UNIVERSIDADE FEDERAL DA BAHIA
FACULDADE DE FILOSOFIA E CIÊNCIAS HUMANAS
DEPARTAMENTO DE SOCIOLOGIA

REYNAN DA SILVA DIAS PAIVA

A IMPORTÂNCIA DA LGPD NA SOCIEDADE BRASILEIRA

Salvador
2022

REYNAN DA SILVA DIAS PAIVA

A IMPORTÂNCIA DA LGPD NA SOCIEDADE BRASILEIRA

Trabalho apresentado à Universidade Federal da Bahia, como requisito para conclusão da disciplina Metodologia e Expressão Técnico-Cientifica.

Orientador: Prof. Dr. Felipe Padilha

Salvador

2022

RESUMO

A Lei Geral de Proteção de Dados (LGPD) expressa um conjunto de normas validas para o território brasileiro sobre como as empresas, pessoas e os órgãos públicos devem guardar, proteger e usar informações pessoais coletadas dos usuarios (Nilton Kleina, 2020). Essa pesquisa apresenta a importância da LGPD na sociedade brasileira, com o objetivo de identificar quais métodos foram implementados tendo como foco o controle do uso e a comercialização indevida de dados pessoais, inclusive em meios digitais. Entre os objetivos específicos, pretende-se identificar e analisar os obstáculos que dificultam a implementação da LGPD. Este trabalho é de extrema importância, para analisar o que vem sendo feito, no âmbito público, empresarial, no tratamento dos dados coletados em saúde e, a partir das mudanças trazidas pela lei 13.709/2018, quais reverberações poderão causar na sociedade. Um dos principais fatores que contruibuiram para implementação dessa lei no Brasil foi quando na Europa, a General Data Protection Regulation (GDPR), entrou em vigor no ano de 2018, sendo esta, uma lei que garante a proteção dos dados de todas as pessoas cidadãs da União Europeia. Deste modo, a pressão por uma regulamentação parecida no Brasil tornou-se um importante tópico para o país (Jessica Compugraf, 2018). A metodologia de pesquisa utilizada é qualitativa, descritiva e bibliográfica, utilizando-se do método dedutivo na fase de investigação, tendo como foco principal os procedimentos ocorridos durante a sua implicação nas instituições públicas e privadas, além do auxilio no combate ao cibercrime.

Palavras-Chave: Lei Geral de Proteção de Dados; Sociedade Brasileira; Ciência Da Computação; Pesquisa Bibliográfica.

SUMÁRIO

1 – INTRODUÇÃO

Para que as pessoas possam viver em sociedade, elas necessitam obedecer determinadas regras e considerar certos aspectos da cultura da sociedade na qual estão inseridas. Em 14 de agosto de 2018, o então Presidente da República, Michel Temer, promulgou a lei número 13.709/18 (PLANALTO, 2018a), a Lei Geral de Proteção de Dados. Nesta ocasião, foi apresentada a lei de um modo geral, o que deixou claro a sua semalhança com a GDPR. O que causou maior impacto foi o fato de que a lei teve vetada a criação da sua autoridade reguladora e fiscalizadora, tal organismo deveria se chamar Agencia Nacional de Proteção de Dados (ANPD). A LGPD, agora oficialmente criada, recebeu um período de 18 meses para que tenha seu regimento devidamente efetivado. Esse período também foi útil para fazer com que as empresas tivessem um determinado tempo para se adaptar a lei, portanto, a lei seria válida a partir de 15 de Janeiro do ano de 2020. A partir de sua vigência, todas as pessoas naturais, pessoas de direito privado e pessoas de direito público ficam obrigadas a cumpri-la, sem exceção.

Para tal fim, os desafios são inúmeros e serão abordados no decorrer deste projeto de pesquisa. Primeiramente, é válido ressaltar quais ações que devem ser tomadas para a implementação da LGPD, de forma a obter a chamada "Compliance", que nada mais é, que estar em "estado de cumprimento" com a mesma. Portanto, na busca por conformidade, as organizações deverão definir estratégias de proteção de dados com apoio de pessoas e tecnologias que permitam aos seus gestores e colaboradores, alcançarem o nível adequado de governança em privacidade e segurança da informação exigido pela Lei (VASCONCELOS, 2020). Nessa medida, antes de comentar sobre a LGPD, reservamos um espaço para abordar as questões relacionadas a falta de privacidade, segurança da informação e os inúmeros casos em que acarretaram no vazamento de dados no Brasil.

Sendo assim, o objetivo desse estudo é analisar a importância nesse novo contexto em que está inserida a pessoa natural e as empresas que atuam no territorio brasileiro quando estamos falando do tratamento de dados, por conseguinte, questões relacionadas a proteção de dados e privacidade que estão previstas na LGPD.

Pessoa Natural: é o ser humano, sem discriminação de qualquer tipo como: idade; sexo, cor; raçã, nacionalidade; saúde etc. É todo ser humano, seja: recém-nascido, criança; adolescente; idoso; absolutamente incapaz; relativamente incapaz; ou seja, todo ser humano nascido com vida.

1.2 Objetivos

Este projeto de pesquisa pretende analisar o contexto de implementação da LGPD, exclusivamente na sociedade brasileira. Tendo como objetivo principal explicar para o leitor deste presente trabalho o que é a lei geral de proteção de dados e qual a sua importância para com a sociedade brasileira.

1.2.1 Objetivo Geral

Este trabalho pretende analisar o contexto de implementação da LGPD, com foco na dificuldades de sua efetivação.

1.2.2 Objetivo Especificos

a) O contexto histórico em que a LGPD está inserida.
b) O que é a General Dat Protection Regulation (GDPR) e a sua relação com o Brasil.
c) Citar como que as outras leis brasileiras se relacionam com a LGPD.

1.3 Justificativa

A preocupação da sociedade atual para as com questões relacionadas a regulamentação do tratamento de dados pessoais ainda é muito pequena, entretanto, os grandes casos de vazamento sobre o uso ilegal dos dados dos indivíduos, tanto no Brasil, quanto em outros países tem começado a alertar a sociedade sobre a importância de uma agência reguladora, para que assim, os seus dados estejam protegidos, desta forma, garantindo a proteção do indivíduo (PIZZATO, 2019).

O principal caso e o mais recente foi o da Cambrydge analytica. Os jornais The New York Times e o The Guardian denunciaram o Faceboook pelo vazamento de informações de mais de 50 milhões de pessoas, sem o devido consentimento. A notícia, que rapidamente foi replicada em todo o mundo, renovou a discussão sobre o que é permitido em relação ao acesso e tratamento de informações na internet e qual a responsabilidade das empresas no vazamento dos dados pessoais dos usuários. O caso Cambridge Analytica foi um esquema de coleta de

dados realizado por meio de um teste psicológico chamado de "T*his is your digital life",* aproveitando uma brecha nos termos e condições do Facebook que não proibia expressamente a venda de dados coletados na rede social por aplicativos. Portanto, quando o usuário fazia o teste, ele não entregava apenas as suas informações, mas as de toda a sua rede de amigos, que posteriormente foi vendida para a Cambridge Analytica, empresa que trabalhava na campanha presidencial de Donald Trump, bem como para o grupo que promovia a saída do Reino Unido da União Europeia. Ao acessar dados, como nome, endereço, e-mail, hábitos e gostos pessoais, a empresa analisava o perfil de cada eleitor e direcionava as suas propagandas políticas a favor de seus clientes (CAMARGO E VIEIRA, 2020).

A questão primordial é que ao seguir devidamente a LGPD, as empresas também estão adotando condutas éticas, agregando valor aos seus negócios, agindo de forma efetiva com o objetivo de suprimir problemas atuais e futuros da sociedade.

Outrossim, a escolha do tema foi em decorrência da necessidade de aprimorar e ampliar os conhecimentos acerca da importância dos dados pessoais e dos dados sensiveis do individuo. Pois com uma maior conscientização dos usuários, a lei de proteção de dados pessoais será mais uma forma de empoderamento do consumidor. Isso vai ter como consequência maiores pressões para que as organizações invistam em segurança da informação. Segundo o advogado Kleber Vasconcelos, a LGPD em vigor trouxe uma excelente oportunidade principalmente para o setor empresarial, tendo em vista o grande fluxo de capital no comércio eletrônico em virtude da Covid-19. Ou seja, o empresa tem a chance de fidelizar os clientes por meio da proteção dos dados deles, bem como proteger o seu negócio de futuras sanções administrativas ou judiciais por algum descumprimento da lei. Logo em seguida, ele destacou algumas vantagens para a implementação da lei, sendo elas: A melhora da reputação e imagem da empresa no mercado; O destaque em relação à concorrência; Mais credibilidade no mercado pela conscientização da proteção dos dados pessoais; O apreço por parte dos clientes e parceiros comerciais; O fortalecimento das relações comerciais em virtude da responsabilidade solidária, ao passo que a empresa poderá fechar mais contratos.

2.0 IMPORTANCIA DOS DADOS PESSOAIS.

De acordo com o pesquisador Grimaldi, um dado pessoal é a sua informação. Aquela que pode identificar você ou levar a identificação de uma determinada pessoa. Os dados

podem ser definidos como dados físicos ou digitais. Seja um cadastro, nome, CPF, endereço, e-mail, data de nascimento. Seu registro de empregado. O dedo que é usado para biometria que coloca no celular. O seu prontuário médico ou qualquer outra informação relacionada a saúde. Sua localização no GPS. As suas alegações de conexão (cookies). Ou seja, pegou alguma informação pessoal sua é considerado seu dado.

Segundo a pesquisa bibliografica produzida pelos autores, Deborah Christina e Ari Fernando, entitulada “Big Data, exploração ubíqua e propaganda dirigida: novas facetas da indústria cultural”; As principais características dos Big Data seriam: volume, velocidade e variabilidade (Mostafa, Cruz, & Amorim, 2015). A primeira característica denota a enorme quantidade de dados, disponíveis em volume crescente - Mayer-Schönberger e Cukier (2013) estimam que a quantidade de dados digitais no planeta seja equivalente a dar hoje a cada pessoa na Terra trezentas vezes a quantidade de informação que se estima que estivesse armazenada na biblioteca de Alexandria, e a perspectiva de uma abordagem desses dados que não seja feita por amostragem, mas tomando a totalidade. O Big Data, assim como as nuvens onde os grandes dados ficam armazenados, “são motores que impulsionam o capitalismo da informação uma vez que permitem uma forma de saber cada vez mais dominante”14 (Mosco, 2014, p. 12). Em suma, o Big Data produz um controle cada vez mais preciso e ubíquo que tem a tendência a se expandir aceleradamente, uma vez que o crescimento do capital circulante, no plano da economia capitalista global, se organiza a partir desse imperativo, apesar das constantes e inevitáveis crises.

Outro ponto importante é entender quem está coletando e o que realmente será feito com seus dados, ou seja, ter conhencimento se os dados dos usuarios serão usados só para empresa ou se ela irá partilhar com outras empresas. É extremamente importamte que a transparência se faça presente. Os usuários também devem voltar as suas atenções aos aplicativos, nada é de graça, deve-se ler atentamente os termos de uso e verificar quais informações estão sendo coletadas em troca do uso do app. E caso identifique o uso abusivo dos seus dados pessoais procurem promotoria de jus tiça da cidade ou advogados especializados. Os corretores de dados também são recursos valiosos para agressores e *stalkers*. O ato de liberar publicamente informações pessoais de alguém sem o seu consentimento é possível, na maioria das vezes, por causa deles. Por mais que seja possível excluir uma conta do Facebook com certa facilidade, fazer com que empresas desse ramo removam as informações referentes ao perfil desativado é um processo demorado, complicado e, às vezes, impossível. Dados pessoais também são usados por pesquisadores de inteligência artificial para treinar programas ou serviços. Usuários de todo o mundo enviam bilhões de fotos, vídeos, postagens de texto e

clipes de áudio para sites como YouTube, Facebook, Instagram, TikTok e Twitter diariamente e essa mídia serve como "alimento" para algoritmos de *machine leaning*.
Com essa tamanha quantidade de dados, a máquina aprende a “enxergar” o que está em uma fotografia ou determinar automaticamente se uma publicação viola a política de termos de uso de determinada rede social.

Stalker: é uma palavra inglesa que significa "perseguidor". É aplicada a alguém que importuna de forma insistente e obsessiva uma outra pessoa que, em muitos casos, é uma celebridade. A perseguição persistente pode levar a ataques e agressões. Com a Internet, a prática entrou para o campo virtual: o cyberstalking é praticado através de meios informáticos com qualquer pessoa que desperte o interesse do agressor.

2.1 TRATAMENTO DE DADOS

A LGPD dispõe, de forma ampla, que dados pessoais são “qualquer informação relacionada a pessoa natural identificada ou identificável”. Uma informação que identifica uma pessoa pode ser um dado simples, como um nome, números ou outros identificadores. Sendo possível identificar um indivíduo diretamente das informações processadas, essas informações podem ser dados pessoais. Se não for possível identificar diretamente um indivíduo a partir dessas informações, deverá ser ponderado se ele ainda é identificável, levando-se em consideração outras informações que poderão ser processadas em conjunto, através de meios razoáveis, para identificar um indivíduo. Um nome ao lado de um endereço residencial, um perfil online que fornece um nome e a empresa para a qual a pessoa trabalha, um endereço de e-mail corporativo, registros de RH, listas de clientes, detalhes de um contato ou até endereços IP (endereço de protocolo da Internet) são exemplos de informações que, se combinadas, podem vir a identificar um indivíduo e, portanto, consideradas pessoais. Em assim sendo, seu tratamento demandará a fixação de bases legais específicas, dispostas na LGPD. A lei determina quais são os considerados sensíveis (sendo estes dados que podem ser rastreados até um indivíduo e que, caso sejam divulgados, podem resultar em danos): dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso; dados filosóficos ou políticos; referentes à saúde ou à vida sexual, além de dados genéticos ou biométricos. A lei prevê tratamento diferenciado nesses casos (como, por exemplo, o consentimento a ser fornecido, de forma específica e destacada, para finalidades específicas) e lista as hipóteses em que o tratamento poderá ocorrer sem o consentimento do titular (LOPES&CASTELO, 2021).

A LGPD define que um dado anonimizado é aquele cujo qual, originariamente, era relativo a uma pessoa, porém que passou por fases que garantiram a desvinculação dele a essa

pessoa. Caso um dado seja anonimizado, então a LGPD não se aplicará a ele. É valido ressaltar que um dado só é considerado efetivamente anonimizado se não permitir que, se reconstrua o caminho para "descobrir" quem era a pessoa titular do dado e se de alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado e sim, apenas, um dado pseudonimizado e estará, então, sujeito à LGPD (SERPRO, 2020).

2.2 BENEFICIOS DO TRATAMENTO DE DADOS PELAS EMPRESAS

Com o aumento da confiabilidade, o vínculo entre corporação e clientes podem acabar adquirindo muita vantagem com a implementação do tratamento dos dados pessoais. Pois é a partir do momento em que as pessoas sabem que a empresa está tomando medidas para manter suas informações em segurança, a confiabilidade dessa relação tende a ampliar. Com o Aprimoramento da comunicação, encontra-se outra exigência da LGPD que é a minimização, ou seja, a coleta apenas dos dados essenciais dos clientes. Essa regra pode ajudar a companhia no sentido de descartar informações que não são relevantes para as estratégias do negócio. Tambem faz-se necessário um estruturação de processos, visando estabelecer um processo de tratamento de dados, também podendo facilitar a organização dessas informações e a implementação de uma padronização na coleta, manipulação e armazenamento. Com isso, a empresa terá uma estruturação de processos que envolvem o tratamento de informações pessoais, que será útil a longo prazo. Deste modo, será mais simples atender às exigências da lei e manter a organização de dados.

3.0 GDPR E A SUA INFLUÊNCIA NO BRASIL

A GDPR (General Data Protection Regulation) é a lei de proteção de dados voltada para países que fazem parte da União Europeia. Esta lei foi aprovada no ano 2016, tendo uma vacatio legis 7 de dois anos, sendo vigente, portanto, a partir de 25 de maio de 2018, este também foi o ano em que começaram a ser realizadas as fiscalizações e aplicadas as multas. Esta regulamentação trouxe mudanças significativas no que tange ao tratamento de dados pessoais. Primeiramente, o consentimento do titular de dados começou a ser o elemento principal para autorizar a coleta e tratamento de dados. Entretanto, o poder de fiscalização e multa, atribuído as autoridades fiscalizadoras chamou a atenção. O descumprimento da GDPR

pode acarretar sanções de até 4% do faturamento anual da empresa, ou 20 milhões de euros. Em um ano de vigência, a lei rendeu, em multas, uma soma astronômica de euros. Também foi introduzida, a figura do DPO - Data Protection Officer, que passou a ser o elo responsável por fazer a interface entre o titular dos dados e a empresa ou a autoridade de fiscalização/regulamentação, o que facilita um controle maior sobre o uso dos dados pessoais. O principal objetivo de um controle tão rígido vem da necessidade de evitar os abusos na coleta ou no processamento das informações dos usuários (POHLMANN, 2020). A GDPR promove a proteção de dados pessoais presentes em bancos de empresas. A proposta principal é que o indivíduo tenha direito de conhecer quais informações ele está fornecendo aos serviços de que usufrui. Ademais, a entidade deve explicar o motivo da requisição de determinados dados do cliente, e para qual finalidade elas serão usadas. A GDPR não delimita um nível de importância, deste modo, de acordo com a legislação, coletar informações menores como cookies no navegador é considerado tão pertinente quanto pedir nome ou endereço de residência (CARDOSO, 2018).

Segundo dados do website de noticias “inventti” no que diz respeito a GDPR, os dados mais importantes que devem ser protegidos são: Informações pessoais básicas, como; nome, endereço e número do documento de identidade. Informações da web, como IP, dados de cookie e etiquetas RFID. Informações de saúde e genéticas. Dados biométricos. Dados raciais ou étnicos. Opiniões políticas.Orientação sexual.

O GDPR já entrou em vigor na União Europeia, e apesar de parecer distante, afetou o Brasil na criação da sua própria lei a LGPD (lei geral de proteção de dados pessoais). Todas as empresas serão impactadas pelo GDPR, porém empresas que necessitam da coleta de dados sofrem impacto maior. Caso sua empresa faça armazenamento de dados de clientes que residem na Europa, então ela também é afetada pelo lei. O GDPR tem impacto em um dos setores principais de qualquer empresa, o departamento de marketing. Os dados coletados para fins de publicidade não poderão ser usados posteriormente para outro fim. Caso a empresa não consiga provar que as informações obtidas foram cedidas de forma consensual isso implicará em multas (CENTRIC, 2021).

Não tem como manter-se em um mundo globalizado, sem seguir determinadas regras coletivas. E, no momento, a preservação dos direitos sobre os dados pessoais é a regra da vez. Sem uma legislação adequada sobre proteção de dados, o Brasil estaria impossibilitado, na maioria das situações, de efetuar negócios com a Europa, o que é impensável, na atualidade. Então, tendo em conta esta realidade, fica patente o motivo pelo qual a nossa lei foi promulgada com tanta pressa (POHLMANN, 2020).

4.0 LEIS BRASILEIRAS QUE SE RELACIONAM COM A LGPD.

O livro do Sergio Pohlmann deixa bem claro que a base legal da LGPD já estava muito bem fundamentada, em outras leis, espalhadas, sendo que algumas são bem antigas, o que deixa explicito que o estado se importar com a segurança dos dados pessoais não é algo tão novo assim, leis para proteção dos dados dos indivíduos já existiam no Brasil, entretanto, não era algo claro e especifico, o que acarreta em muitas brechas.

Valido ressaltar que essas informações relacionadas as leis que estão relacionadas com a lei geral de proteção de dados foram retiradas do livro escrito pelo Sérgio Pohlmann intitulado: LGPD Ninja: Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas.

Relativas ao Setor Financeiro, é possível encontrar leis como a Resolução do BACEN 9 n 4.658 – 2018: Aborda a política de segurança cibernética e os requisitos para a contratação de serviços relacionados ao processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e as demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Com respeito a saúde do indivíduo, encontramos a CFM 10 - Resolução 1.821/2007: Esta lei determina os procedimentos de segurança com o foco na digitalização e armazenamento de prontuários médicos, sendo esses, dados pessoais sensíveis. Também é possível encontrar leis com o foco diretamento ao indivíduo, sendo elas: A Constituição Federal do Brasil – 1988: Cita que todos são iguais perante a Lei, e reforça o direito do cidadão para com as questões relacionadas à intimidade, à imagem e à privacidade. Lei do Habeas Data - Lei 9.507/1997 11: Regulamenta o uso do habeas data, como um recurso jurídico que possibilita que alguém possa tomar completo conhecimento sobre as informações existentes relativas à sua pessoa, tal como possa retificar seus dados, caso os mesmos estejam com determinadas informações incorretas.

Relativas ao Estado, há leis como o Crime de inserção da dados falsos em sistemas de informação pública - Lei 9.983/2000: Estabelece como crime a atuação de alteração ou criação de dados falsos em sistemas relativos à administração pública. Cadastro único para programas soficiais do Governo Federal - Decreto 6.135/2007: Delimita as regras para o Cadastro Único para Programas Soficiais do Governo Federal, e o intercâmbio destas informações entre os órgãos do Estado. Política de Dados Abertos do Governo Federal - Decreto 8.777/2016: Melhora os processos de tratamento de dados públicos, definindo, inclusive a questão da portabilidade e da transferência de dados entre entes públicos.

Valido ressaltas as leis Relativas as Comunicações, dentre elas, temos: Lei de Interceptação Telefônica e Telemática - Lei 9.296/1996: Disciplina a interceptação de comunicações, interferindo, de forma legal, na privacidade ou intimidade da pessoa sob curso de uma investigação. Lei Geral de Telecomunicações - Lei 9.472/1997: Regulamenta o direito à privacidade e aos dados pessoais, aos usuários de serviços de telecomunicações no país.

Além dessas leis que foram citadas, também existem leis que tem ligação direta para com a Internet ou a dispositivos Eletrônicos, como, por exemplo: Crime de invasão de dispositivos informáticos - Lei 12.737/2012: Esta é a chamada Lei Carolina Dieckmann, na qual se típica como crime a invasão de equipamentos e dispositivos informáticos. Marco Civil da Internet - Lei 12.965/2014 e Decreto 8.771/2016: Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. É uma prévia da LGPD, mas apenas para provedores de serviços de internet.

Mais voltadas ao Consumo é notavel a SDE/MG 13: Considera abusivas as cláusulas de contratos de fornecimento de produtos e serviços que violem a privacidade do consumidor. Serviço de SAC 14 - Decreto 6.523/2008: Estabelece o sigilo dos dados pessoais em uso pelos Serviços de Atenção ao Consumidor. Cadastro Positivo - Lei 12.414/2011: Reconhece os direitos do usuário, garantindo a que os mesmos estejam relacionados à finalidade específica ao qual foram requisitados. Também disciplina a consulta de bases de dados com informações de adimplemento, tanto de pessoas naturais, quanto de pessoas jurídicas.

5.0 ANPD - (Autoridade Nacional de Proteção de Dados)

A cerca criação da Autoridade Nacional de Proteção de Dados, Sérgio Pohlman afirma que originalmente vetada na criação da Lei, foi determinada na MP869/18, com o objetivo de assumir a posição de autoridade máxima para fiscalizar e regulamentar a proteção de dados no país. A ANPD será responsável pela regulamentação adicional sobre a LGPD. Significa que alguns aspectos ainda não tratados ou definidos pela LGPD poderão ser tratados, definidos ou regulados, através de normas ditadas pela ANPD. Em princípio, a ANPD efetuará as fiscalizações pertinentes, e poderá derivar a aplicação de multas a autoridade judicial competente. Já previstos na LGPD, os valores das multas podem ser bastante significativos: Até 2% do faturamento anual da empresa, limitado ao valor de R$ 50.000.000 (cinquenta milhões de reais). Também poderão haver multas diárias por incumprimento, como forma adicional de acelerar o cumprimento por parte das empresas irregulares. Também cabe à ANPD o

acolhimento de denúncias diretas por parte dos titulares de dados. Ainda que as solicitações de dados devem ser efetuadas diretamente junto ao Encarregado de dados ou pessoa equivalente, a ANPD poderá estabelecer, através de meios eletrônicos ou físicos, mecanismos facilitados para que o titular possa comunicar-se de forma eficiente, diretamente com a Agência, informando ou denunciando irregularidades (Sérgio Pohlmann, 2020).

6.0 ASPECTOS GERAIS DA LGPD

Valido ressaltar que os dados pessoais são todas as informações relacionadas a pessoa natural, dentre elas, estão: nome, sobrenome, data de nascimento, entre outros, a lei também dispõe sobre os dados pessoais sensíveis , sendo sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, esses dados sensíveis, por conter maiores informações da pessoa, a lei traz um tratamento mais rigoroso (VAGNER, 2020).

No dia 14 de agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados (“LGPD”, Lei n° 13.709/2018, publicada em 15/08/2018), que entraria em vigor em fevereiro de 2020, após um período de 18 meses para adaptação. No entanto, algumas mudanças legislativas permitiram, inicialmente, a alteração da entrada em vigor para Agosto de 2020. Na sua essência, a LGPD é um novo conjunto de regras destinadas a dar aos cidadãos mais controle sobre seus dados pessoais e pretende simplificar o ambiente regulatório para as empresas, de forma que tanto os cidadãos como as empresas possam se beneficiar plenamente da economia digital. Um dos pontos mais importantes da nova lei é seu impacto transversal, visto que influenciará muitos setores da economia e a maior parte das entidades, públicas ou privadas, online ou offline (de P&D ao marketing, de clientes a empregados, de serviços à indústria). Encontra-se sob o escopo da norma qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: Operação de tratamento seja realizada no território nacional; A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; Os dados pessoais objeto do tratamento tenham sido coletados no território nacional, isto é, quando o titular dos dados aqui se encontre no momento da coleta.

Pelos argumentos e conteudos anteriormente apresentados, é compreensivel que a LGPD tem como objetivo proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas. Este é o primeiro ponto: a LGPD não tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, sejam elas funcionárias, terceiras, clientes, acionistas etc… Ou seja, todo mundo. Qualquer empresa, organização, instituição pública ou privada que coleta ou que utiliza dados de pessoas físicas precisa se adaptar a ela. A lei traz conceituações importantes. Para a lei, dado pessoal é uma "informação relacionada à pessoa natural identificada ou identificável", ou seja, dados como nome, endereço, sexo, RG e CPF. A lei define ainda o conceito de dado pessoal sensível como um "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Segundo a lei geral de proteção de dados, dentre os papeis principais, encontramos:

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado de dados: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional.

Caso o responsável legal seja menor de 18 anos, a lei exige o consentimento do responsável legal, papel geralmente exercido pelos pais, quando se trata de dados de menores de idade. Considerando tal público e seu interesse em jogos, a lei endereça um parágrafo para deixar restrita a captura de dados nestes casos, assim como solicita que se trabalhem elementos além dos meramente textuais com o intuito de oferecer melhor experiência e entendimento das crianças e adolescentes ao fornecer seus dados. A lei também exige que o Controlador e o Operador tenham uma gestão rigorosa de tudo o que for feito com os dados. Também exige que seja enviada para o Titular, a qualquer momento que por ele for solicitada, uma declaração contendo a discriminação dos dados e de seus tratamentos.

Entre os direitos dos usuários sobre os seus dados estão aconfirmação da existência de

tratamentos consentidos, a revogação de seu consentimento de acesso aos dados, assim como devida correção, anonimização, bloqueio ou eliminação do que não concordar; portabilidade a terceiro que indicar; informações sobre possíveis compartilhamentos.

De forma simplificada, o Poder Público pode coletar dados e tratá-los, além das hipóteses do consentimento, nos casos em que houver persecução do interesse público, para executar suas competências legais ou cumprir com suas atribuições. Ou seja, caso o Poder Público precise realizar algum ato previsto em lei, poderá coletar os dados necessários, com ou sem o consentimento do Titular. Isso não exclui os direitos do Titular com relação à transparência, ou seja, ele pode solicitar uma declaração de todos os dados aos quais o Poder Público tem acesso, quais os tratamentos realizados, assim como compartilhamentos, mas não pode solicitar exclusão ou bloqueio se o tratamento estiver previsto nas hipóteses apresentadas. Caberá à ANPD a responsabilidade de fiscalizar eventuais abusos ou desvios do Poder Público com relação ao uso dos dados, assim como cabem a ela eventuais pareceres técnicos sobre dúvidas não endereçadas pela lei.nNa sequência, a lei também tem como foco a fiscalização da aplicação da lei, versando especialmente sobre as sanções administrativas a serem aplicadas pela ANPD, além de eventuais sanções civis ou penais. A lei também determina as responsabilidades da ANPD e do Conselho Nacional de Proteção de Dados Pessoais que basicamente é uma entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República e da Privacidade (CNPDPP). As sanções administrativas seguem uma gradação de advertência; multa simples; multa diária; bloqueio dos dados; eliminação dos dados; suspensão do funcionamento do banco de dados; suspensão do exercício do tratamento de dados; proibição parcial ou total do exercício de atividades que se relacionem com o tratamento de dados. Além dessas sanções, há também a possibilidade de dar ampla publicidade à infração, e, em todos os casos, é preciso notificar o motivo do problema e as medidas corretivas planejadas e executadas.

6.1 CASOS QUE SÃO EXCEÇÕES À LGPD

A lei só não seram aplicadas ao tratamento de dados pessoais quando é: realizado por pessoa natural para fins particulares. Realizado para fins jornalísticos ou artísticos ou acadêmicos. Realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (que será objeto de lei

específica); ou provenientes de fora do território nacional e que não seja objeto de comunicação, uso compartilhado com agentes de tratamento brasileiros ou objeto de transferência de dados com outro país que não o de proveniência, desde que este país de proveniência proporcione grau de proteção adequado aos da lei brasileira.

6.2 LGPD E SUA APLICAÇÃO NO ÂMBITO EMPRESARIAL

Como já mencionado, a Lei Geral de Proteção de Dados se aplica a toda empresa ou organização pública ou privada que processa dados pessoais de usuários localizados no Brasil. Portanto, todas as empresas que se encaixam de alguma forma nessas características, então a implantação da LGPD é obrigatória.

A aplicação desta Lei nas empresas irá alterar o modo como a mesma processa os dados pessoais de seus clientes, funcionários, leads e contatos. O primeiro passo para a aplicação desta Lei em uma empresa é delimitar os seguintes aspectos: Análise do cenário geral sob a visão da LGPD; Realizar um mapeamento de dados e identificar a aderência de todas as informações coletas à Lei; Estruturar e qualificar todo e quaisquer dados conforme a Lei Geral de Proteção de Dados. Quando todos estes pontos já estiverem resolvidos, é preciso conferir a implantação dos procedimentos corretos do tratamento dos dados nos processos e no âmbito tecnológico. Para finalizar, é necessário aderir a um sistema de monitoramento que irá garantir que a adequação da Lei Geral de Proteção de Dados esteja de acordo com a Autoridade Nacional de Proteção de Dados. Neste processo de adequação, é preciso que as empresas providenciem alguns documentos que irão provar que estão em conformidade com a Lei Geral de Proteção de Dados. Um desses documentos deve conter a descrição de todos os processos que a empresa utiliza para fazer o tratamento dos dados pessoais de todos os indivíduos envolvidos com a mesma. O outro documento é o que prova quais os mecanismos e quais as medidas estão voltados a atenuação de riscos, como treinamentos, auditorias e modificações de contratos. A aplicação incorreta ou a não implementação da Lei Geral de Proteção de Dados pode ocasionar multas e, até mesmo, o fechamento da empresa e a proibição total da execução de atividades relacionadas ao tratamento de dados pessoais.

6.3 COMPARTILHAMENTO DE DADOS PELAS EMPRESA

A lei também estipula que este compartilhamento de dados deve ser feito somente com

autorização e consentimento explícito do titular, e deve também informá-lo de que forma eles serão utilizados na empresa.

O ideal é definir processos e práticas para todos os colaboradores, garantir que eles estejam seguindo ativamente, e educá-los sobre a importância dessas medidas. A empresa também pode implementar: Criptografia de dados; Monitoramento de atividades; Contratar ferramentas antivírus; Usar autenticação de dois fatores; Criar senhas fortes; Escolher locais seguros para armazenar dados.

7.0 CASOS EM QUE HOUVERAM VAZAMENTO DE DADOS NO BRASIL

Segundo a pesquisa recentemente feita pelo Massachusetts Institute of Technology (MIT), os vazamentos de dados aumentaram 493% no Brasil. Para esclarecer como esses crimes ocorrem, fora explicado alguns casos de vazamentos de dados que foram tratados com a LGPD no Brasil. Essa grande porcentagem de dados vazados apresentados pelo Massachusetts Institute of Technology reforça a importância da Lei Geral de Proteção de Dados que está em vigor no Brasil desde 2020 e agora teve suas sanções administrativas valendo a partir de agosto de 2021 (Veirago Advogados, 2021).

A Cyrela foi a primeira empresa brasileira a ser condenada por vazamentos de dados tratados com a LGPD. O caso aconteceu em novembro de 2018 e teve seu desfecho na justiça em 2020, com a decisão de indenização de R$10 mil ao cliente que teve seus dados partilhados com parceiros da empresa sem sua autorização. Tudo começou quando um cliente fechou a compra de um apartamento com a Cyrela em 2018. Depois ele começou a receber ligações de instituições financeiras e empresas de decorações ofertando serviços para seu imóvel recém adquirido. O cliente abriu um processo contra a empresa e ganhou com base na LGPD e seus direitos previstos no Código de Defesa do Consumidor. A juíza Tonia Yuka Koroku, da 13ª Vara Cível de São Paulo, interpretou que a Cyrela feriu preceitos como a honra e privacidade do cliente, além de violar sua intimidade ao revelar seus dados e detalhes da compra do imóvel. Além da indenização, a empresa foi condenada a não repassar mais os dados pessoais ou financeiros de clientes, sob pena de multa de R$ 300,00 a cada contrato mal utilizado (softwall, 2021).

A Operação Deepwater, em janeiro de 2021, a Autoridade Nacional de Proteção de Dados (ANPD) requisitou que a Polícia Federal abrisse uma investigação para apurar o vazamento de dados de mais de 223 milhões de brasileiros, número maior que a população do país, levando em conta que esses dados incluiam pessoas que já são falecidas. Psafe, foi a empresa responsável pelo vazamento. Em um comunicado divulgado na época, a ANPD informou que iria "apurar a origem, a forma em que se deu o possível vazamento, as medidas de contenção e de mitigação adotadas em um plano de contingência, as possíveis consequências e os danos causados pela violação". O vazamento incluía nome completo das pessoas, fotos, endereço, renda mensal e CPF, entre outras informações pessoais. Até hoje, não tem conhecimento de onde veio a fonte das informações. A principal suspeita é que haja mais de uma fonte e que os dados tenham sido agregados durante anos. O relatório da Polícia Federal sobre o caso ainda não foi concluído. Em março, a PF cumpriu mandados de prisão autorizados pelo ministro Alexandre de Moraes, do Supremo Tribunal Federal (STF), na Operação Deepwater. Foram presos em Uberlândia (MG) e em Petrolina (PE) dois suspeitos de terem oferecido o banco de dados em fóruns na internet (Alexandre Aragão, 2022).

O caso de vazamento de dados no Ministério da Saúde, em dezembro do ano de 2020, a reportagem do jornal O Estado de S. Paulo revelou que dados de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) ou como beneficiários de planos de saúde ficaram expostos na internet por falhas de segurança do Ministério da Saúde. As informações que ficaram expostas na internet, que incluiam nome completo, CPF, endereço e telefone, deveriam estar protegidas por login e senha, mas, infelizmente, havia uma vulnerabilidade no código que permitia que qualquer usuário consultasse o banco de dados. Uma falha semelhante já havia sido reportada ao ministério pela Open Knowledge Brasil (OKBR), organização do terceiro setor que promove segurança digital, transparência e acesso a dados públicos. Em nota ao jornal, o Ministério da Saúde afirmou que "os incidentes reportados estão sendo investigados para apurar a responsabilidade da exposição de base cadastral do ministério". A pasta acrescentou também que "ações de segurança estão sendo tomadas para impedir novos incidentes, tal como ações administrativas para apurar o ocorrido". Desde o momento, outro sistema do Ministério da Saúde ficou fora do ar durante meses, por uma possível ação de hackers. Em dezembro do ano de 2021, o DataSUS ficou inacessível, deixando os cidadãos sem informações. O problema demorou quase um mês para ser sanado (Alexandre Aragão, 2022).

A H&M foi acusada de coletar informações impertinentes ao trabalho de seus colaboradores, como práticas religiosas, histórico de doenças e dados familiares. A lei de proteção de dados da União Europeia não perdoou a empresa e a puniu no valor de 35,3 milhões de euros (softwall, 2021).

No ano de 2016 a Uber decidiu esconder um vazamento de dados que acorreu em sua plataforma e afetou 7 milhões de motoristas e 57 milhões de usuários, destes, 196 mil eram brasileiros. O caso foi descoberto em 2018 e nesse mesmo ano também ocorreu a sua punição, com uma multa de 148 milhões de dólares. O vazamento aconteceu devido a um ataque de hackers ao sistema da empresa. Na época, a Uber tentou esconder o caso embaixo do tapete, oferecendo 100 mil doláres para os hackers responsáveis, que concordaram manter em segredo o escândalo. A revelação do ataque veio a público quando o ex-diretor de segurança da empresa foi demitido e, durante uma auditoria externa no setor, encontrou-se o vazamento de telefones, nomes, e-mails e carteiras de motoristas expostas no ataque (Felipe Demartini, 2022).

8.0 REGRAS QUE DEVEM SER SEGUIDAS

A cerca dos técnicos do time, a LGPD prevê que dentre os agentes de tratamento de dados pessoais: tem o controlador, que é a quem compete as decisões relativas ao tratamento; tem o operador, que é quem realiza o tratamento, em nome do controlador. Também existe o encarregado que, é o responsável por atender as demandas dos titulares, interagir com a ANPD e orientar funcionários e contratados quanto às práticas de proteção de dados pessoais e ele poderá ou não ser exigido, a depender da natureza ou porte da empresa e do volume de dados tratados por ela (Lei 13.709, 14/08/2018). Com relação ao gerenciamento dos dados, cabe identificar, entre as informações que gerencia, quais são dados pessoais (cheque também se há aqueles que exigem um tratamento ainda mais específico, como os sensíveis, e sobre crianças e adolescentes). Verifique os meios em que se encontram, seja no meio físico ou digital (Lei 13.709, 14/08/2018). Pertinente ao consentimento: O titular deve concordar, de forma explícita e inequívoca, que seus dados sejam tratados. E o empresário deve fazer esse tratamento levando em conta princípios da LGPD, sendo estes: finalidade, adequação, livre acesso, qualidade dos dados, transparência, prevenção, não discriminação, responsabilização (Lei 13.709, 14/08/2018). Para uma melhor adaptação com relação a prevenção de erros: Construa planos de contingência para tratar incidentes de segurança e trate os problemas com agilidade. Faça auditorias de tempos em tempos (Lei 13.709, 14/08/2018). ´E primordial adquirir ransparência

e proatividade: Seja ágil no atendimento aos pedidos do titular dos dados, segundo os critérios definidos pela LGPD e pela autoridade nacional. Se causou, comprovadamente, algum dano patrimonial, moral, individual ou coletivo, responda por eles. Tenha atenção, ainda, às questões sobre quando deve encerrar um tratamento e informe sobre o término ao titular (Lei 13.709, 14/08/2018). Uma lei Extraterritorial: A LGPD se aplica a empresas que não ou têm estabelecimento no Brasil, e/ou oferecem produtos e serviços ao mercado brasileiro, e/ou coletam e tratam dados de pessoas que estejam no país. Vale lembrar que não interessa: se o titular dos dados é brasileiro ou não; qual o meio de operação de tratamento dos dados (físico ou digital); qual o país sede da empresa; se os dados estão hospedados em datacenters no país ou não. Vale reforçar que a LGPD permite a transferência de dados além-fronteira, desde que seja: com o consentimento específico do titular; a pedido do titular para que esse possa executar pré-contrato ou contrato; para proteção da vida e da integridade física do titular ou de terceiro; para ajudar na execução de política pública; para país ou organismo internacional que projeta dados pessoais de forma compatível com o Brasil; para cooperar juridicamente com órgãos públicos de inteligência, investigação, ou por conta de compromisso assumido via acordo internacional; para cumprir obrigação legal; com a autorização da ANPD; comprovado que o controlador segue a LGPD na forma de normas globais, selos, certificados e códigos de conduta (Lei 13.709, 14/08/2018).

9.0 PRESSUPOSTOS TEÓRICOS.

A lei é muito recente e o Brasil tem ainda um longo caminho para percorrer até que possamos alcançar de maneira efetiva os direitos fundamentais de liberdade, intimidade e privacidade de nossos dados. Ainda existem questões complexas, como a Autoridade Nacional de Proteção de Dados e como ela irá elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, além de como irá fiscalizar e aplicar sanções em caso de descumprimento da legislação. Este é um enorme avanço nos direitos fundamentais de liberdade e de privacidade e certamente ajudará o Brasil na sua evolução. O espírito da lei é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para a governança da segurança das informações, do outro lado, dentro do ciclo de vida do uso da informação que identifique ou passa

identificar uma pessoa e o que estiver relacionada a ela, incluindo a categoria de dados sensíveis. A nova lei prevê em seu teor 9 hipóteses que tornam legais os tratamentos de dados. Dentre eles, 2 merecem destaque: É necessário obter o consentimento explícito por parte do titular dos dados. Ou seja, ele deverá ser claramente informado dos termos de uso e extensão da autorização e precisa concedê-lo livremente. A partir ddo momento em que a lei foi sancionada, uma empresa só poderá recolher determinados dados a partir da autorização do proprietário desses dados, ou seja, o titular, comprovando que a sua coleta será útil para sua interação com seus consumidores.

10.0 – METODOLOGIA.

A cerca dos termos metodologicos, passaremos a explanar os fatores que nos levam a situar esta pesquisa dentro do paradigma qualitativo. Este estudo revela sua natureza qualitativa (Santos Filho & Gamboa, 2002; André, 2003; dentre outros), através de sua abordagem naturalística e holística do fenômeno em questão, uma vez que procura compreender, descrever e interpretar o processo de partição do conhecimento a cerca da LGPD e sua influência para com a sociedade brasileira "em seu acontecer natural, sem a manipulação de variáveis ou tratamento experimental" (André, 2003: 17).

O presente estudo tem também caracter bibliográfico. Segundo Matos & Vieira (2002: 49), um estudo define-se como bibliográfico ao realizar um trabalho "a partir de um levantamento de material com dados já analisados, e publicados sobre o tema que se deseja conhecer", ou seja, a pesquisa bibliográfica envolve "fontes secundárias" (Gonsalves, 2003:).

O objetivo principal foi utilizar das revisões bibliograficas para encontrar uma resposta mais próxima possível para o problema apresentado.

A escolha do tema, ocorreu após uma série de analises sobre diversos assuntos, sendo este, o que mais chamou a atenção do autor deste presente trabalho.

Após o compreendimento a cerca do assunto que será abordado no decorrer do projeto, fora feita uma pesquisa bibliografica que tem por objetivo uma análise relativamente superficial a cerca dos tópicos mais importantes que se relacionam com o tema. Para um maior compreendimento a cerco do tema, foi realizado um levantamento de dados que consiste na reunião e organização de dados que darão embasamento ao projeto propriamente dito. Tal pesquisa fora feita com base no projeto de pesquisa produzida pelos seguintes autores:

Beatriz Cardoso, com a sua pesquisa retratando "o que é a GDPR? Entenda o que muda para

você com a nova lei", esta que fora feita no ano de 2018. **Felipi Demartini,** produziu uma pesquisa sobre o tema: "Uber sofre vazamento de dados internos em ataque cibernético", tal pesquisa que é recente, do ano de 2022. **Miguel Mendoza,** citando "Por que é importante proteger seus dados pessoais?", tal pesquisa fora divulgada no ano de 2016. **Cairo Noleto,** tratando sobre a **"**LGPD: o que é, por que foi criada e o que muda?", no ano de 2020. **Carlos Oliveira,** comentando a cerca da "LGPD: A importância dos dados pessoais", pesquisa realizada no ano de 2020. **Sérgio Pohlmann, com o seu livro intitulado:** "LGPD Ninja: Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas". Sendo esta a 2° Edição. Lançada no estado do Rio de Janeiro, pela Editora Fross, no ano de 2019. **Herique Raabello,** dissertando a certca da **"**LGPD: entenda como surgiu a nova Lei Geral de Proteção de Dados", sendo tal essa do ano de 2019. Os pesquisadores **Vasconcelos, Charles Rogério; Salib, Marta Luiza Leszczynski,** Com o tema: "LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: Desafios e impactos para o Poder Público", produzido no estado de Rondônia, no ano de 2020.

O processo de uma maior busca a cerca da literatura ocorrerá novamente, caso a pesquise necessite de maiores avanços bibliográficos. Caso seja necesssário uma revisão bibliografia mais aprodundada, então, será desenvolvida uma nova versão final desta pesquisa, visando um maior aprofundamento do conteúdo.

Ao final, com uma versão final do projeto elaborada. O autor deste presente trabalho irá compartilhá-lo com colegas de trabalho e pessoas mais próximas.

11.0. Cronograma de execução da pesquisa.

Periodo	2022											
Meses	Mês 01	Mês 02	Mês 03	Mês 04	Mês 05	Mês 06	Mês 07	Mês 08	Mês 09	Mês 10	Mês 11	Mês 12
Pesquisa Bibliografica			**X**	**X**								
Definição do Tema	**X**	**X**										
Definição da Metodologia					**X**	**X**						
Entrega do Projeto								**X**				
Apresentação do Projeto									**X**			
Discurssão dos resultados										**X**		
Elaboração da Conclusão							**X**					
Ajustes Finais											**X**	
Apresentação do TCC											**X**	
Entrega versão final												**X**

12. Referências Bibliográficas.

ADVOGADOS, Veirano. Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT. **chc ADVOCACIA**, 2021. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-

493-no-brasil-segundo-pesquisa-do-mit/. Acesso em: 02 nov. 2022.

Antunes, Deborah. Big Data, exploração ubíqua e propaganda dirigida: novas facetas da indústria cultural. **Scielo,** 2018 .Disponivel em: tps://www.scielo.br/j/pusp/a/xkMCGk7zrtXX4TT8jqhnfHv/. Acesso em: 23 nov. 2022.

BBC NEWS. Empresas como Google, Amazon e Facebook estão ficando grandes demais?. **BBC News**, 2017. Disponível em: https://www.bbc.com/portuguese/geral-40205922. Acesso em: 02 nov. 2022.

Carmargo e Vieira Blog, 2020. Disponível em: https://blog.camargoevieira.adv.br/caso-cambridge-analytica-entenda-como-ele-influenciou-a-lgpd/ Acesso em: 23 out. 2022.

CARDOSO, Beatriz. O que é a GDPR? Entenda o que muda para você com a nova lei. **techtudo**, 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/05/o-que-e-a-gdpr-entenda-o-que-muda-para-voce-com-a-nova-lei.ghtml. Acesso em: 25 out. 2022.

CENTRIC. O que é GDPR? E seu impacto no Brasil. **CENTRIC SOLUTION**, 2021. Disponível em: https://centric.com.br/blog/o-que-e-gdpr/. Acesso em: 25 out. 2022.

Compugraf. Por que existe a LGPD? – Por trás da lei. **Compugraf**, 2018. Disponível em: https://www.compugraf.com.br/por-que-existe-a-lgpd/. Acesso em: 09 dez. 2020.

CRUZ, Carlos Henrique. Lei Geral de Proteção de Dados: 5 motivos para implementá-la agora mesmo!. **chc ADVOCACIA**, 2020. Disponível em: https://chcadvocacia.adv.br/blog/lei-geral-de-protecao-de-dados/. Acesso em: 09 dez. 2020.

DEMARTINI, Felipi. Uber sofre vazamento de dados internos em ataque cibernético. **Canaltech**, 2022. Disponível em: https://canaltech.com.br/seguranca/uber-sofre-vazamento-de-dados-internos-em-ataque-cibernetico-225474/. Acesso em: 02 nov. 2022.

INVENTTI. GDPR: Como o Regulamento de Proteção de Dados afeta o Brasil. **inventti**, 2020. Disponível em: https://inventti.com.br/gdpr-como-afeta-brasil/. Acesso em: 25 out. 2022.

LEGALCLOUD. Lei Geral de Proteção de Dados: Um Resumo da LGPD (ATUALIZADO). **Legalcloud**, 2018. Disponível em: https: https://legalcloud.com.br/lei-geral-de-protecao-de-dados-resumo-lgpd/. Acesso em: 26 out. 2022.

Lopes&Castelo. Dados Sensíveis da LGPD: Quais são e por que devo protegê-los?. **Lopes&Castelo Sociedade de advogados**, 2021. Disponível em: https://lopescastelo.adv.br/dados-sensiveis-da-lgpd-quais-sao-e-por-que-devo-protege-los-2/. Acesso em: 02 nov. 2022.

MENDOZA, Miguel. Por que é importante proteger seus dados pessoais?. **welivesecurity**, 2016. Disponível em: https://www.welivesecurity.com/br/2016/06/28/proteger-dados-pessoais/. Acesso em: 25 out. 2022.

NEGÓCIOS. Por que os dados pessoais são importantes?. **Jusbrasil**, 2020. Disponível em: https://fabiolafgrimaldi.jusbrasil.com.br/artigos/828886498/por-que-os-dados-pessoais-sao-importantes. Acesso em: 25 out. 2022.

NOLETO, Cairo. LGPD: o que é, por que foi criada e o que muda?. **Betrybe**, 2020. Disponível em: https://blog.betrybe.com/tecnologia/lgpd-lei-geral-de-protecao-de- dados/. Acesso em: 09 dez. 2020.

NOLETO, Cairo. O que você precisa saber sobre como seus dados pessoais são coletados — e quem os utiliza. **NEGÓCIOS**, 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/04/o-que-voce-precisa-saber-sobre-como-seus-dados-pessoais-sao-coletados-e-quem-os-utiliza.html. Acesso em: 25 out. 2022.

OLIVEIRA Carlos. LGPD: A importância dos dados pessoais. **Jusbrasil**, 2020. Disponível em: https://carloswag.jusbrasil.com.br/artigos/820978158/lgpd-a-importancia-dos-dados-pessoais. Acesso em: 25 out. 2022.

Paredes,Arthur. Avanços tecnologicos: vantagens e desvantagens. **IEBS,** 2019. Disponivel em: https://www.iebschool.com/pt-br/blog/software-de-gestao/tecnologia/avancos-tecnologicos-vantagens-e-desvantagens/. Acesso em: 23 nov. 2022.

Pizzato, Giovana. A Proteção de Dados Pessoais na Internet no Brasil: uma breve análise da nova Lei n. 13.709 de 14 de Agosto de 2018. **Jusbrasil,** 2019. Disponivel em: https://giovanapbruno1.jusbrasil.com.br/artigos/770637321/a-protecao-de-dados-pessoais-na-internet-no-brasil-uma-breve-analise-da-nova-lei-n-13709-de-14-de-agosto-de-2018. Acesso em: 23 nov. 2022.

POHLMANN, Sérgio. LGPD Ninja: Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas. 2° Edição. Rio de Janeiro: Editora Fross, 06-08-2019.

REBELLO, Herique. LGPD: entenda como surgiu a nova Lei Geral de Proteção de Dados. **Alterdata**, 2019. Disponível em: https://blog.alterdata.com.br/introducao- algpd-entenda-como-surgiu-a-nova-lei-geral-de-protecao-de-dados/. Acesso em: 09 dez. 2020.

SERPRO. Como cumprir a LGPD?. **gov.br**, 2020. Disponível em: https://www.serpro.gov.br/lgpd/empresa/como-cumprir-a-lgpd. Acesso em: 26 out. 2022.

SERPRO. O que são dados anonimizados, segundo a LGPD. **gov.br**. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd. Acesso em: 25 out. 2022.

Vasconcelos, Charles Rogério; Salib, Marta Luiza Leszczynski. **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: Desafios e impactos para o Poder Público**, Rondônia: 2020.

[26] **Reynan Da Silva Dias Paiva. Cursnado Ciência Da Computação na UFBA. Contato: <reynanwq@gmail.com>.**