de uma gestão adequada, é importante assegurar-se de que a mesma esteja sendo suprida por processos, politicas, softwares e hardwares, tendo consciência de todos os riscos e atividades do negócio, para assim solucionar todas suas necessidades. A melhor maneira de averiguar que tudo está sendo feito de maneira correta e segura, é através de normas de segurança da informação, que estabelecem regras, controles, diretrizes e protocolos da área, à serem seguidos como forma de orientação.

Normas e padrões tem como finalidade determinarem diretrizes, regras e características básicas para serviços ou atividades. Um órgão reconhecido, através de vários processos, aprova essas normas e padrões, assim, as empresas que são

capacitadas e atendem seus requisitos e exigências, tem direito de receber uma comprovação para sua empresa, como forma de excelência da mesma. Essa comprovação de excelência serve em alguns casos por exemplo, onde clientes solicitam que a instituição possua estas determinadas certificações, como forma de comprovar a excelência da empresa com a qual eles estão fechando um negócio, com a garantia de que a mesma venha prestar serviços e produtos conforme as boas práticas internacionais.

A princípio algumas normas não são obrigatórias por serem elaboradas em uma instituição privada e não pelo poder público, porém há existência de leis que promovem a obrigatoriedade de determinados padrões e normas. Fazer a utilização e aplicação das recomendações destas normas e padrões, voltadas para a segurança da informação, é um passo bastante importante, já que as mesmas garantem a excelência do setor na sua instituição. A equipe de Tecnologia da Informação pode utilizar as recomendações das normas ISO/IEC (International Organization for Standardization/International Electrotechnical Commission)) como guia, utilizando de suas boas práticas através de suas recomendações, como a gestão de riscos, gestão de segurança da informação (SGSI), monitoramentos, aplicações e revisões.

4.3.1 ISO – International organization for standardization

International Organization for Standardization, ou organização internacional de Padronização é uma organização que teve seu início em 1946, com a proposta da criação de normas que ajudem a promover boas práticas, utilizada para manter controle de qualidade de produtos e serviços de uma empresa, a ISO 9001 é umas das normas técnicas que mais se utiliza no Brasil tem como objetivo padrões de sistema de gestão e qualidade que visa procurar melhor o funcionamento possível.

4.3.2 ABNT – Associação brasileira de normas e técnicas

No brasil temos a ABNT (Associação Brasileira de Normas Técnicas) foi fundada em 28 de setembro de 1940. A ABNT por sua vez tem a função de criação

das Normas brasileiras (NBR) para produções de textos científicos, teses, monografias e principalmente na preparação de dissertações acadêmicas como o trabalho de conclusão de curso (TCC).

4.3.3 NBR – Norma brasileira

NBR (Norma Técnica brasileira) são normas técnicas que dispõem uma ampla possibilidade de implementação de um padrão em documentos, processos produtivos e procedimentos de gestão, tem por objetivo o aumento da produtividade das empresas e a melhoria da qualidade visando o aumento da competitividade do produto no mercado. Um exemplo de norma é a NBR 9050 que define padrões técnicos focados para as acessibilidades incluindo pessoas que possuem problemas de mobilidade ou portadoras de necessidades especiais, está norma deve ser seguida em projetos de prédios e locais públicos mantendo assim a inclusão social.

4.3.4 Segurança da informação e sua importância para a privacidade e proteção dos dados

Atualmente vivemos em uma sociedade de tempos modernos, cujo o acesso as informações do usuário é algo extremamente valioso, onde existe uma dependência desses dados, seja para as empresas, como forma de utilizar esses dados para oferecer uma melhor produtividade em seus produtos ou para ganhar um espaço maior no mercado; ou para os cyber-criminosos que visam a coleta destes dados dos usuários com fins de cometer dos mais diversos crimes virtuais, como o roubo dos dados, tanto de usuários “comuns” quanto de empresas valiosas mundialmente, com a finalidade da venda ou vazamento desses dados, e das brechas e vulnerabilidades encontradas através do ataque na segurança de tais empresas. Por tanto esses dados são bens altamente valiosos para as empresas que atuam no mercado no mundo que vivemos hoje, logo a proteção destes dados é uma preocupação constante, e a perda dos mesmos é uma das maiores preocupações das empresas atualmente.

Mas esta preocupação não pode caber somente as empresas, é indispensável que o usuário “comum” também tenha ciência de que ele é a principal causa de todo esse processo. Todos os dias surgem novas ameaças cibernéticas; nos noticiários de telecomunicações, seja na internet, através de blogs, sites ou redes sociais, ou por meio de um canal aberto de televisão é comum vermos constantemente noticiários de ameaças e ataques de hackers a grandes empresas e seus valiosos dados, mas o que não é comum de pensarmos e refletirmos, é que normalmente uma grande parcela de “culpa”, é mérito do usuário, já que é o usuário e suas ações não medidas durante a utilização da internet e seus meios de utilização, através de computadores e até mesmo dispositivos móveis, que facilitam e dão brechas para o hacker invadir a rede de uma empresa e assim conseguir comprometer o seu sistema e ter acesso aos seus dados, podendo assim causar prejuízos a essas empresas, isso ocorre mediante as ações do usuários, ou seja, neste caso, do funcionário da empresa, que muitas vezes não tem o conhecimento devido das consequências dos resultados que suas ações incapacitadas podem ocasionar, seja por falta de um treinamento mais adequado e capacitado ou talvez por falta de comprometimento do mesmo, com a utilização indevida dos recursos de seu local de trabalho.

Temos o dever de cuidar e fazer um bom uso, dos meios computacionais que utilizamos diariamente em nossos locais de trabalhos, seja ele uma empresa grande ou pequena, seja na faculdade ou no conforto de sua residência, ou até mesmo na palma da sua mão, como usuários é nossa obrigação zelar com boas práticas de usos os mesmos. É preciso se ter em mente que a internet é um parque de diversão para os criminosos virtuais que nela habitam, e que nela se encontram riscos presentes estabelecidos diariamente, com o grande aumento nos números de crimes e ataques cibernéticos, as empresas precisam cada vez mais se capacitar e capacitarem seus funcionários e usuários para lidarem com as consequências originadas a partir do mau uso desses recursos, é preciso educar os seus usuários sobre os riscos e suas consequências que podem trazer. É importante que tenhamos como ser humano a consciência de que nem todas as nossas ações desrespeita somente a nós mesmos, e que muitas vezes os impactos gerados por elas, podem afetar e comprometer o ambiente e as pessoas ao nosso redor. Por isso seja no seu ambiente de trabalho ou no seu lar familiar, é imprescindível ter em

mente os perigos ao utilizarmos a internet de forma livre e espontânea, sem ter um senso, com a segurança dos nossos dados nela contidas.

4.3.5 Os pilares da segurança da informação: CIDAL

De forma breve, segundo as boas práticas ITIL (Information Technology Infrastructure Library), normas ISO 27000 e também de gestão da Segurança da Informação, a mesma é composta basicamente por três pilares principais que juntos formam os principais critérios de segurança da informação, mas conhecidos hoje como “CID”, que são eles: Confidencialidade, Integridade e Disponibilidade, é importante lembrarmos que quando falamos desse tríplice da segurança da informação, temos que também citar outros dois critérios de segurança que complementam os três pilares, estamos falando dos princípios de: Autenticidade e Legalidade.

Confidencialidade

Quando se é falado na segurança de uma informação, primeiramente deve-se ter em mente que é preciso se ter a confidencialidade de que a propriedade dessa informação não seja disponível e nem esteja esclarecida/revelada, a pessoas, usuários, empresas, processos ou entidades não autorizadas. A confidencialidade tem ligação direta com a privacidade das informações, dos dados, seja esses dados de uma organização, entidade, ou de um usuário doméstico, isto na verdade tem a ver com as ações decididas e consequentemente tomadas pelo usuário para realizar a utilização de forma segura das informações críticas e confidenciais, para que as mesmas, não sejam vazadas, roubadas, disponibilizadas ou acessadas por criminosos virtuais, através de meios não autorizados, como por meio de ataques ou espionagens aos sistemas organizacionais que contém essas informações sigilosas e confidenciais.

Integridade

Integridade equivale a corresponder de forma a preservar com exatidão, consistência, precisão, e completeza as informações que fazem parte da empresa, durante o período dos processos ou de sua vida útil, no sistema da empresa a qual elas correspondem e fazem parte. É indispensável que os dados sejam armazenados, repassados ou circulem, em sua mesma forma originaria que foi criado, ou seja, de uma tal forma que não venha a ter interferências ou mudanças externas indevidas e não autorizadas, pois com isto pode haver o comprometimento dos dados, podendo o mesmo ser corrompido ou até mesmo danificado. Para que os sistemas possam operar de forma correta é importante manter a integridade dos dados, para que se tenha um sistema trabalhando com os dados adequados. A comunicação interna e externa em uma empresa deve ser de forma segura e clara, onde não ocorra o comprometimento da mesma, por isso é de extrema importância o cuidado na troca de mensagens, orientações e instruções entre profissionais e departamentos aos seus destinatários, onde deve ocorrer a preservação e mantimento dos dados enviados da mesma forma que os mesmos foram recebidos, assim não comprometendo a comunicação de uma forma geral, com isso, ajudando a evitar falhas nas execuções dos afazeres no local, assim como o não desgaste entre as pessoas de equipes diferentes na empresa, dentre outros problemas agravantes.

Disponibilidade

Disponibilidade busca a qualidade de estar disponível quando necessário independente do momento ou ocasião. O pilar que visa a importância e a necessidade de sempre está acessível ao usuário os dados relacionados a uma empresa, porém, ainda sim respeitando o pilar de confidencialidade. Para que tenhamos sempre este pilar funcional devemos fazer planos de manutenção para a prevenção de que não ocorra a quebra do mesmo, sempre verificando funcionalidade de equipamentos de infraestrutura até mesmo a segurança das salas localizadas os servidores, deve-se garantir a estabilidade e desempenho de software a serem utilizados, fazendo correção de erros e evitar conflitos, e até mesmo a

utilização de equipamentos para contornar ocasiões não esperadas, como: queda de energia com nobreaks/ geradores ou mal funcionamento do link de comunicação com um ou mais links secundários para contornar o ocorrido.

Autenticidade

Este pilar tem a função de garantir que os dados devem manter a informação do seu local de origem e usuário que está alterando ou enviando, e não devem ser modificadas estas informações, e visa dar acesso e poder de alteração de dados somente para aquele que seja por alguém autorizado. Requer que haja a confirmação para que saiba se realmente é a pessoa que está sendo apresentada, de ambos usuários (emissor e receptor), um exemplo de verificação de autenticidades que podem ser utilizadas são a implementação de senhas, tokens ou até biometria.

Legalidade

No pilar da legalidade, temos como objetivo principal, a garantia de que as informações e o uso da tecnologia computacional e suas comunicações, sejam utilizados e produzidos seguindo e respeitando a legislação vigente do seu país ou local. Por isso se faz importante e necessário a aplicação de uma boa Política de Segurança, para garantir que todos os processos ligados à informação dentro de uma empresa, estejam sendo produzidos de acordo com as leis. Possuir o conteúdo devidamente adequado à legislação é de extrema importância, já que em agosto do ano de 2020 entrou em vigor a nova Lei Geral de Proteção de Dados Pessoais (lei nº 13.709), na qual se exige um rigor maior das empresas de forma geral, logo evitando também averiguações ou que ocorram impedimentos operacionais por meio de órgãos fiscalizadores e afins.

5 RISCOS E BOAS PRÁTICAS PARA A PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS

Neste capítulo iremos abordar os principais riscos encontrados diariamente em nosso cotidiano no uso da Internet, em nossos dispositivos, sejam eles computadores, notebooks, ou até mesmo dispositivos móveis, como nossos aparelhos celulares. Estamos sempre propensos a esses riscos na rede, seja em nosso lar doméstico (casa), ou em nosso ambiente de trabalho (instituição); por isso é de suma importância falarmos sobre eles, e termos em mente as principais causas e consequências dos mesmos.

Em seguida veremos de forma detalhada, uma série de recomendações/sugestões, a serem seguidas pelo usuário, através de boas práticas para a privacidade e proteção de seus dados pessoais, com o objetivo de evitar uma série de crimes virtuais praticados por cyber criminosos através dos meios eletrônicos, que tem como alvo nossos dados pessoais na rede, com o intuito de roubar os mesmos, de formas ilegais e sem autorização.

Para isso abordaremos acerca dos principais riscos encontrados, e em seguida as principais boas práticas para cada tipo de risco, que serão eles: Vírus digital, Antivírus, Firewall, O não uso de softwares piratas, Senhas, E-mails, O uso de recursos computacionais em instituições, Backups, Dispositivos móveis, Redes sociais e Engenharia social. Por fim, veremos de forma resumida, essas principais boas práticas sugeridas para o usuário.

5.1 Vírus digital

Assim como o vírus biológico da COVID-19, que o mundo vem enfrentando nos últimos anos, que tem como característica, ser um micro-organismo biológico que tem como poder, infectar um sistema e outros organismos, criando cópias de si próprio como forma de “ataque”, por analogia, o vírus digital utiliza do mesmo princípio, o vírus digital é um programa malicioso que tem como habilidade principal, infectar o sistema computacional, ele age de forma criando cópias de si mesmo, para espalhar-se em outras máquinas, e essa propagação pode ocorrer de vários

tipos de meios, como por exemplo, o meio principal e de maior foco desses tipos de arquivos maliciosos: a rede do local, podendo assim afetar outros computadores que utilizam e fazem parte desta mesma rede.

De forma técnica um vírus computacional é uma forma de programa com códigos maliciosos, com intuito de alterar a forma do funcionamento de um computador e infectar outros computadores se distribuindo na rede dos mesmos. Quando se fala em proteção de dados, a primeira coisa em que pensamos, é sobre vírus de computadores, este tipo de vírus atua principalmente se anexando de forma sigilosa em documentos ou programas, para assim então poder executar seu código, por isso a principal recomendação é que:

- Se tenha sempre na máquina de trabalho (ex: computadores e notebooks) ou de uso pessoal (ex: smartphones e tablets), a utilização de um software antivírus e de um firewall.

5.2 Antivírus

Os softwares denominados antivírus, tem a função de fazer buscas e varreduras na máquina ou dispositivo em que ele é instalado e executado, o intuito desta varredura é procurar pela existência de vírus na máquina, esses vírus podem ser conhecidos e detectados mais fáceis através do banco de dados de informações que o antivírus carrega consigo para utilizar nesta busca, mas como sabemos os vírus se propagam rapidamente se não forem neutralizados assim que detectados, portanto a criação e propagação de novos tipos e formas de vírus existem diariamente na internet, com isso o software antivírus tem o importante papel também, de tentar procurar por novos vírus desconhecidos, utilizando assim de outras técnicas.

Algumas recomendações a serem seguidas:

- Sempre manter o software antivírus ativo e em execução, na máquina ou dispositivo utilizado, seja o mesmo para uso pessoal (uso doméstico) ou profissional (uso no local de trabalho);

- Sempre manter o seu software antivírus atualizado, pois assim ele estará com seu banco de dados sempre o mais atualizado e recente possível, e com novas funcionalidades e técnicas de detecção e remoção dos vírus, podendo ter assim uma melhor eficácia na proteção e neutralização contra novos vírus que virá a surgirem (alguns softwares de antivírus já vem com esta funcionalidade habilitada de forma automática, é importante que mesmo assim verifique manualmente.);

- Caso perceba acontecimentos ou eventos incomuns dos característicos em sua máquina, como programas não sendo reconhecidos, arquivos abrindo por conta própria/sozinhos, lentidão ou propagandas no sistema, procure imediatamente um técnico adequado da área de informática, para o mesmo fazer uma averiguação em sua máquina;

- Não relaxar em relação a vulnerabilidade de seu computador, assim como de seus outros dispositivos, não é porque um aparelho está livre de vírus maliciosos, que todos os outros estarão também. Sempre reforce repetidas vezes durante a semana o processo de verificação nos seus dispositivos, tanto em computadores como também nos dispositivos móveis;

- Ter cuidado com os dispositivos/mídias inseridos no computador, por você ou por outros usuários que venham a utilizar também os seus dispositivos, pois não se sabe a procedência de origem por onde essas mídias estiveram conectadas antes, podendo assim trazer eventuais riscos a sua máquina. Por isso se faz importante a verificação por vírus através do software antivírus, nessas mídias removíveis, sempre que conectadas ao seu computador;

- Caso ocorra uma situação em que o vírus foi detectado, é imprescindível que ele seja removido/eliminado o mais rápido possível, imediatamente, suspenda o uso da máquina, e remova o cabo de rede da mesma, para assim evitar a propagação do vírus nas outras máquinas da mesma rede

na qual ela faz parte, e em seguida comunicar o ocorrido imediatamente a um profissional técnico em informática para lhe auxiliar;

5.3 Firewall

A palavra firewall tem como significado: parede-de-fogo, em termos técnicos na informática, o firewall serve para fazer a proteção contra a transmissão de dados maliciosos ou dados que não foram autorizados, ou seja, dados que não tem a devida permissão, entre uma rede e outra. Existem alguns tipos de firewalls assim como várias formas e métodos de configura-los, eles podem ser usados por exemplo atuando na rede de uma organização/empresa, ou também podem ser usados de forma alternativa pessoal, fazendo a proteção do equipamento do usuário em si, de forma individual, podendo assim controlar, monitorar ou bloquear os acessos, os recursos, as conexões e tráfegos no sistema, criando e gerando logs (registros) de todos e eventuais acessos ao sistema.

Enganasse os usuários que acham que suas máquinas computacionais não sejam alvos interessantes suficiente, para que sejam atacadas e invadidas por criminosos virtuais (hackers), é aí que geralmente ocorre um erro, pois é justamente esse tipo de máquina que os criminosos virtuais buscam ter acesso, pois tecnicamente a máquina de um usuário “comum”, ou uma máquina que talvez não tenha arquivos e dados tão interessantes na rede, geralmente tem uma segurança inferior ou menor na rede, ou seja, é um alvo fácil para o hacker, o invasor pode usar esse tipo de máquina como escada na rede, e assim conseguir ter acesso e invadir outras máquinas mais importantes, assim conseguindo se mascarar na rede e executar um ataque de forma mais simples. Uma vez que o invasor se infiltra na máquina de um usuário pode também conseguir obter informações e dados confidenciais e sigilosos, registros bancários, ou números de cartões de créditos, roubando, sequestrando ou vazando os mesmos, e usar extorsão para que seja devolvido esses dados ao usuário ou empresa proprietária dos mesmos.

Por isso é importante a implementação, configuração e uso de um bom firewall, seja na rede ou também de forma individual em cada máquina:

- A empresa Microsoft, oferece um firewall nativo, em seu sistema operacional (Windows) que normalmente é habilitado em sua instalação, mas hoje no vasto mercado, existem outros produtos disponíveis, produtos estes mais robustos e com maiores possibilidades, mas que consequentemente requerem maior conhecimento para a configuração do mesmo.

Seguem algumas funcionalidades de um Firewall:

- Fazer o bloqueio de conexões suspeitas e que gerem algum risco;
- Dificultar o hacker invasor de identificar o computador na Internet, ocultando o mesmo;
- Bloquear o envio de informações confidenciais sem o conhecimento do usuário;
- Bloquear anúncios na Web, através do uso de navegadores;
- Evitar e inibir mensagens enviadas de forma automática por e-mails;
- Estipular/definir, os programas que poderão ser conectados de forma segura à Internet e
- Evitar ataques da Internet, por meio de bloqueio.

5.4 O não uso de softwares piratas

O uso e instalação de softwares piratas em nossos dispositivos, na verdade podem abrir brechas e facilitar a entrada do perigo, como se tivéssemos convidando-os para entrar em nossos aparelhos. A instalação e uso de softwares piratas não apenas é sobre o uso não autorizado do mesmo, sem ter adquirido de forma legal e justa, mas por serem softwares que não são devidamente e legalmente licenciados,

logo, eles são produtos que não possuem suporte, estão mais expostos a bugs e vulnerabilidades que podem ser exploradas e comprometer assim, o funcionamento devido do sistema, em outras palavras, o bom funcionamento do sistema.

Esses softwares normalmente têm alterações feitas no seu código-fonte especialmente feitas para quebrar as proteções contra a pirataria, e existem muitos casos em que estes códigos costumam ser modificados e adicionados mecanismos com o objetivo de permitir o acesso indevido e não autorizado em sua máquina por invasores, criminosos virtuais (hackers). Ou seja, o uso ilegal desses tipos de softwares, põe em risco o seu computador, e compromete a sua segurança, de seus dados, e em questão de passos as outras máquinas conectadas na mesma rede que a sua.

Entende-se que softwares piratas podem conter falhas e brechas vulneráveis propositalmente, que podem ser exploradas e aproveitadas pelos hackers, por isso é de extrema importância adquirir de forma legal e correta a licença de um software e nunca fazer uso de softwares piratas, seja na sua casa ou local de trabalho. Quando se adquire de forma legal um software você tem o suporte e aparato da empresa que disponibiliza o produto, tendo disponível correções e novos recursos adicionados a cada atualização da versão do software.

Recomendações sugeridas para o usuário seguir:

- Jamais fazer a instalação e uso de softwares piratas, pois como explicado, os mesmos podem permitir o acesso de forma remota aos dispositivos computacionais do usuário, através de seus códigos-fonte maliciosos, podendo assim, então deixar vulnerável e com sérios riscos de comprometimento da máquina e de todas as outras que estiverem conectadas a mesma rede;

- Sempre comprar de forma legal, as licenças e produtos de softwares que tem sua utilização paga, assim o mantendo sempre atualizado e obtendo um suporte e aparato total, na utilização do produto da empresa fabricante do mesmo;

- Instalar softwares gratuitos disponibilizados na Internet, somente se os mesmos forem disponibilizados de fontes confiáveis, por exemplo efetuar o download do software sempre do site do desenvolvedor/fabricante;

- Caso esteja utilizando a máquina do seu local de trabalho, é importante sempre verificar com o técnico de informática responsável no local, a autorização, antes de instalar qualquer software;

- Sempre que possível, é preferível utilizar as versões web de aplicativos ao invés de versões executáveis;

- Não fazer uso de softwares de Seeds (distribuição) P2P, como o uTorrent ou BitTorrent. Pois estes tipos de softwares possibilitam ao usuário fazer o compartilhamento de arquivos e dados com centenas de outros usuários, esses softwares têm como característica abrir portas/falhas para invasores, e eventualmente está espalhando arquivos contaminados para outros usuários, além é claro de quebrar direitos autorais;

- Ser criterioso com os softwares que instala no computador, ler os termos de uso e prestar atenção ao aceitar, ou clicar em caixas de seleção, com frases do tipo: “sim, eu aceito e estou ciente dos riscos. ”;

- Tomar o devido cuidado com softwares que exibem propagandas na tela de forma abusiva. Caso clique nelas, provavelmente será redirecionado para efetuar o download de um software invasor malicioso.

5.5 Senhas

Senhas são chaves de segurança, que disponibiliza o acesso ao usuário e proprietário da chave, à algum serviço, funcionando como um meio de autenticação de segurança, que sem a senha correta, o mesmo seria inacessível pelo o usuário. As senhas são formadas por um conjunto de caracteres, sejam eles letras minúsculas, maiúsculas, numéricos ou ainda caracteres especiais. A senha tem o

objetivo de assegurar o processo de verificação de sua identidade como proprietário de uma conta, ou serviço, por exemplo, usamos senhas para desbloquearmos o acesso ao nosso aparelho celular, nos computadores, notebooks, tablets, e também para acessar serviços na Internet, como: nosso e-mail ou contas de redes sociais (Facebook, Instagram, Twitter e etc.).

Senhas são uma questão importante, cada usuário é unicamente responsável pelas senhas de contas e serviços que administra, o cuidado com o compartilhamento destas senhas é de extrema importância, como usuário devemos compreender que:

- O usuário proprietário da senha é o único responsável pelas contas que ele administra, ao compartilha-la com terceiros, em caso de mau uso ou invasão, o total e único responsável a arcar com as consequências será o mesmo. A responsabilidade não é terceirizada como a senha;

- Quando compartilhamos nossas senhas, o risco de comprometimento ou invasão da mesma, é maior;

- E-mails no qual o autor se passa por um administrador solicitando sua senha, tem como objetivo obter o acesso a sua conta, para uso de fins maliciosos da mesma. Administradores nunca deverão fazer a solicitação de senhas através de e-mails;

- Nunca se deixe ser induzido por sites falsos com aparência de sites famosos/grandes (legítimos), pedindo para preencher formulários com seus dados e senhas;

- Faça o uso de senhas difíceis de serem quebradas ou descobertas, é algo simples mais muito eficaz, geralmente a maioria das pessoas criam senhas de fácil memorização, como: data de aniversário, idade, primeiro ou último nome, nome do companheiro, local onde trabalha, cidade onde mora, comida preferida, ou até mesmo número de identidade e CPF, afim de facilitar o uso.

Esse tipo de senha deve ser evitado, pois tem ligação direta a dados do usuário, facilitando assim o acesso a sua máquina;

- Uma senha forte e ideal, deve ser totalmente aleatória em relação a dados do usuário, e conter diferentes tipos de caracteres, tais como: letras maiúsculas, letras minúsculas, números e ainda caracteres especiais. Exemplo de uma senha ideal: 5audaded4c4s4_v3rm3lh@!;

- Alterar com frequência suas senhas, pois assim a segurança das mesmas estarão sempre sendo reforçada.

- Manter as senhas em local seguro e com acesso restrito a demais usuários.

5.6 E-mails

Ao passar dos tempos, os serviços de e-mails cada vez mais tornaram-se presente e necessário em nossas vidas, como usuário e como pessoa, é por lá que gerenciamos dezenas de mensagens em forma de e-mail diariamente, sejam elas sobre trabalho ou de fins pessoal. São dezenas de e-mails em nossas caixas de mensagens por dia, logo, é importante sempre estarmos em alerta sobre esses e-mails recebidos, filtrando tudo que é recebido. Pois existem e-mails com fins maliciosos, que não são explícitos, podendo se passar por administradores de sistemas ou por falsos avisos de segurança, que tem o objetivo de roubar seus dados, solicitando os mesmos através do e-mail.

Por isso é importante o cuidado diário com os e-mails recebidos, muitos têm a presença de links redirecionáveis quando clicados, se passando por promoções ou propagandas de marcas ou empresas conhecidas no mercado, mas que na verdade são hackers querendo seduzir o usuário, com alguma “oferta imperdível” ou “promoção”, com o intuito final do usuário clicar no link anexado no e-mail recebido, correndo assim o risco de fazer o download e instalação de um programa malicioso no seu dispositivo, para invadir sua máquina e roubar seus dados pessoais, como: cartões de créditos, contas bancarias, senhas, entre outros.

Veja algumas recomendações de boas práticas, no uso de e-mails:

- Sempre verificar e confirmar a procedência do e-mail recebido;

- Nunca fazer a instalação de softwares, programas ou aplicativos anexados em e-mails. Em casos específicos em que precise realmente baixa-los, é altamente recomendado que o mesmo passe por uma verificação em seu software antivírus, antes de serem executados em sua máquina.

- E-mails que contenham links falsos, para sites de órgãos governamentais ou se passando por uma empresa conhecida, devem ser excluídos pelo o usuário imediatamente, depois de verificado sua não autenticidade;

- Não clicar em links redirecionáveis anexados em e-mails, antes de verificar sua veracidade.

- Sempre desconfiar de e-mails recebidos se passando por falsos avisos de segurança, ou e-mails que solicitem seus dados pessoais.

- Criar o hábito de sempre filtrar seus e-mails recebidos, verificar o que é fralde e encaminhar para sua caixa de SPAM, e lembrar de sempre esvazia-la.

- Sempre fazer logout (se desconectar) de sua conta de e-mail, depois que utilizada, mesmo se a utilização da mesma tenha sido feita em seus dispositivos pessoais, muito menos caso tenha sido utilizada em computadores públicos ou de outras pessoas.

5.7 O uso de recursos computacionais em instituições

Novas ameaças cibernéticas surgem a todo momento, é fato que empresas/instituições são os principais alvos de criminosos virtuais (hackers), que tem o objetivo de invadi-las, para roubar dados, e praticar outros tipos de crimes virtuais. No entanto, diferente do que muitas pessoas pensam, estáticas mostram

que o usuário é a causa principal do comprometimento dos sistemas de informação nas instituições, por conta de suas ações como usuário, que muitas das vezes podem ser falhas, e afetar não somente o usuário em si, mas a instituição de modo geral, deixando-as vulneráveis e suscetíveis a ataques virtuais.

Essas ações deficientes por parte do usuário, pode ser atribuída a alguns fatores, como a falta de treinamento e de comprometimento, quando não há conhecimento das consequências que suas indevidas e despreparadas ações podem vir causar ao sistema da instituição, devido ao mau uso, de forma irresponsável dos recursos disponibilizados pela mesma.

O zelo e o bom uso dos recursos computacionais, disponibilizados para o uso por nossas instituições, é dever nosso, como usuário. É importante ter a consciência dos riscos e de suas consequências presentes no mau uso destes recursos no ambiente institucional.

Algumas recomendações de boas práticas no uso dos recursos computacionais em instituições:

- Sempre que possível, evitar a utilização da máquina de trabalho, para objetivos de uso particulares/pessoais;

- Mantenha sua privacidade como usuário, ao terminar de utilizar sua estação de trabalho, não deixe documentos ou arquivos pessoais abertos, e nem armazenados na mesma, pois outras pessoas no local, podem ter acesso ao computador;

- Não fazer consumo da Internet do local de trabalho para fins pessoais, seja para assistir vídeos online ou até mesmo para baixar arquivos. Além do consumo de espaço em disco e o uso de banda da internet do local, os arquivos baixados podem estar infectados por vírus/malware, e deixar o sistema do local vulnerável e comprometido, prejudicando não somente você, mas também, os demais usuários na mesma rede;

- Se possível evite o uso, assim como o compartilhamento, de mídias graváveis removíveis, como pendrives e cartões de memórias (SD), pois ocorre o risco dos mesmos, voltarem para você contaminados por vírus maliciosos;

- O uso de e-mails corporativos deve ser feito somente para atividades que sejam voltadas e fazem parte das funções da corporação/instituição. Utilize do e-mail pessoal, para fins particulares;

- Você representa sua instituição, então zele pela imagem da mesma, não compartilhe correntes e notícias falsas (fakes news), através da sua conta de e-mail de uso organizacional, antes de verificar se sua fonte é verídica;

- O mesmo vale para o compartilhamento de informações e dados confidencias restritos a instituição;

- Sempre utilizar um software antivírus na sua máquina de trabalho e

- Nunca instalar programas e aplicativos piratas e de procedências duvidosas;

- É necessário o uso de bom senso, caso tenha dúvida sobre alguma medida que pretende tomar, como por exemplo, a instalação de um software baixado da web, solicite o auxílio de um membro da equipe de informática responsável no local;

- Nunca fornecer para terceiros: senhas ou dados que comprometam a segurança da instituição e suas informações privadas;

- Caso ocorra algum incidente de segurança, acione imediatamente o setor responsável pela segurança da informação presente na instituição, para que os mesmos tomem as medidas cabíveis para solucionar este tipo de problema da melhor forma possível;

5.8 Backups

Quando se fala em segurança de dados, ouvimos bastante sobre o termo americano chamado de Backup, que traduzindo significa “cópia de segurança”, que pode ser entendida como a criação e armazenamento de uma ou mais cópias de arquivos/dados ou informações digitais importantes, seja para uma empresa ou para um usuário doméstico. A política de backup se aplicada com regularidade, é de extrema importância, pois através do backup é possível executar a restauração desses dados importantes, caso os arquivos e dados originais sejam perdidos ou excluídos, seja por problemas de software ou de hardware.

Os dados confidencias de empresas, assim como os dados pessoais de usuários, são informações altamente valiosas no “mercado negro” dos hackers, e acabam virando alvo destes tipos de criminosos virtuais. Por isso hoje em dia é tão importante a aplicação de uma boa política de proteção de dados e de backups dos mesmos, aplicadas nessas empresas. Um ataque bastante usado por esses criminosos á bancos de dados de empresas, são os chamados Ransomwares, que se trata de um tipo de Malware, que tem como objetivo infectar o sistema, e sequestrar dados importantes e sigilosos de empresas, e que em seguida é feito um pedido de resgate em dinheiro (valores altíssimos), para que a empresa vitima tenha o acesso restaurado aos seus dados roubados de volta. Caso o pagamento não ocorra, a mesma pode ter seus dados perdidos ou excluídos por esses criminosos.

Como já citado neste trabalho anteriormente, a melhor precaução são o conjunto de boas práticas e recomendações, especialmente neste tipo de caso o hábito de fazer backups dos dados regulamente, para que caso ocorra alguma situação com seus dados, seja por invasões de hackers ou até mesmo por problemas de software ou hardware, os dados tenham uma cópia de segurança devidamente feita e armazenada, pronta para efetuar a restauração dos mesmos.

Boas práticas a seguir sobre backups:

- Backups devem virar rotina no seu dia-a-dia como usuário;

- Sempre lembrar-se de fazer backups dos dados com frequência regular, sejam eles corporativos ou pessoais(Ex: contatos, documentos, e-mails, etc.);

- Lembrar periodicamente de checar, se o backup foi efetuado corretamente, para caso seja necessário o uso futuro das informações (dados) guardadas. Garantindo assim a recuperação/restauração das mesmas;

- Sempre fazer o backup de todos os arquivos de dados, tendo vários conjuntos diferentes de backups, para caso perca um backup, ainda sim tenha uma cópia de segurança do mesmo;

- Estabelecer e efetuar periodicamente uma rotação de armazenamento dos backups, em nuvem ou em mídias externas.

5.9 Dispositivos móveis

O avanço tecnológico acontece de forma muito rápida, assim como a sua popularização. Hoje através do avanço tecnológico, somos capazes de carregarmos no bolso um smartphone (aparelho celular), com capacidade superior à de computadores que ocupavam salas inteiras nos primórdios computacionais. Atualmente esses dispositivos, tem ótimas configurações de hardwares, como processadores e memórias de altas capacidades, fora suas várias opções de conectividades, e sua mobilidade, possuindo todo esse poder remoto na palma da sua mão, podendo levar consigo a vários lugares.

A segurança em relação a dispositivos móveis, fica cada vez mais evidente e relevante. Já é comum vermos ameaças como vírus maliciosos, e softwares com fins criminosos, circulando e se proliferando entre os dispositivos móveis, de forma parecida como ocorre em computadores e notebooks hoje. Criminosos virtuais, de fato destinam-se também a ataques a esses dispositivos móveis, atualmente, com os mesmos objetivos, o roubo de dados e informações pessoais dos usuários, feito através de monitoração e controle remoto desses dispositivos, observando o crescente e veloz aumento de usuários fazendo o uso intenso diariamente dos mesmos.

Assim, a segurança nos dispositivos móveis se tornou parte do cotidiano e preocupação diária das organizações voltadas para a área de segurança de dados,

da mesma forma que computadores e notebooks, foi percebido o risco também, na utilização dos dispositivos móveis. Hoje os dispositivos móveis são considerados também ferramentas de trabalho, onde deve-se conter segurança na utilização, e boas práticas de uso por parte do usuário. Assim como nos dispositivos computacionais, nos dispositivos móveis o cuidado deve ser o mesmo:

- Fazer a instalação de aplicativos somente de fontes confiáveis;

- Preferencialmente instalar aplicativos somente da loja oficial de aplicativos do seu sistema móvel, como a Google Play Store (sistema android) e a Apple Store (sistema IOS), já que todos aplicativos contidos nelas, passam por uma série de requisitos, dentre eles requisitos de segurança, para estarem aptos de sua regular disponibilização, nessas lojas oficiais;

- Instalar e habilitar um aplicativo antivírus móvel em seu aparelho;

- Manter o devido cuidado com aplicativos que exibem de forma abusiva, anúncios na tela do seu smartphone;

- Sempre verificar as permissões que você irá fornecer aos novos aplicativos instalados. Por exemplo: um jogo de dama não necessita do uso da câmera do seu aparelho celular para funcionar, logo não precisa da permissão da mesma;

- Cuidado com o fornecimento da sua localização, habilite-a somente em caso de uso, lembre-se de desabilita-la sempre que chegar na sua casa por exemplo, e

- Faça o mesmo com as tecnologias Bluetooth e NFC quando não forem usadas por você, pois as mesmas podem fornecer acesso ao seu dispositivo móvel;

- Utilizar meios de autenticação para uso, no seu aparelho móvel, através de bloqueios de tela como senhas, PINs e biometria digital (se disponível no modelo do seu aparelho);

- Evitar o uso de reconhecimento facial para desbloquear o acesso ao seu aparelho celular, pois o mesmo ainda pode ser falho. A casos em que utilizado uma foto sua ou de seu irmão gêmeo, o desbloqueio é possível de ser efetuado;

- Evitar deixar salvo dados pessoais como: números de cartões de créditos, números de contas bancarias ou endereços, como forma de preenchimento automático, ou de fácil acesso;

- Deixe sempre dados de contato para emergência salvo, caso você perca seu aparelho, e alguém o ache, com a intenção de lhe devolver;

- Sempre que disponível mantenha seu smartphone com a versão do sistema operacional o mais recente possível, disponibilizado pela fabricante do aparelho, assim como os patchs de segurança mensais disponibilizados pela mesma;

- Fazer regulamente backup de seus dados, na nuvem ou em um computador de sua posse.

5.10 Redes sociais

A facilidade ao acesso e utilização das redes sociais, tomou uma proporção grandiosa, tanto que nos dias atuais, o uso das redes sociais se estendeu até mesmo para o trabalho, já que nelas “habitam” uma enorme quantidade de pessoas (usuários). Muitas informações importantes em forma de mensagens, estão sendo transmitidas através dessas redes sociais, por meio de plataformas como o Facebook, WhatsApp e Instagram, dentre outras, seja por meio de dispositivos

computacionais ou por dispositivos móveis (devido seu fácil acesso e sua fácil locomoção, podendo levar consigo a qualquer lugar praticamente, em função da correria no dia-a-dia de nossas vidas.).

Já que tanto perfis pessoais, quanto perfis profissionais estão disponíveis no mundo virtual da Internet, as pessoas que ás utiliza, vieram a ficar mais expostas, trazendo mais riscos e vulnerabilidades para si, já que existem nas centenas de mensagens trocadas e envidas diariamente, todo tipo de malwares (tipo de vírus virtual), assim como links redirecionáveis e clicáveis que podem levar as pessoas a acessar sites falsos, criados por criminosos virtuais, com o intuito de comprometer a segurança do usuário de várias formas maliciosas possíveis.

Outra preocupação atual de pessoas, instituições ou empresas, diz respeito à circulação de notícias não verídicas (falsas), mas conhecidas como Fake News, assim como boatos que podem e venham manchar ou comprometer a imagem dessas empresas, instituições e até mesmo de pessoas, podendo causar desconforto, e em casos mais graves, pode ser até cabível de penalidades civis. Por isso, seguem algumas dicas de boas práticas, para o usuário se prevenir durante o uso das redes sociais:

- A ética assim como o bom senso, é sempre importante, durante o uso das redes sociais;

- A preservação de sua privacidade é a regra básica ao utilizar as redes sociais, por isso evite sempre expor seu perfil de maneira indiscriminada, assim como o não fornecimento e exposição de suas informações pessoais e profissionais;
- Seja criterioso e cuidadoso ao aceitar convites, para entrar/fazer parte de grupos ou comunidades, e ao aceitar pedidos de solicitações de amizades ou contatos;

- Aceitar ter contato, troca de mensagens, minimamente com pessoas que você conhece;

- Usar os serviços de localizações próximas de forma cuidadosa, pois pessoas com más intenções podem estar fazendo utilização desse recurso, para monitorar seu deslocamento físico de forma indevida;

- Ser cauteloso no compartilhamento de notícias falsas (fake news). Sempre busque pesquisar a veracidade da fonte da notícia, antes de sair compartilhando e espalhando esses tipos de notícias, de forma duvidosa;

- Ter sempre respeito a privacidade do próximo, assim como a sua, evitando circular notícias e fotos dos outros através do compartilhamento sem a previa autorização do mesmo;

- Ter cuidado com links clicáveis e arquivos anexados ás mensagens, mesmo que as mensagens tenham sido recebidas de pessoas conhecidas.

5.11 Engenharia social

A engenharia social tem um papel importante em muitos crimes virtuais, é uma técnica de persuasão clássica mais bastante utilizada por cibercriminosos, em seus crimes cometidos. A engenharia social tem como base a manipulação psicológica, ou seja, persuadir e manipular outras pessoas a fazer o que você quer que elas façam. Esta técnica é muito utilizada por criminosos virtuais, para tentar conseguir dados de pessoas (usuários) vulneráveis e suscetíveis a confiarem em outras pessoas, aproveitando assim de sua ingenuidade.

Pense que, descobrir uma vulnerabilidade, falha de segurança ou uma brecha no sistema do computador de alguém, é muito mais difícil e complexo do que por exemplo, persuadir uma pessoa se passando como gerente do banco dela, solicitando a confirmação dos dados pessoais e senha da mesma através de uma ligação telefônica. O sucesso do ataque através do uso da engenharia social, depende da decisão tomada pela vítima, no fornecimento ou não de seus dados, com isto, a engenharia social se torna eficaz e requer de menos esforço por parte do infrator.

Por mais que a engenharia social tenha seu maior foco, em atingir funcionários ou gerentes de grandes empresas por exemplo, usuários “comuns” nunca devem pensar que estão livres desses tipos de técnicas utilizadas por criminosos virtuais, devemos sempre estar atentos, e em alerta, durante nosso cotidiano, pois nunca sabemos quando podemos estar sob “efeito” da técnica de engenharia social. Como todo ser humano, somos falhos, e propícios a cometer erros, o fator humano sempre será o elo mais fraco da segurança da informação, por isso é de extrema importância possuirmos bom senso ético e um bom caráter.

5.12 Boas práticas resumidamente

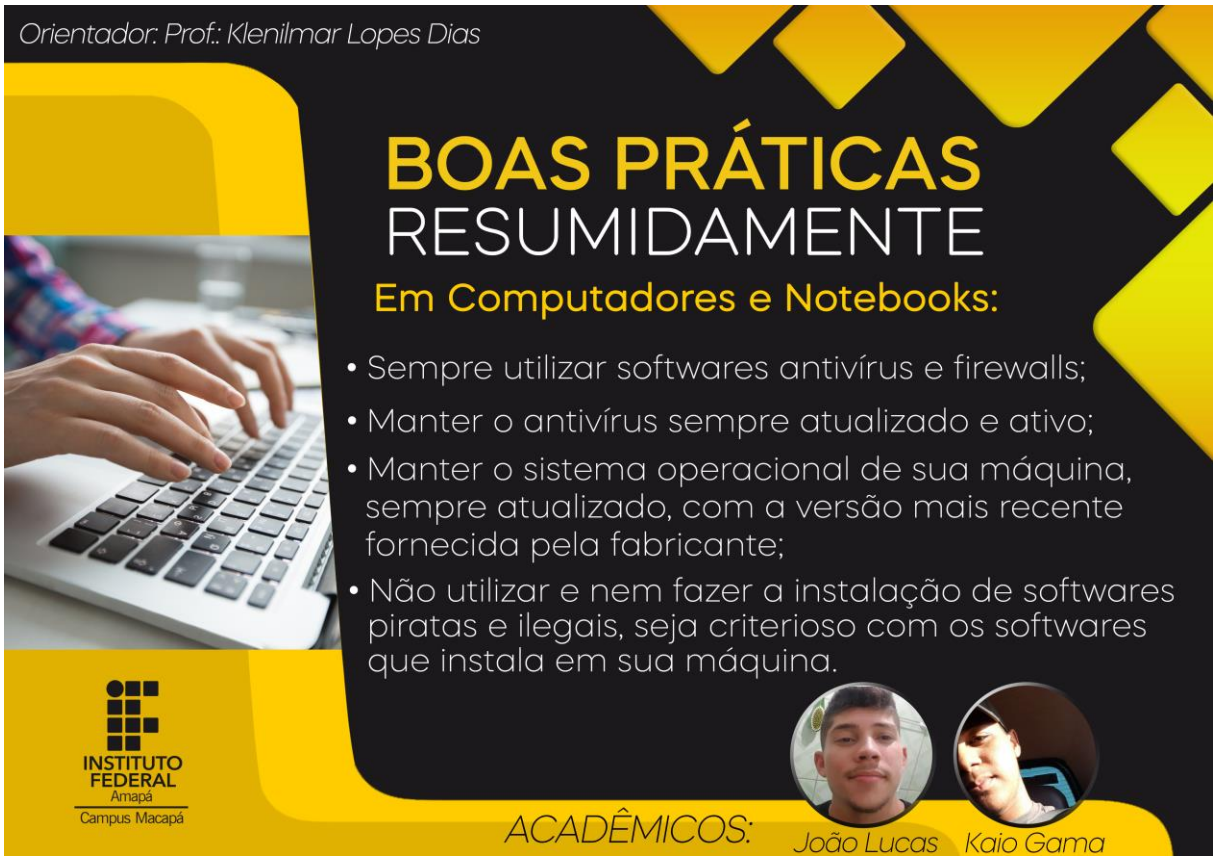
As principais precauções e boas práticas para o usuário se ter em relação a proteção e segurança de seus dados pessoais:

Em Computadores e Notebooks:

- Sempre utilizar softwares antivírus e firewalls;
- Manter o antivírus sempre atualizado e ativo;
- Manter o sistema operacional de sua máquina, sempre atualizado, com a versão mais recente fornecida pela fabricante;
- Não clicar em links redirecionáveis anexados em e-mails recebidos;
- Não executar arquivos anexados em e-mails recebidos;
- Não utilizar e nem fazer a instalação de softwares piratas e ilegais;
- Ser criterioso com os softwares que instala em sua máquina;
- Ter cuidado com mídias removíveis inseridas em sua máquina, como por exemplo: pendrives ou cartões de memória SD;

- Faça backups de seus dados com frequência e regularidade;

Figura 1 – Boas práticas resumidamente em computadores e notebooks.



Fonte: Gerada pelo próprio autor, 2021.

Na Navegação:

- Sempre manter atualizado o navegador utilizado;

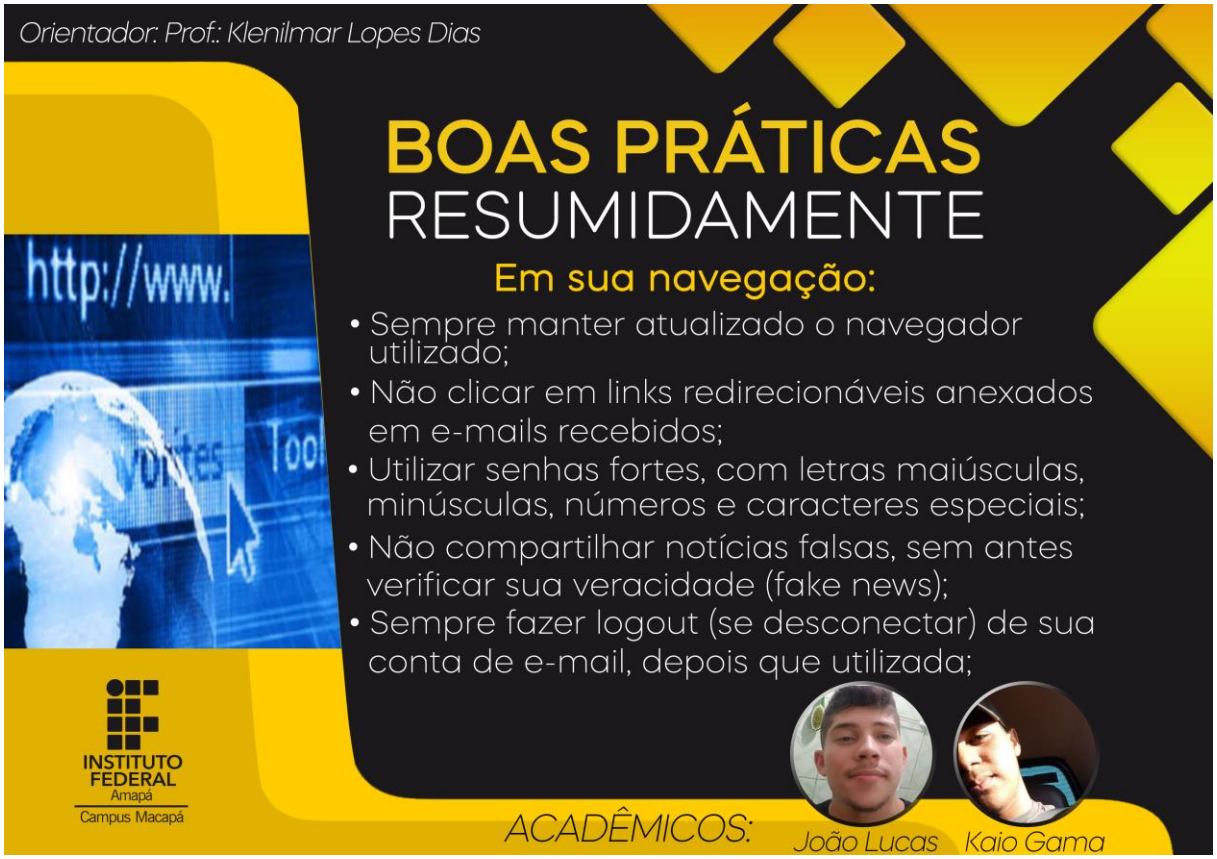
- Nunca clicar em links que sejam suspeitos, prometendo prêmios e chances imperdíveis;

- Jamais habilitar cookies, JavaScript e pop-ups em sites não confiáveis;
- Utilizar senhas fortes, com letras maiúsculas, minúsculas, números e caracteres especiais;
- Alterar com frequência suas senhas, a cada 6 meses no mínimo;

- Não expor e nem compartilhar dados pessoais, como: CPF, dados bancários, cartões de créditos e endereços, em redes sociais;
- Não compartilhar notícias falsas, sem antes verificar sua veracidade (fake news);

- Sempre fazer logout (se desconectar) de sua conta de e-mail, depois que utilizada;

Figura 2 – Boas práticas resumidamente em sua navegação.



Fonte: Gerada pelo próprio autor, 2021.

Em celulares/dispositivos móveis:

- Utilizar e sempre manter atualizado um aplicativo móvel de antivírus;
- Fazer a instalação de aplicativos somente de fontes confiáveis;

- Preferencialmente instalar aplicativos somente da loja oficial de aplicativos do seu sistema operacional móvel;

- Manter o cuidado com aplicativos que exibem de forma abusiva, anúncios na tela do seu celular;

- Sempre verificar as permissões fornecidas para aplicativos instalados;

- Habilitar o recurso de localização, NFC e Bluetooth somente quando forem utilizadas, assim que possível as desative;

- Utilize senhas, PINs e biometria digital, quando disponível, para o bloqueio do uso não autorizado de seu aparelho;

- Evite o uso de reconhecimento facial, pois o mesmo não é 100% seguro ainda;

- Mantenha seu celular atualizado, com a última versão do sistema operacional e patch de segurança mensal, disponibilizado pela fabricante;

- Fazer regulamente backup de seus dados, na nuvem ou em um computador de sua posse;

Figura 3 – Boas práticas resumidamente em celulares/dispositivos móveis.

Fonte: Gerada pelo próprio autor, 2021.

Figura 4 – Boas práticas resumidamente de forma geral.

Fonte: Gerada pelo próprio autor, 2021.

6 MATERIAIS E METODOS

Foram realizadas pesquisas bibliográficas acerca do tema tratado, no qual foi utilizado para a elaboração desse trabalho, fazendo uso a partir de documentos oficiais, além de artigos, livros e pesquisas na Internet, sobre o assunto em questão. Após ao termino dos estudos sobre o levantamento literário do tema, e também o contexto histórico, juntamente com o apanhado geral das leis em vigor em nosso país voltadas para o tema tratado no trabalho, iniciamos o desenvolvimento do artigo, seguindo as etapas: problema, justificativa, objetivo, metodologia e cronograma.

Em seguida procuramos abordar no trabalho, os principais riscos que o usuário está sujeito diariamente, acessando a rede de Internet, através de seus dispositivos, seja em sua casa ou em seu local de trabalho por exemplo, para isso fizemos uma pesquisa acerca dos principais e mais frequentes riscos.

Por fim sugerimos as principais boas práticas que o usuário deve ter em relação a privacidade e proteção dos dados pessoais, com o intuito de coibir, evitar ou ao menos diminuir o roubo e uso de forma ilegal desses dados, por criminosos virtuais, e conscientizar as pessoas (usuários) sobre os riscos encontrados na Internet e a importância da privacidade de seus dados. Para isso foram sugeridas uma série de recomendações, detalhadas e específicas para cada área de nossas vidas na sociedade da informação. Finalizadas estas etapas, foram feitas as considerações finais sobre o trabalho, apresentando os resultados esperados, acerca do tema e problemática tratados em questão.

6.1 Participantes da pesquisa

Trata-se de uma pesquisa de revisão bibliográfica, o estudo a ser desenvolvido não terá participantes.

6.2 Cenário da pesquisa

Essa proposta de pesquisa não possuirá cenário definido em virtude de que serão analisadas bases de dados online e documentos oficiais.

6.3 Etapas da pesquisa

Trata-se um estudo de abordagem qualitativa, no qual se buscará alcançar os objetivos e confirmar e/ou refutar as hipóteses deste estudo. Para isto, os proponentes da pesquisa farão buscas em diversas bases de dados, análises de documentos oficiais para a escrita do artigo de revisão bibliográfica, conforme critérios a seguir estipulados.

7 RESULTADOS ESPERADOS

O referido trabalho tem como resultado esperado, elencar medidas que venham a coibir, o furto virtual de dados dos usuários da rede.

Todos os dias, milhões de pessoas usam a Internet para obter informações, estabelecer conexões e fazer compras. Hoje, os dados pessoais são considerados uma mercadoria real. Tanto é que a revista The Economist destacou que os dados são o "novo petróleo" do século 21 devido ao seu valor e influência na economia digital.

Na verdade, serviços aparentemente gratuitos são pagos em troca de um ativo de alto valor: dados do consumidor. Por exemplo, empresas como Facebook, Google e Youtube coletam informações sobre usuários e rastreiam sua navegação para personalizar anúncios e conteúdo em suas plataformas.

Esses dados pessoais permitem a criação de perfis de usuários com base em algoritmos que podem compreender padrões de comportamento e influenciar as escolhas do usuário. Os dados gerados pelo usuário ajudam a direcionar melhor as campanhas publicitárias, conduzir pesquisas estatísticas, monitorar os hábitos de consumo, projetar produtos melhores e ajustar as atividades políticas. Nos próximos anos, o uso da tecnologia de inteligência artificial pode levar o aprendizado de máquina a outro nível. Por meio da análise das informações do usuário, o sistema pode prever seu comportamento futuro e fornecer suas necessidades potenciais.

Em maio, a União Europeia aprovou o GDPR (Regulamento Geral de Proteção de Dados), um novo regulamento de proteção de dados criado para proteger a privacidade dos cidadãos. Esta medida é efetiva para todos os estados membros da UE. O GDPR se aplica a todas as empresas ou organizações que fornecem bens ou serviços para coletar dados pessoais de residentes da EU (União Europeia). As suas medidas representam um conjunto de boas práticas nas atividades dirigidas ao tratamento de dados pessoais. A nova lei representa a maior mudança no campo da privacidade online em 20 anos e pode fortalecer sua posição como um padrão internacional. Ele moderniza a atual Lei de Proteção de Dados de 1998.

O GDPR cria uma regra de que os dados pessoais só podem ser usados com o consentimento do usuário. Qualquer entidade que queira usar os dados

pessoais de alguém deve pedir sua autorização e explicar sua finalidade. Para crianças, o pai ou responsável legal deve dar autorização. Qualquer serviço de Internet que coleta direta ou indiretamente dados sobre pessoas precisa reportar esses dados de forma clara, acessível e transparente. O controle será feito por meio de fiscalizações e, se a organização descumprir as regras, poderá ser multado.

Existem algumas exceções ao uso deste mecanismo, como o fornecimento de dados que estejam em conformidade com a lei ou o fornecimento de dados pessoais necessários para os serviços que você contratou. Além disso, qualquer pessoa tem o direito de acessar, transferir, corrigir ou excluir informações sobre si mesma a qualquer momento, e tem o direito de solicitar a interrupção da coleta de dados.

Por exemplo, no Brasil, se fotos privadas vazarem ou dados de cartão de crédito vazarem ou forem danificados devido a uma quebra de segurança, os consumidores podem precisar de um provedor de serviços baseado na Internet do Marco Civil para reparos. No entanto, ainda não existe uma lei que proíba a vigilância e comercialização de dados sem o consentimento do usuário. Também podemos sofrer vazamentos de dados de grandes empresas que foram hackeadas e não têm direito a qualquer forma de compensação. Os novos regulamentos da UE devem afetar as mudanças no Brasil. O impacto direto ocorrerá em empresas brasileiras que prestam serviços na União Europeia, que processam os dados de residentes na região.

8 CONSIDERAÇÕES FINAIS

Durante a pandemia da COVID-19, observou-se um grande aumento no uso da Internet mundial, de uma forma globalizada, pois devido ao isolamento social, como principal forma de precaução ao contagio do vírus, tivemos uma maior requisição e necessidade de utilizar com mais frequência e intensidade a rede mundial de computadores.

Este trabalho teve como finalidade destacar a importância da proteção de dados pessoais durante uma pandemia, pois os mesmos são essenciais para o exercício de muitos direitos básicos. A informação é um bem valioso da sociedade contemporânea. A pandemia do COVID-19 fez com que observássemos que embora seja necessário garantir a proteção da vida e da saúde das pessoas, a proteção dos direitos humanos básicos não pode ser descartada, por isso prova a necessidade urgente de entrada em vigor, de leis mais severas, e punições maiores para crimes cometidos em meios eletrônicos (Crimes Virtuais), e também a reformulação/modificação das leis já existentes no Código Penal Brasileiro – para garantir a segurança das relações sociais e jurídicas que envolvem o processamento de dados pessoais, para assim então proteger a vida e a saúde das pessoas, e evitar ferir o direito da personalidade das mesmas.

Em seguida destacamos meios para ajudar as pessoas (usuários) manterem a privacidade e a proteção aos dados pessoais, durante a pandemia da COVID -19 ou não; através de recomendações e boas práticas para serem seguidas, tentando assim, diminuir a vulnerabilidade do usuário e seus dispositivos conectados na rede, consequentemente aumentando a segurança de seus dados pessoais. Através desta conscientização, diminuísse os riscos dos usuários, e teremos menos crimes virtuais sendo praticados por cyber criminosos na Internet.

Durante uma pandemia, o processamento de dados pessoais precisa encontrar um equilíbrio entre a proteção da saúde pessoal e a proteção à privacidade de milhões de proprietários de dados pessoais. Mesmo em alguns casos em circunstâncias especiais, o processamento de dados deve ser realizado de acordo com os seguintes princípios: Proporcionalidade, integridade, segurança, prevenção, igualdade, eficiência e eficácia, desta forma, é possível conciliar,

equilibrar e proteger os direitos à vida e a saúde, privacidade, igualdade e liberdade, para garantir a proteção da dignidade humana na sociedade da informação.

REFERÊNCIAS

BARROS, Bruno Mello Correa de; FLAIN, Valdirene Silveira. **O MARCO CIVIL DA INTERNET: UM OLHAR SOBRE A PROTEÇÃO DOS DIREITOS E GARANTIAS DOS USUÁRIOS NA SOCIEDADE EM REDE.** 2016. Disponivel em: https://online.unisc.br/acadnet/anais/index.php/sidspp/article/viewFile/15760/3663 Acessado em: 09/10/2020

BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 2014. Disponivel: em:** http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acessado em: 12/10/2020

BRASIL. **Projeto de Lei 1179/2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid- 19).** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2247564. Acessado em: : 02/03/2021

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. Disponivel em: http://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/5973/2019_bioni_protecao_dados_pessoais.pdf?sequence=1 Acessado em: 15/10/2020

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo. Saraiva. 2000.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar; 2006. Disponivel em: https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais Acessado em: 14/10/2020

GEDIEL, J. A. P.; CORRÊA, A. E. . **Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado.** Revista da Faculdade de Direito. Universidade Federal do Paraná, v. 47, p. 141, 2008. Disponivel em: https://revistas.ufpr.br/direito/article/view/15738 Acessado em: 12/10/2020

GIL, A. C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2007. Disponivel em: http://home.ufam.edu.br/salomao/Tecnicas%20de%20Pesquisa%20em%20Economia/Textos%20de%20apoio/GIL,%20Antonio%20Carlos%20-%20Como%20elaborar%20projetos%20de%20pesquisa.pdf Acessado em: 14/10/2020

JESUS, Damásio de **Marco Civil do Internet : comentários ò Lei n. 12.965, de 23 de abril de 2014** / Damásio de Jesus, José Antonio Milagre. - São Paulo : Saraiva, 2014. Disponivel em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2014;001025737 Acessado em: 10/10/2020

JÚNIOR, Marcos Ehrhardt. **Privacidade e proteção de dados pessoais durante a pandemia da COVID-19.** Disponível em: https://direitocivilbrasileiro.jusbrasil.com.br/artigos/824478175/privacidade-e-protecao-de-dados-pessoais-durante-a-pandemia-da-covid-19. Acesso em: 10/03/2020

KUJAWSKI, Fábio Ferreira; THOMAZ, Alan Campos Elias. **Da proteção aos registros, dados pessoais e comunicações privadas – um enfoque sobre o Marco Civil da Internet,** p. 677-694. In.: LEITE, G. L, LEMOS, R. Marco Civil da Internet. São Paulo: Altas, 2014.

LEMOS, Ronaldo. **O Marco Civil como símbolo do desejo por inovação no Brasil**, p. 03 – 11. In.: LEITE, G. L, LEMOS, R. Marco Civil da Internet. São Paulo: Altas, 2014.

LEONARDI, Marcel. **Tutela e privacidade na internet**. 11ª ed. São Paulo: Saraiva, 2012. Disponivel em: http://leonardi.adv.br/wp-content/uploads/2012/01/mltpi.pdf 24/10/2020

PAESANI, Liliani Minardi, **Direito e Internet**. 3 ed. São Paulo. Atlas. 2006.

PEREIRA, Lucas de Almeida. **Os primórdios da informatização no Brasil: o "período paulista" visto pela ótica da imprensa**. 2014. Disponivel em: https://www.scielo.br/pdf/his/v33n2/0101-9074-his-33-02-00408.pdf Acessado em: 12/10/2020

PINHEIRO, Patrícia Peck**. Proteção de Dados Pessoais**: comentários à Lei 13.709/2018. São Paulo: Saraiva, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/ books/9788553608324/cfi/3!/4/4@0.00:48.7. 14/10/2020

SCHREIBER, Anderson (Coord.). **Direito e Mídia**. São Paulo: Atlas, 2013. Disponivel em: https://www.academia.edu/35741516/Direito_e_M%C3%ADdia Acessado em: 24/10/2020

CIDALE, Ricardo A. **Vírus Digital: tudo o que as empresas precisam saber sobre a ameaça do vírus digital, como evitá-lo e como recuperar sistemas contaminados.** McGraw Hill, 1990.

PORTAL TERRA. Disponível em: <https://duvidas.terra.com.br/duvidas/600/quais-cuidados-devo-ter-para-minha-seguranca-na-internet/>. Acesso em: 23/02/2021.