LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E GENERAL DATA PROTECTION REGULATION (GDPR): UMA ANÁLISE ENTRE OS PRINCIPAIS ELEMENTOS DAS LEGISLAÇÕES E SUAS SANÇÕES AOS CASOS DE VAZAMENTO DE DADOS[1]

GENERAL DATA PROTECTION LAW (LGPD) AND GENERAL DATA PROTECTION REGULATION (GDPR): AN ANALYSIS OF THE MAIN ELEMENTS OF THE LEGISLATIONS AND THEIR SANCTIONS FOR DATA BREACH CASES

Maria Eduarda Marçal VILELA[2]

Cildo GIOLO JÚNIOR[3]

RESUMO

A presente pesquisa teve por objetivo principal a realização de uma análise da LGPD, no Brasil, e da GDPR, na União Europeia, a fim de compreender suas motivações ante as características que a sociedade contemporânea vem assumindo, bem como seus princípios norteadores e objetivos além analisar suas sanções e punições em casos de descumprimento por vazamentos de dados a partir da ótica de cada uma. A fim de exemplificar e tornar mais concreto o que foi desenvolvido ao longo de todo o trabalho, foram apresentados casos os quais foram julgados pelas legislações em questão, em virtude do descumprimento das mesmas.A principal fonte de pesquisa consistiu em pesquisas

[1]O presente artigo sintetiza a monografia de conclusão da pesquisa, realizada para o Programa Internode Bolsas de Iniciação Científica (PIBIC 2022-2023) da Faculdade de Direito de Franca (FDF),Franca/SP.

[2]DiscentedaFaculdadedeDireitodeFranca(FDF),Franca/SP.BolsistadoProgramaInternodeBolsasde IniciaçãoCientífica(PIBIC2022-2023)

[3]Pós-Doutor em Direitos Humanos pelo "Ius Gentium Conimbrigae" (IGC/CDH) da Faculdade de Direito da Universidade de Coimbra (Portugal). Doutor em Direito pela Universidade Metropolitana de Santos, Santos - São Paulo (Brasil). Doutor em Ciências Jurídicas e Sociais pela UMSA, Buenos Aires - Capital Federal (Argentina). Mestre em Direito Público pela Universidade de Franca.

bibliográficas exploratórias a partir de legislação, doutrinas, artigos científicos, páginas de web sites, entre outros. Assim, sendo possível estabelecer um contato direto com um grande número de materiais já escritos acerca do tema em questão, tanto no âmbito nacional, quanto internacional.
Palavras-Chave: Direito Digital; Dados Pessoais; Lei Geral de Proteção de Dados (LGPD); General Data ProtectionRegulantion (GDPR).

ABSTRACT
The mainpurposeofthisresearchwastoconductananalysisofthe LGPD in Brazilandthe GDPR in theEuropean Union, in ordertocomprehendtheirmotivations in light ofthecharacteristicsthatcontemporarysocietyhasbeenassuming. Additionally, thisstudyaimedto explore theirguidingprinciplesandobjectives, as well as to examine theirsanctionsandpenalties in cases of non-compliance with data breachesfromthe perspective ofeachregulation. Toprovide concrete examplesandsolidifythefindingsthroughouttheresearch, cases thatwereadjudicatedundertherespectivelegislationsduetotheirviolationswerepresented. The primarysourcesofresearchencompassedexploratorybibliographicstudiesinvolvinglegislation, doctrines, scientificarticles, websites, andotherrelevantmaterials. This approach facilitated direct engagementwith a significant volume ofpre-existingliteratureconcerningthesubjectmatter, bothatthenationalandinternationallevels.
Keywords: Digital Law; Personal Data; GeneralData Protection Law (LGPD); General Data ProtectionRegulation (GDPR).

1 INTRODUÇÃO

A sociedade contemporânea com seus avanços tecnológicos e digitais conectam os cidadãos às mais variadas plataformas, aplicativos, redes sociais e demais meios capazes de coletar dados e informações pessoais, e, assim, armazená-los e manuseá-los de forma com que a privacidade esteja em uma posição de vulnerabilidade e insegurança.

Diante desse cenário, uma discussão a respeito da proteção de dados tornou-se algo recorrente, e, embora o Direito seja uma ciência que demanda contínua e ininterrupta inovação e atualização, a lei não conseguiu acompanhar tais mudanças no âmbito geral, e dessa forma mostrou-se necessária a criação de legislação específica, culminando em duas regulamentações distintas: a *General Data Protection Regulation*, a GDPR na União Europeia, e a Lei Geral de Proteção de Dados, a LGPD no Brasil.

A GDPR, ou Regulamento Geral Sobre a Proteção de Dados, é a lei que visa à proteção de dados pessoais e privacidade dos indivíduos da União Europeia. Seu objetivo principal é permitir que os usuários tenham controle e conhecimento das formas de tratamento e armazenamento de seus dados pessoais, a partir das empresas ou quem quer que os solicite. Então, é possível que as pessoas tenham a opção de aceitar ou não tal

fornecimento, além de obrigar os receptores a se responsabilizarem pelos atos, a partir das normas relacionadas ao manuseio de tais informações.

O Brasil criou a Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709, de 14 de agosto de 2018, entretanto, só entrou em vigor no ano de 2020.

Inspirada na GDPR, seu objetivo está na defesa dos direitos fundamentais à privacidade e liberdade, que recaem, por sua vez, na proteção dos dados pessoais. Destarte, ainda que tardiamente, a criação desse dispositivo representa um marco histórico na regulamentação do tratamento de dados pessoais no país.

No âmbito das consequências jurídicas aplicadas aos "autores" de vazamentos de dados, as sanções estão regulamentadas nos artigos da LGPD, mas a indenização por esses atos exige prova de dano, o que abrange um conhecimento além da legislação específica. Isso demonstra a importância de se comparar a norma brasileira, com a regulamentação europeia.

Portanto, essa pesquisa tem por objetivo analisar a LGPD, no Brasil, e a GDPR, na União Europeia, buscando compreender seus princípios e fundamentos norteadores, bem como descrever suas sanções e punições em casos concretos, como o caso Google e o da empresa *Telekall Infoservice.*

Para tanto, a metodologia utilizada consiste em uma revisão de literatura, com extensa pesquisa bibliográfica e exploratória, a partir de legislação, doutrinas, jurisprudências, artigos científicos, revistas e relatórios nacionais e internacionais, jornais, tabelas estatísticas, e todo material que agregue fundamentação teórica sobre o tema.

Os tópicos abordados são: os marcos regulatórios da proteção de dados digitais, descrevendo os caminhos adotados para a criação da GDPR e da LGPD; seus contextos, processos de criação e desenvolvimentos das leis, princípios, fundamentos e objetivos, efetividade; dados sensíveis e sanções, o que são, seu vazamento sob a ótica de ambas as regulamentações; comparações de casos julgados por ambas as leis; exploração dos casos da Google e da *TelekallInfoservice*.

Concluindo, assim, um trabalho teórico, com elaboração possíveis soluções aos casos propostos, visando equilibrar os conflitos de interesses, e também estudar casos concretos semelhantes.

2 MARCOS REGULATÓRIOS DA PROTEÇÃO DE DADOS DIGITAIS: A PRIVACIDADE E SUA INFLUÊNCIA NOS CAMINHOS ADOTADOS PARA A CRIAÇÃO DA GDPR E DA LGPD

2.1 A PRIVACIDADE NA ERA DIGITAL

A proteção da privacidade pessoal, nem sempre foi um assunto discutido e debatido na área jurídica com a devida proporção que lhe é cabida.

Antes de ser tratada como um direito fundamental, a privacidade não era entendida como um direito autônomo. Era entendida como um reflexo do direito à liberdade, propriedade e até mesmo do direito à honra. Pode-se dizer que era estabelecida em conformidade com seu ciclo social e suas prioridades, ou seja, um liame subjetivo do direito.(Sampaio, 2018, p. 33-34)

Somente no final do século XIX que os pesquisadores *Warren* e *Brandeis*, publicaram o artigo *The RighttoPrivacy*, na revista de Direito da faculdade de Harvard, a *Harvard Law Review*, o qual teve grande inspiração nos avanços tecnológicos vivenciados à época.

Com inspiração no artigo publicado na revista de Harvard, a privacidade passou a fazer parte da Declaração Universal dos Direitos do Homem, e, a partir da ideia apresentada por Warren e Brandeis e das grandes transformações ocorridas no século XX, de forma gradual, a privacidade deixou de ser entendida apenas como um reflexo de áreas do direito e destinada somente ao íntimo do indivíduo, para ser enxergada como um direito real e concreto, hoje englobado nas constituições dos Estados.

Na esfera digital e tecnológica, a internet adquiriu um papel fundamental e pode-se dizer essencial nas relações dos indivíduos, sejam elas pessoais, de trabalho ou até mesmo comerciais. A facilidade com que as informações são transmitidas e a velocidade que acontecem as conexões têm impactado significamente na vida dos usuários, gerando assim uma evidente Evolução Tecnológica. (Machado, 2014)

Essas mudanças nas relações, com a consequente Evolução Tecnológica, são entendidas e nomeadas por Canto (2019, p.31), como Hiperconectividade.

Magrani (2018, p.20) definiu a hiperconectividade como:

> O termo hiperconectividade foi cunhado inicialmente para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento. Esse termo possui alguns desdobramentos importantes. Podemos citar alguns deles: o conceito de always-on, estado em que as pessoas estão conectadas a todo o momento; a possibilidade de estar prontamente acessível (readilyaccessible); a riqueza de informações; a interatividade; e o armazenamento ininterrupto de dados (alwaysrecording). O termo hiperconectividade encontra-se hoje atrelado às comunicações entre indivíduos (person-to-person, P2P), indivíduos e máquina (human-to-machine, H2M) e entre máquinas (machine-to-machine, M2M) valendo-se, para tanto, de diferentes meios de comunicação. Há, neste contexto, um fluxo contínuo de informações e uma massiva produção de dados.

Nesse sentido, tem-se a conclusão de Vidal (2017, p. 4), aplicada ao entendimento amplo, atual e ligado à era digital, da Privacidade:

> A privacidade não pode ser vista somente através da ótica da invasão (como decorre dos conceitos de direito de estar só e de resguardo contra interferências alheias), ela deve ser tida também como controle de dados pessoais e de acesso a tais dados. Contudo, entendê-la somente neste sentido, também, não é suficiente, visto que estaria deixando de lado a questões atinentes à tomada de decisões no âmbito da vida privada e da própria invasão da mesma.

Dessa forma, ante a importância da privacidade no cenário das grandes mudanças e inovações tecnológicas, foi visualizada a necessidade de criação de regulamentações específicas e destinadas à proteção da privacidade voltada aos dados pessoais. Sendo criadas assim a GDPR na União Europeia e posteriormente a LGPD no Brasil.

2.2 O GDPR: SEUS FUNDAMENTOS, OBJETIVOS E PRINCÍPIOS

Em meio à desenfreada globalização e grandes avanços tecnológicos, digitais nos mais diversos âmbitos sociais, entrou em vigor em 25 de maio de 2016 a *General Data ProtectionRegulation*, o GDPR.

Diante o contexto de avanços do mercado europeu internacional, principalmente na área digital e de serviços fornecidos via internet, mostrou-se de extrema necessidade uma regulamentação mais específica aos dados pessoais.

Dessa forma, em meados de 1950, as primeiras noções a respeito da privacidade pessoal, tomaram forma. Foram criadas a Declaração Universal dos Direitos Humanos (1948) pela ONU e Declaração Europeia dos Direitos do Homem (1950). Tais declarações carregavam consigo o ideal democrático que surgiram no contexto pós 2ª Guerra Mundial.

Ambas as declarações, em seus artigos 12º[3] e 8º[4], respectivamente, versavam sobre a privacidade, embora que de forma simples e vaga, para a época, a discussão e legislação acerca de tais temas, de fato era um grande avanço.

Com o avanço global, as necessidades de regular os dados, foi se tornando cada vez maior, alguns países, como Suécia, Dinamarca, França e Alemanha, por volta de 1970, começaram a criar suas legislações próprias a respeito da proteção de dados, entretanto, todas as leis eram genéricas e restritas somente aos países mencionados. (Doneda, 2018. p. 197)

Mais adiante, em 1980, a Comunidade Econômica Europeia, adotou a Convenção 108, a qual aconteceu Strasbourg. Tal convenção estabelecia o livre fluxo de dados entre seus membros signatários, modo de garantir ainda mais a proteção, uma vez que todos obedeciam às diretrizes por ela estabelecidas, entretanto aos Estados não membros da, eram estabelecidos alguns critérios para o fluxo de dados.

Nesse sentido, foi definida pelo Conselho Europeu como "primeiro instrumento internacional vinculativo que protege o indivíduo contra os abusos que podem acompanhar a recolha e o tratamento de dados pessoais e que visa regular ao mesmo tempo o fluxo transfronteiriço de dados pessoais". (Conselho Europeu, 1981).

[3]Art 12:Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

[4]Art 8: Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

Posteriormente, após um período de quase duas décadas, marcado pela globalização cada vez mais desenfreada e o grande interesse econômico em dados pessoais, a em 1995 foi promulgada a Diretiva 95/46.

A Diretiva teve como objetivo principal estabelecer instrumentos a fim de promover uma igualdade e harmonia no tratamento dos dados pessoais pelos seus Estados-membros, ou seja, "traduzir, em normas mais específicas, a promessa antes firmada na Convenção de Strasbourg de assegurar aos indivíduos o controle sobre suas informações pessoais" (Bioni, 2020. p.117). Além disso, estabeleceu um rol de autoridades competentes para assumirem a responsabilidade de fiscalização, legislação e arbitragem envolvendo questões que adentrassem a esfera da proteção de dados pessoais. Tais autoridades eram denominadas autoridades centrais de proteção de dados. (Guidi, 2017, p. 8)

E por fim, passados anos sem grandes inovações na área de proteção ao tratamento de dados pessoais, em 2016, foi criado o GDPR, por meio do Regulamento 679/2016, que passou a substituir a Diretiva 95/46.

No contexto de criação do Regulamento supramencionado, a União Europeia enfrentava uma grande dificuldade na questão de uniformidade do tratamento de dados de seus países membros, em virtude da expansão do mercado interno europeu. Dessa forma, o GDPR busca unificar o tratamento de dados pessoais dentro da União Europeia.

> [...] as inconsistências na proteção de dados entre os Estados-Membros da União Europeia. Também foram destacadas pela Comissão Europeia, a necessidade de uma regulamentação única e harmoniosa da proteção de dados abrangendo todo o território da União Europeia, em particular a fim de remover ou reduzir a margem de escolha dos legisladores nacionais, das autoridades de controle e dos tribunais. (Diaz, 2016).

Por se tratar de um Regulamento, é aplicável a todos os Estados-membros da União Europeia, não sendo necessária regulamentação própria em cada Estado, contudo não impede a coexistências de regulamentações próprias nos países da UE. (Doneda, 2021, p. 195)

Fundamentada na unificação dos tratamentos dos dados pessoais dos países membros da União Europeia, o GDPR é organizado em

11 capítulos e 99 artigos, a legislação europeia, teve seu formato estabelecido de uma forma que pudesse sempre se manter atual, uma vez que as disposições tratadas envolvem tecnologia e dados, assuntos esses que apresentam constantes mudanças e inovações:

> Essa configuração é de imensa importância diante das dificuldades inerentes à regulação de um setor tão influenciado pelo desenvolvimento tecnológico, como é o caso dos dados pessoais. O importante, a essa altura, é perceber que essa estrutura hierarquizada de valores, princípios e regras é essencial por um fator crucial: a sincronia entre a lei e a realidade. Em um campo fático de rápida evolução, é importante que a lei mantenha um patamar mínimo de aplicabilidade e sejam, no mais, envidados esforços para a atualização constante das normas, de modo que estas possam acompanhar - ainda que a certa distância - o desenvolvimento tecnológico. (Guidi, 2017. p. 9)

No primeiro capítulo do regulamento europeu, o qual abrange os artigos 1º ao 4º, são estabelecidas todas as Disposições Gerais da lei, que versam desde seus objetivos, aplicação material e territorial, bem como as definições de conceitos-chaves estabelecidos pela legislação em questão, destacando-se no referido capítulo.

O Regulamento europeu evidencia que serão respaldados por ele os dados pessoais de cidadãos europeus, tratados de forma digital, bem como de formas manuais, as quais a lei se refere como ficheiros.

Importante destacar que o Regulamento é aplicado, por força do Direito Internacional Público, a qualquer país que trate dados pessoais de cidadãos da UE, ou seja, uma empresa estrangeira à União Europeia, deve seguir o regulamento acima retratado, pelo fato de manter interações com indivíduos europeus.

No artigo 4º, são definidos diversos conceitos-chave os quais são utilizados ao logo de toda a legislação, justificando suas importâncias. Dentre tais conceitos, alguns foram previamente definidos na Diretiva 95/46/CE, mas aprimorados pelo novo regulamento.

Tais disposições gerais possuem grande influência ao longo de todo o Regulamento, visto que são os tópicos basilares do mesmo.

A fim de estabelecer um norte e um limite ao que versa o Regulamento 679/2016 o capítulo II, que vai do artigo 5º ao 11º, traz

consigo os princípios que deverão ser observados no que tange ao tratamento de dados pessoais.

A partir da leitura da Lei é notório que os princípios estabelecidos versam sobre: a Licitude, Equidade e Transparência quanto ao tratamento dos dados pessoais.

Os princípios da Finalidade da coleta dos dados, da Minimização dos dados, da Confidencialidade e da Responsabilidade, se destacam por gerarem ramificações que baseiam os outros princípios secundários adotados.

Portanto, todos os Princípios têm como finalidade principal conferir maior segurança na proteção dos dados pessoais dos cidadãos, no caso europeus, tendo em vista que esses possuem maior vulnerabilidade, dessa forma garantindo amparo jurídico necessário para suprir tal condição.

Por fim, um dos tópicos que lei trata com maior importância se trata do consentimento, esse definido pelo regulamento como "uma manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;" esse sendo um requisito indispensável para que seja legal e legítimo tratamento de dados pessoais, pelo responsável por tal tratamento.

Ademais, é estabelecido também que o dono dos dados pessoais fornecidos tem a faculdade de retirar seu consentimento a qualquer momento, de forma igualmente simples à do consentimento, ensejando assim no descarte de tais dados.[5]

Por fim, o GDPR estabelece que é direito do titular dos dados pessoais a retificação ou apagamento de seus dados, quando solicitado, conforme disposto nos artigos 16º[6] e 17º[7].

É indiscutível o fato de que o GDPR foi um grande marco regulatório global, no que tange não só à privacidade, mas também a todos

[5] Art. 7º (3), GDPR: O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.

[6] Art. 16º, GDPR: O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

[7] Art. 17º, GDPR: O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

os âmbitos que unem tecnologia e informação. Serviu de “espelho” para diversas regulamentações referentes à proteção de dados pessoais, sendo a principal delas a Lei Geral de Proteção de Dados, que regula tal área no Brasil

O regulamento europeu determina que todos os dados pessoais de cidadãos europeus de países membros da UE devem ser tratados conforme regulam seus dispositivos. Tal fato culminado com a existência de entidades reguladoras de cada Estado- membro gerou um alcance muito alto em todos os países, tendo em vista a circulação cada vez mais acerbada de dados, garantindo assim o sucesso e eficácia do marco regulatório.

2.3 A LGPD: SEUS FUNDAMENTOS, OBJETIVOS E PRINCÍPIOS

Por grande influência da União Europeia com a criação e efetividade do GDPR, o Brasil voltou-se com mais foco ao tratamento de dados pessoais e cria a Lei Geral de Proteção de Dados, em 2018. Nesse sentido, Doneda estabelece sobre a regulamentação da proteção de dados pessoais no Brasil:

> A proteção de dados pessoais no ordenamento brasileiro somente se estruturou em torno de um conjunto normativo unitário muito recentemente. Seu desenvolvimento histórico se deu a partir de uma série de disposições cuja relação, propósito e alcance foram fornecidos pela leitura da cláusula geral da personalidade e efetivados a partir de estruturas como a defesa do consumidor, antes que fosse possível observar uma propensão autônoma para a proteção de dados. (Doneda, 2021. p. 206)

Antes da criação da LGPD, o Brasil não possuía uma regulamentação específica acerca do tema, mas o mesmo já vinha sendo tratado de maneira geral pela Constituição Federal de 1988 do dispositivo do *habeas data*.

O processo para chegar à LGPD, não foi célere. Por muitos anos, o Código de Defesa do Consumidor, especialmente em seus artigos 43 e 44, ao dispor sobre a regulamentação de bancos de dados e cadastros dos consumidores, foi o único diploma legal que tratava sobre proteção de dados em si.Nas palavras de Danilo Doneda:

> [...] a primeira das garantias a este respeito é a da transparência, como direito do consumidor de ser comunicado de que a informação a seu respeito está sendo processada (artigo 43, § 2º). Os outros direitos do consumidor estabelecidos pelo CDC no que toca à proteção de seus dados pessoais é o direito de acesso (correspondente ao princípio do livre acesso) e de retificação (correspondente ao princípio da qualidade). (DONEDA, 2006, p. 379).

Posterior ao Código de Defesa do Consumidor, a criação do o Marco Civil da Internet, foi um grande avanço na área legislativa da informação e tecnologia, que nas palavras de Tarcísio Teixeira:

> Trata-se de uma lei principiológica, pois estabelece parâmetros gerais acerca de princípios, garantias, direitos e deveres para o uso da internet no Brasil, além de determinar algumas diretrizes a serem seguidas pelo Poder Público sobre o assunto. (Teixeira, 2015, p. 5).

Voltando-se exclusivamente à uma legislação própria para proteção de dados pessoais, no ano de 2010, constatada a necessidade de uma lei acerca de tal tema, o Ministério da Justiça Brasileiro redigiu um Anteprojeto de Lei de Proteção de Dados (APLPD), o qual foi aberto à consulta e sugestões ao público, por meio de uma plataforma digital, a *culturadigital.org.*

Após alguns anos da realização da consulta à APLPD, houve a criação de três projetos de Lei que foram cruciais para a criação da LGPD, sendo eles 4.060/2012; 330/2013 e 5.276/2016.

Tal cenário foi palco para que ocorresse a construção do Projeto de Lei nº 53/2018, que viria a ser aprovado pelo Congresso Nacional e sancionado pela Presidência da República em 14 de agosto de 2018.

Nasce assim, a Lei Geral de Proteção de Dados, Lei nº 13.709 de agosto de 2018, primeira lei no Brasil com o propósito de regular e harmonizar o interesse referente aos dados pessoais tanto pela parte das empresas, quanto pelos indivíduos, a qual entrou efetivamente em vigor em 2020.

Faz-se necessário mencionar que a LGPD possui uma autoridade supervisora, a Autoridade Nacional de Proteção de Dados (ANPD), que possui como função: a) fiscalizar o cumprimento da legislação, seja pelas

empresas, seja pelo Poder Público; b) assegurar os direitos aostitulares dos dados pessoais; c) editar normas e diretrizes que complementem e elucidem as disposições da LGPD; d) aplicar sanções administrativas.

Com o principal intuito de velar pelos direitos fundamentais de liberdade e privacidade, A LGPD, versa sobre tratamento de dados feito por pessoa jurídica ou física, de direito público ou privado, e abrange um grande conjunto de operações localizadas nos âmbitos manuais e principalmente digitais. São abrangidos pela Lei, os dados de brasileiros ou estrangeiros, que estejam no Brasil no momento da coleta.

A criação da LGPD marcou um importante progresso na evolução das leis para regular questões relacionadas à privacidade. Isso permitiu que as leis se adaptassem às demandas surgidas devido à interação social no ambiente digital e à intensa conexão que caracteriza a atual realidade de muitas sociedades.

A lei brasileira conta com 65 artigos, os quais estão divididos em 10 capítulos. Cada capítulo aborda aspectos específicos relacionados à proteção de dados pessoais, desde as definições iniciais até as sanções administrativas e disposições transitórias. Os 65 artigos detalham os direitos dos titulares, as obrigações dos controladores e operadores de dados, as responsabilidades da ANPD, entre outros temas relevantes para a proteção de dados no Brasil.

Estabelecidos nos artigos 6º[8] da referida legislação, são estabelecidos como princípios regimentais da proteção de dados pessoais, os princípios da Finalidade, Adequação, Necessidade, Livre Acesso,

[8]Artigo 6º, LGPD - As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

Qualidade dos dados, Transparência, Segurança, Prevenção, não discriminação e, por fim, responsabilização e prestação de contas.

Evidente que ambas as legislações possuem princípios norteadores muito similares. Dessa forma, no âmbito dos princípios da LGPD, inicialmente é importante fazer referência ao princípio da boa-fé, uma vez que esse deve ser pressuposto de qualquer relação jurídica, o que não seria diferente da relação jurídica de quem coleta os dados e de quem fornece os dados a serem tratados.

Em síntese, as leis de proteção de dados baseiam-se em princípios bem-determinados para conferirem direitos aos indivíduos sobre seus próprios dados, sendo estabelecidas obrigações para os entes que efetuarem o processamento desses dados, de tal modo que meios idôneos ao cumprimento da lei e a compensação de danos causados devem ser acionados sempre que estas obrigações e deveres forem descumpridos. (Rodotá, 2018, p. 18).

No que se refere à efetividade da Lei Geral de Proteção de Dados, tal tema ainda se encontra prematuro para discussão, em virtude de sua recente entrada em vigor.

Em curto prazo, pode-se observar um aumento significativo na conscientização sobre a proteção de dados pessoais por parte das organizações e dos próprios cidadãos. As empresas, principalmente as que envolvem o âmbito digital, foram impostas à adequações e implementações de medidas de segurança, que seguissem as regulamentações impostas pela lei.

A efetividade da LGPD dependerá da aplicação consistente da lei e da punição efetiva em casos de violação. A sociedade como um todo precisa estar engajada e consciente dos seus direitos e deveres em relação à proteção de dados.

O órgão responsável pela fiscalização e aplicação da LGPD, é a Autoridade Nacional de Proteção de Dados (ANPD), que começou a operar em 2021. A ANPD tem a função de regulamentar a lei, orientar as organizações e aplicar sanções em caso de descumprimento. A atuação efetiva da ANPD é fundamental para garantir a eficácia da LGPD e ainda se encontra em debate.

Portanto, é essencial destacar que, embora a LGPD represente um marco importante na proteção de dados pessoais no Brasil, sua efetividade será percebida de forma gradual, à medida que as disposições trazidas no corpo da lei brasileira forem devidamente implementadas e fiscalizadas.

3 DADOS PESSOAIS E SANÇÕES

3.1 CONCEITO DE DADOS PESSOAIS E SUA IMPORTÂNCIA NA SOCIEDADE DIGITAL

Como retratado no capítulo anterior, a sociedade atual atravessa o fenômeno da hiperconectividade, no qual os indivíduos estão cada vez mais conectados e integrados ao mundo virtual e tecnológico.

Destarte, é possível dizer que a todo instante, inúmeros dados pessoais são coletados e fornecidos às empresas. A partir da coleta de dados, seja de uma simples busca em uma plataforma online, é possível elencar incontáveis informações passíveis de serem adquiridas, e por tal razão, vêm se tornando cada vez mais valiosos.

De forma acertiva e pontual, a revista americana *The Economist* e a revista *Forbes*, através de matérias publicadas nos anos de 2017 e 2019, apontaram a importância dos dados pessoais na economia global atual.

Nesse sentido, Gustavo Tepedino cita Nick Srineck:

> Vistos já como o novo petróleo, os dados são hoje insumos essenciais para praticamente todas as atividades econômicas e tornaram-se, eles próprios, objeto de crescente e pujante mercado. Não é sem razão que se cunhou a expressão *data-driveneconomy*, ou seja, economia movida a dados, para designar o fato de que, como aponta Nick Srnicek, o capitalismo do século XXI passou a centra-se na extração e no uso de dados pessoais. (Srineck, 2018, p. 39) (tradução livre)

Estabelecidos nos artigos 4º(1) do GDPR e no artigo 5º da LGPD como todas as informações relacionadas à pessoa natural identificada ou identificável, ou seja, a titular dos dados, os dados pessoais são divididos em duas categorias: dados pessoais sensíveis e dados pessoais anonimizados.

Sergio Pohlmann classifica dados pessoais sensíveis como:

> Dado pessoal que possa relacionar uma pessoa natural com algum tipo de associação, movimento, sindicato, partido político, ou questões de ordem étnica,

> religiosas, políticas, filosóficas, vida sexual, etc. Estão incluídos nesta categoria, todos os dados médicos, biométricos e genéticos. (Pohlmann, 2019. p. 36)

A caracterização de dados sensíveis exige uma análise profunda e cautelosa, devendo ser levado em consideração os desdobramentos perante a privacidade, identidade pessoal e discriminação, uma vez abrangidas pelo princípio constitucional da Dignidade da Pessoa Humana. (Tepedino, Frazão, Oliva, 2019, p. 34).

3.1.1 DADOS PESSOAIS SENSÍVEIS E VAZAMENTO SOB A ÓTICA DO GDPR

São classificados como dados pessoais sensíveis, os dados passíveis de revelar a origem racial ou étnica, opiniões políticas e filiações sindicais, pensamento e ideologias religiosas e até mesmo filosóficas; dados genéticos e biométricos tratados com a finalidade de identificação de um indivíduo; dados referentes à saúde; dados que revelem vida ou orientação sexual. Tais dados possuem um tratamento específico e são coletados somente em casos estipulados pela legislação.

A partir de uma sucinta análise do Regulamento europeu tratado no presente artigo, é possível perceber que houve uma descrição e definição maior e especificação quanto aos dados pessoais, diferente da legislação brasileira, que os tratou de forma mais genérica.

De maneira geral e breve, esses dados sensíveis exigem uma maior observância por parte dos controladores de dados, no que tange ao consentimento explícito, à existência de uma base legal e finalidade que justifiquem seu processamento, gerando dessa forma, uma maior proteção e segurança jurídica, o que justifica sua coleta somente em casos específicos.

Adentrando ao campo das sanções aos casos de vazamento de dados, essas estão previstas no regulamento europeu no capítulo VIII, que abrange os artigos 77 a 84.

A reparação dos danos causados pelo vazamento de dados é direito de todos os indivíduos que tiveram seus dados expostos, como estabelecido pelo artigo 82 (1) do Regulamento

Inicialmente, é garantido ao titular dos dados o direito de apresentar uma Reclamação a uma autoridade de fiscalização e controle

competente, em face da empresa controladora dos dados. Tal reclamação é feita no Estado-membro onde reside o indivíduo, ou no Estado-membro do local onde ocorreu a infração.

Adiante, é garantida também ao titular dos dados sensíveis a propositura de recurso judicial em face do responsável direto pelo tratamento de dados ou seu subcontratado.

No artigo 839, são apresentadas as condições gerais para a aplicação de sanções administrativas e multas. É estabelecido que a aplicação de uma multa deve observar a eficácia e a proporcionalidade da sanção conforme o caso de vazamento de dados tratado.

No que tange ao valor que será estabelecido às multas, deverão ser considerados os aspectos da gravidade do caso a ser aplicada a penalidade, mais uma vez, deixando clara a necessidade da proporcionalidade nas sanções.

As multas apresentam-se dentro de três parâmetros apresentados no artigo supra mencionado do regulamento: o primeiro que estabelece o limite de 10. 000.000,00 (dez milhões) de Euros ou, no caso de uma empresa, até de 2% (dois por cento) do volume de negócios anual total no nível mundial correspondente ao exercício financeiro anterior; o segundo parâmetro estabelecido pelo ponto que elava o limite até 20.000.000 (vinte milhões) de euros ou, no caso de uma empresa, até de 4% (quatro por cento) do volume de negócios anual total no nível mundial como registrado no exercício financeiro anterior; e por fim o terceiro parâmetro, que discorre sobre o não cumprimento de uma ordem da autoridade de supervisão, que pode acarretar multa ao sujeito a de até 20.000.000,00 (vinte milhões de euros) ou, no caso de uma empresa, até 4% (quatro por cento) do total do volume de negócios anual mundial do exercício anterior, sendo considerado aqui, qual das opções gerar mais valor.

Por fim, no que se refere às sanções, o Regulamento Europeu definiu que há possibilidade de aplicação de outras sanções aos controladores e processadores nos casos envolvendo vazamento de dados, entretanto tais sanções alternativas devem ser estabelecidas por cada Estado-membro, de forma individual e observando novamente a eficácia e proporcionalidade.

[9]Art. 83, REGULAMENTO (UE), 2016/679.

3.1.2 DADOS PESSOAIS SENSÍVEIS E VAZAMENTO SOB A ÓTICA DA LGPD

Os dados sensíveis são definidos no artigo 5º, inciso II da Lei Geral de Proteção de Dados, como "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." (Brasil, Lei nº 13.709, 2018).

Observa-se que a legislação brasileira apresenta um rol taxativo ao definir tais dados, e dessa forma delimita quais são eles. Tal taxatividade é motivo de crítica por parte dos doutrinadores, uma vez que a combinação de dados não considerados sensíveis, pode, muitas vezes, acarretar na transformação de tais dados, em dados sensíveis. (Frazão, 2018).

No que tange ao tratamento de tais dados sensíveis, inicialmente, cumpre ressaltar que, assim como o Regulamento europeu, a lei brasileira estabeleceu critérios específicos para que o esse tratamento seja legal.

O artigo 11º da Lei nº 13.709 versa especificamente sobre os requisitos necessários para o tratamento dos dados sensíveis.

Logo em seu primeiro inciso, é apresentado que o dado sensível somente poderá ser tratado caso haja o consentimento do titular do dado desde que esse seja específico e que antes tenham sido apresentadas todas as razões que levaram à coleta desses dados, contudo existem casos que permitem sem a necessidade do consentimento, como por exemplo, o cumprimento de obrigação legal ou regulatória pelo controlador.

Quando mencionadas as responsabilidades, sanções e multas aos casos de vazamento de dados, novamente ambas as legislações apresentam muitas semelhanças.

Um vazamento de dados é quando informações pessoais ou confidenciais são divulgadas ou expostas a pessoas ou entidades não autorizadas. Inúmeras são as causas que levam ao vazamento, podendo ser essas desde falha de segurança ou de um incidente em que dados privados são tornados públicos, podendo ser acessados e utilizados por terceiros sem a devida autorização.

A Lei Geral de Proteção de Dados brasileira estabelece em sua Seção III, a Responsabilidade e o Ressarcimento dos danos causados aos titulares dos dados, nos casos de vazamento.

A referida seção inicia apontando que tanto o controlador, quanto o operador possuem responsabilidade solidária sobre a indenização do

dano ao titular dos dados vazados. Tal responsabilidade atinge qualquer controlador que estivesse ligado aos dados vazados.[10].

Tendo em vista a necessidade de sanções aos casos de vazamento de dados, inicialmente, ao analisar tais medidas, é notório que existem muitas convergências com a GDPR, quando analisado o ponto em questão, contudo, o regulamento europeu apresentou-se mais específicos quanto aos valores das sanções estabelecidos em cada caso, enquanto a lei brasileira estabeleceu limites de forma mais genéricas.

Sendo assim, a LGPD definiu em seus artigos 52 a 54 tais sanções administrativas que incluem desde advertências, multas, bloqueio e eliminação dos dados pessoais, suspensão de banco de dados e suspensão até proibição do exercício de atividades que envolvam o tratamento de dados pessoais por parte da empresa infratora, essas estabelecidas proporcionalmente à gravidade da infração.

A LGPG estabelece que as mediadas punitivas serão aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD)[11]. Inicialmente a agência controladora, ao tomar ciência do vazamento de dados, pode aplicar uma multa à empresa infratora estabelecendo um prazo para a regularização da infração e assim para a adoção de medidas coercitivas, caso o órgão controlador dos dados não cumpra com o estabelecido pela ANPD.[12]

Em seguida, nos incisos do mesmo artigo 52, são tratadas as multas as serem aplicadas, essas que atingem o limite de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, podendo essas serem aplicadas diariamente, observado limite mencionado, caso não a parte infratora ainda não cumpra o determinado.[13]

Ainda caso o controlador dos dados ainda não solucione a questão do vazamento, serão aplicadas as sanções de publicização da infração após devidamente apurada e confirmada a sua ocorrência, bloqueio dos dados pessoais a que se refere a infração até a sua

[10]Artigo 42, LGPD nº 13.709.

[11] Observação minha: A ANPD é o órgão que fiscaliza e regula a aplicação da LGPD no Brasil. Seu objetivo principal é proteger os dados pessoais dos cidadãos, garantindo que empresas e organizações cumpram as regras da LGPD ao coletar e processar esses dados. Criada pela Lei nº 13.853/2019 e vinculada ao Ministério da Justiça e Segurança Pública, a ANPD tem como missão assegurar a privacidade e a segurança das informações dos brasileiros.

[12]Artigo 52, inciso I, LGPD nº 13.709:

[13] Artigo 52, inciso II e III, LGPD nº 13.709.

regularização, eliminação dos dados pessoais a que se refere a infração, suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, e por fim, como grau máximo de medida coercitiva, a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.[14]

A LGPD assegura que as sanções só serão aplicadas após um processo administrativo que permita a ampla defesa do infrator. Essas sanções podem ser aplicadas de maneira gradual, isolada ou cumulativa, dependendo das circunstâncias específicas de cada caso. Isso significa que antes de impor qualquer penalidade, é garantido ao infrator o direito de se defender e apresentar seus argumentos, considerando a natureza e a gravidade da infração cometida.

3.2 BREVE RELATO DE CASOS ENVOLVENDO O GDPR E A LGPD

3.2.1 O CASO DA GOOGLE

Em 2019, a maior empresa de tecnologia global Google, recebeu uma multa no valor de aproximadamente 50 milhões de euros, aplicada pela Agência de Proteção de Dados Francesa (CNIL), por claro descumprimento aos preceitos estabelecidos no GDPR.

A empresa Google, foi acusada pela CNIL, com base em denúncias recebidas por duas ONGs francesas, as quais alegavam que a companhia americana não apresentava de forma clara, objetiva e simples o consentimento aos seus usuários acerca da coleta de dados pessoais realizadas.

Após a investigação, a agência de proteção de dados francesa concluiu que de fato a empresa norte americana descumpria o Princípio de Transparência, estabelecido com fundamental e basilar pela GDPR, uma

[14] Artigo 52, inciso IV, V, VI, X, XI e XII, LGPD nº 13.709

vez que não apresentava de forma clara em seu consentimento a motivação da coleta dos dados e o período que tais dados seriam armazenados.

A referida sanção foi a primeira multa aplicada a uma empresa de tecnologia americana, tendo em vista que a GDPR protege os dados de cidadãos europeus independentes de onde foram coletado e tratados.

A CNIL ao final do recurso de sanção, afirmou que a medida adotava teve como base a gravidade das infrações observadas.

Além disso, válido ressaltar que a medida adotada cumpriu com o critério da razoabilidade e proporcionalidade sanção, estabelecido pela GDPR, uma vez que a multa poderia ter sido aplicada no valor de 4% do faturamento da empresa em seu último exercício, o que teria tingido um valor extremamente maior.

3.2.2 O CASO DA TELEKALL INFOSERVICE

O caso envolvendo a microempresa brasileira de telefonia *TelekallInfoservice*, ganhou bastante atenção no campo do direito digital, tendo em vista que foi o primeiro caso em que a ANPD aplicou uma multa por infração da LGPD, uma vez que a empresa foi acusada de violar os artigos 7º e 41 da legislação brasileira.

A multa foi aplicada em julho de 2023, tendo como motivação principal a falta de registro das operações de tratamento de dados, ausência de encarregado de dados nomeado, não envio do relatório de impacto e não atendimento às solicitações da ANPD e ausência de base legal para tratamento de dados.

Nesse sentido, apresenta a advogada Ursula Ribeiro:

> A interpretação da ANPD é no sentido de que a falta de indicação de encarregado por agentes de pequeno porte é uma infração leve ou média, tendo em vista que somente esses tipos de infração estão sujeitas à advertência e no caso concreto não foi imposta medida corretiva. Porém, o entendimento não deve ser o mesmo em relação a agentes que *não* sejam de pequeno porte, visto que *a LGPD* é taxativa quanto à obrigatoriedade de indicação do encarregado (Almeida, 2018).

A ANPD, antes da aplicação da multa, advertiu a empresa para que as correções necessárias fossem feitas sem a necessidade de medidas coercitivas mais gravosas, como a multa. Contudo a empresa brasileira não cumpriu com o estabelecido pela agência de proteção de dados brasileira, o que acarretou na multa no valor de R$14 mil.

Conforme exposto em tópico anterior do presente artigo, relativo à "Efetividade da Lei Geral de Proteção de Dados", a aplicação da primeira multa pela ANPD, marca um grande avanço no que se refere aos desdobramentos da lei e na efetividade em si, uma vez que esses serão observados a partir da aplicação de sanções que surgirão.

4 CONSIDERAÇÕES FINAIS

O presente trabalho científico teve como objetivo principal uma análise acerca das legislações que versam sobre a proteção de dados, sendo elas o *General ProtectionRegulation* (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil, dando enfoque aos contextos e marcos que levaram à criação de ambas, aos seus elementos principais como princípios, fundamentos e objetivos, bem como uma exploração acerca dos dados pessoais sensíveis e as sanções aplicadas por ambas aos casos de vazamento de dados.

Além disso, como forma de apresentar uma ideia mais clara e concreta do que foi explorado ao longo de todo o trabalho, foram apresentados casos reais de descumprimento de preceitos estabelecidos tanto no regulamento europeu, quanto na legislação brasileira, assim como como as medidas punitivas adotadas, pelos órgãos responsáveis pelo ocorrido.

Restou claro que a sociedade passou por uma grande mudança e reforma na qual a internet adquiriu um papel fundamental e essencial em todas as relações estabelecidas pelos indivíduos.

Tal Evolução tecnológica, como apontado anteriormente, foi palco para grandes mudanças no que se refere à visão da privacidade ante uma economia na qual os dados se tornaram grande movimentadores econômicos.

A União Europeia, ao adotar o regulamento 679, como único para tratar sobre os dados pessoais de todos os cidadãos dos países-membros, teve um papel de grandiosa importância ao estabelecer novas condições ao

mercado internacional, mas também ao servir de fonte de inspiração normativa aos outros países, especialmente ao Brasil.

A Lei nº 13.709, a LGPD, criada em 2018, como ressaltado por especialistas apontados ao longo do trabalho, teve como espelho para sua criação, o regulamento europeu. A parir da análise de ambas as legislações, é possível identificar inúmeros pontos de semelhança entre ambas, nos mais diversos aspectos observados.

Tanto o GDPR quando a LGPD, possuem princípios e fundamentos basilares extremamente semelhantes, principalmente no que tange à finalidade, responsabilidade, necessidade do tratamento e por fim, o consentimento. Ambas o tratam de forma importante e dão ênfase ao longo de todo o texto legal.

Adentrando às definições de dados sensíveis, a legislação brasileira possui uma classificação mais genérica a respeito de tais dados, especificando em seu artigo quais são eles. Já o regulamento europeu, estabelece categorias de dados sensíveis, o que deixa o rol mais restrito e detalhado.

No que tange às sanções, novamente são observadas semelhanças, contudo existem algumas diferenças. O regulamento europeu, possui um detalhamento mais específico e atento às multas e quando essas serão aplicadas, além de que a aplicação de tais multas é feita por uma Agência controladora do Estado- membro em que ocorreu a violação, e não por uma agência que fiscalize todos os países. Por sua vez, a lei brasileira, estabelece parâmetros e limites para a aplicação das multas e sanções, contudo, de uma forma geral, além de nomear a ANPD como agente responsável pela fiscalização e a aplicação das multas pecuniárias.

A atuação da ANPD, a partir de seu funcionamento pleno, será primordial para a efetividade da LGPD, assim como as entidades fiscalizadoras dos Estados- membros foram para o GDPR.

Dessa forma, conclui-se com o presente trabalho que através de estudo aprofundado à ambas as leis tratadas, é clara a influência do GDPR sobre a LGPD, existindo pontos de divergências, contudo muitos mais pontos de semelhança.

Além disso, é notória a importância de ambas as legislações perante o contexto atual envolvendo o fenômeno da Hiperconectividade e importância dos dados pessoais.

5 REFERÊNCIAS

ALECRIM, Emerson. Google recebe multa de 50 milhões de euros na França por violar GDPR.**Revista Tecnoblog.** 2019. Disponível em: https://tecnoblog.net/noticias/2019/01/21/google-multa-gdpr-franca/. Acesso em 29 jul.2023.

ALMEIDA, Ursula Ribeiro de. **A primeira multa aplicada pela ANPD**: a linha interpretativa da Autoridade e a perspectiva para os casos futuros. JOTA, 2023. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-primeira-multa-aplicada-pela-anpd-29072023. Acesso em 29 jul. 2023.

BHAGESHPUR, Kiran. Data Is The New Oil -- AndThat's A Good Thing. **Forbes**, USA. 15 Nov. 2019. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=46bb0a1b7304. Acesso em: 10 jul. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed, Rio de Janeiro: Forense, 2020.

BRANDEIS, L. D.; WARREN S. D. The right to privacy. **Harvard Law Review**, Boston, V. 4, nº 5, dec, 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acessoem: 30 jun. 2023.

BRASIL. [Lei Geral de Proteção de Dados Pessoais (LGPD) (2018)]. **Lei nº 13.709/18.** Brasília, DF: Presidência da República, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13. fev. 2023.

CANTO, A. P. DE LIMA; CAIO, G. R SATERO; VASCONCELOS, M. G DE CABRAL; BARBOSA, M. B. SABOYA; MELO, R. CORREA; HOLANDA YANNE. **O que estão fazendo com os meus dados**?. A importância da Lei Geral de proteção de dados pessoais. Editora SerifaFina. Recife, 2019.

COELHO, Pablo M. B.; GIOLO JÚNIOR, Cildo; BENFATTI, Fabio F. Neves (orgs.). **O direito digital e proteção de dados.** São Paulo: Editora Andradina, 2022.

CONSELHO EUROPEU. ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Estrasburgo***, 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 09 jul. de 2023.

DIÁZ, Efrén. The new European Union General Regulation on Data Protection and the legal consequences. In: **Church, Communication and Culture**, 2016.
DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo. Ed. Thomson ReautersBrasil, 2021.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais.São Paulo: Editora Renovar, 2006. Apud: COELHO, Pablo M. B.; GIOLO JÚNIOR, Cildo; BENFATTI, Fabio F. Neves (orgs.). **O direito digital e proteção de dados.** São Paulo: Editora Andradina, 2022.

FRAZÃO, Ana**. Nova LGPD: o tratamento dos dados pessoais sensíveis**. *Jota*. 19.09.2018. Disponível em: www.jota.info/opiniaoe-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 19 jul. 2023.

GUIDI, Guilherme. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acessoem: 10 fev. 2023.

MACHADO, J. D. M. S. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista da AJURIS - QUALIS A2**, *[S. l.]*, v. 41, n. 134, 2014. Disponível em: https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/206. Acesso em: 6 jul. 2023.

MAGRINI, Eduardo. Entre dados e robôs: Ética e privacidade na era da Hiperconectividade. Porto Alegre – RS: Editora Arquipélago. 2019.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** Paris, 1948. Disponível em: http://www.un.org/en/universal-declaration-human-rights/. Acesso em: 10 fev. 2023.

POHLMANN, Sergio Antonio. **LGPD NINJA:** Entendendo e Implementando a Lei Geral de Proteção de Dados nas Empresas. Editora Fross. 2019.

PORTER, Jon. **Google fined €50 million for GDPR violation in France.** The Verge, 2019. Disponível em: https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil. Acesso em: 29 jul. 2023.

RODOTÀ, Stefano. ***A vida na sociedade da vigilância***. A privacidade hoje. Trad. Danilo Doneda e Laura Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SAMPAIO, J. A. L. **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoas, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SRNICEK, Nick. ***Platform capitalism***. Cambridge: Polity Press, 2018.

TEIXEIRA, Tarcísio. **Comércio eletrônico**: conforme o Marco Civil da Internet e a regulamentação do e-commerce no Brasil. São Paulo: Saraiva, 2015.
TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019.

THE ECONOMIST. ***The world'smostvaluableresourceis no longeroil, but data***. The Economist, London, v. 425, n. 9075, p. 20-22, 6 May 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 10 jul. 2023.

UNIÃO EUROPEIA. ***General Data ProtectionRegulation.*** 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 10 ago. 2023.

VIDAL, Gabriel Rigoldi. **Conceituação do direito à privacidade em face das novas tecnologias**. Estudo entregue à Universidade Estadual Paulista – Faculdade de Ciências Humanas e Sociais (Campus Franca). Franca, 2017. Disponível em: https://www.direitorp.usp.br/wp-content/uploads/2014/11/GabrielVidalConceituacao.pdf. Acesso em 30 jun. 2023