FACULDADES INTEGRADAS DE BAURU- FIB

DIREITO

Joyce da Silva Lopes

A LEI GERAL DE PROTEÇÃO DE DADOS E O DIREITO À PRIVACIDADE

Bauru
2021

Joyce da Silva Lopes

A LEI GERAL DE PRETEÇÃO DE DADOS E O DIREITO À PRIVACIDADE

Monografia apresentada às Faculdades Integradas de Bauru para obtenção do título de bacharel em Direito em 2021, sob a orientação do Professor Me. Tales Manoel Lima Vialôgo.

Bauru
2021

Lopes, Joyce da Silva

A lei geral de proteção de dados e o direito à privacidade. Joyce da Silva Lopes. Bauru, FIB, 2021.

67f. FOLHAS

Monografia, Bacharel em Direito. Faculdades Integradas de Bauru - Bauru

Orientador: Me. Tales Manoel Lima Vialôgo.

1. LGPD. 2. Dados Pessoais. 3. Direito Digital. I. A lei Geral de Proteção de Dados e o Direito à Privacidade II. Faculdades Integradas de Bauru.

CDD 340

Joyce da Silva Lopes

A LEI GERAL DE PROTEÇÃO DE DADOS E O DIREITO À PRIVACIDADE

Monografia apresentada às Faculdades Integradas de Bauru para obtenção do título de Bacharel em Direito, Bauru, 07 de janeiro de 2021.

Banca Examinadora:

Presidente/ Orientador: Me. Tales Manoel Lima Vialôgo

Professor 1: Me. Camilo Stangherlim Ferraresi

Professor 2: Me. Cesar Augusto Micheli

Bauru
2021

Dedico este trabalho a Deus, pois sem ele não estaria aqui. Dedico também à toda a minha família, ao meu namorado e amigos por todo o apoio, amor e companheirismo dados a mim ao longo destes cinco anos. Ao meu orientador por todo o suporte para a conclusão deste trabalho.

AGRADECIMENTOS

Agradeço primeiramente à Deus, por ser essencial em minha vida, a Jesus Cristo e a Virgem Maria, por serem tão misericordiosos e benevolentes para comigo.

Agradeço a toda minha família, em especial minha mãe, Eloisa Elena da Silva, pois é graças ao seu esforço que hoje posso concluir o meu curso, por ser o meu exemplo de mulher e a melhor mãe que alguém poderia ter, por todo apoio e amor incondicional por mim e ao meu irmão.

Ao meu namorado, Lucas Sanches Lorca, por todo o amor, respeito e companheirismo, pela cumplicidade e pelo apoio em todos os momentos delicados da minha vida, por todo o suporte para que eu pudesse desenvolver este projeto e apoio em tudo que faço.

Aos meus amigos e colegas de curso por compartilharem comigo tantos momentos de descobertas, felicidade e aprendizado, por todo o companheirismo e conselhos ao longo deste percurso. Aos meus colegas do Ministério Público do estado de São Paulo, por todo o ensinamento e amizade durante os dois anos de estágio.

Aos professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso. Ao meu orientador, Professor Tales Manoel Lima Vialôgo, por ter aceitado acompanhar-me neste projeto, pelos ensinamentos, conselhos e orientações essenciais para a conclusão desse trabalho.

“Os que não querem ser vencidos pela verdade, serão vencidos pelo erro” - Santo Agostinho de Hinopa.

LOPES, Joyce da Silva. **A Lei Geral de Proteção de Dados e o Direito a Privacidade.** 2021 67f. Monografia apresentada às Faculdades Integradas de Bauru, para obtenção do título de Bacharel em Direito. Bauru, 2021.

RESUMO

O presente trabalho tem como objetivo analisar a Lei Geral de Proteção de Dados (LGPD) e apresentar seus principais temas sobre os dados pessoais, com a intenção de mostrar a importância do tema tanto para estudantes e professores de direito quanto para aqueles que por ora tiverem interesse sobre o tema. O trabalho demonstra ainda as inovações da lei e seus principais objetivos como a segurança ao universo de dados pessoais, a preservação dos direitos fundamentais do titular dos dados e a relevância destes dados no mundo contemporâneo. Neste intuito, a partir de pesquisas bibliográficas, documentais e digitais sobre o tema, o trabalho abrange desde a evolução do direito digital no Brasil, passando para todas as etapas do tratamento de dados, do inicio até o termino, abrangendo conceitos e tipos de tratamento. Em seguida trata ainda sobre a abrangência da lei brasileira, inclusive sobre os casos de tratamento internacional de dados, tendo por fim, tratado sobre a responsabilidades que a lei traz e os ressarcimentos nos casos de irregularidades com a lei. Concluindo-se por fim que no atual contexto de evolução digital, onde vivemos em um mundo de explosões de tecnologias todos os dias, as informações pessoais tornam-se cada vez mais valiosas como um produto. Medidas como a promulgação da Lei nº 13.709/2018 (LGPD), fazem com que se exija um desenvolvimento social saudável dentro e fora do mundo virtual, sem que se ultrapasse os limites da privacidade.

Palavras-chave: LGPD. Dados Pessoais. Direito Digital.

LOPES, Joyce da Silva. **A Lei Geral de Proteção de Dados e o Direito a Privacidade.** 2021 67f. Monografia apresentada às Faculdades Integradas de Bauru, para obtenção do título de Bacharel em Direito. Bauru, 2021.

ABSTRACT

This job aims to analyze the General Data Protection Law (LGPD) and present its main topics on personal data, with the intention of showing the importance of the topic both for students and professors of law and for those who have so far interest on the topic. The work also demonstrates the innovations of the law and its main objectives such as the security of the universe of personal data, the preservation of the fundamental rights of the data owner and the relevance of this data in the contemporary world. To this end, based on bibliographic, documentary and digital research on the subject, the job ranges from the evolution of digital law in Brazil, passing through all stages of data processing, from the beginning to the end, covering concepts and types of treatment Then, it also deals with the scope of Brazilian law, including cases of international data processing, and finally, dealt with the responsibilities that the law brings and the reimbursement in cases of irregularities with the law. Finally concluding that in the current context of digital evolution, where we live in a world of explosions of technologies every day, personal information becomes increasingly valuable as a product. Measures such as the enactment of Law nº 13.709/2018 (LGPD), demand a healthy social development inside and outside the virtual world, without exceeding the limits of privacy.

Keywords: LGPD. Personal Data. Digital Law.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho visa compreender as implicações jurídicas advindas da legislação infraconstitucional da Lei Geral de Proteção de Dados e suas disposições legais, das quais tem por finalidade a proteção do indivíduo e as relações que envolvam seus dados pessoais.

Sob a influência internacional europeia, que criou o Regulamento Geral de Dados Pessoais (GDPR), foi regulamentado no Brasil a referida lei (LGPD), trata-se, portanto, de um marco regulatório da proteção de dados pessoais nas relações entre usuários e setor público/privado, em consonância aos princípios fundamentais de liberdade, livre desenvolvimento da personalidade e da privacidade.

Em prol de tudo isto, analisa-se a vulnerabilidade da privacidade dos indivíduos ante a globalização e os avanços dos meios de comunicação, como por exemplo a internet e por consequência, estuda-se a legislação especifica sobre a proteção de dados pessoais no ordenamento jurídico brasileiro.

Hoje, os dados pessoais se tornaram um dos ativos mais importantes do mundo e podem, sem dúvida, ser considerados uma fonte de riqueza no século XXI. Por exemplo, o progresso tecnológico e informações detalhadas sobre milhões de pessoas podem prever tendências de compras e pensamentos políticos. Portanto, é muito importante entender como as pessoas pensam, expressam e agem. É aqui que a análise desses dados orienta como fornecer produtos ou serviços no mercado. Mais importante ainda, as atividades de marketing estratégico podem atingir mercados consumidores específicos mais rapidamente. Esse é o propósito da LGPD, trazer maior transparência, garantir o respeito aos direitos básicos dos cidadãos, para que as pessoas possam controlar as informações que são divulgadas sobre elas (MOREIRA, 2020).

Faz-se necessário, portanto, analisar a contextualização do tema na realidade que a população se encontra atualmente, pois, é indubitável o fato de que dia-pós-dia a inclusão de dados possibilita inerentemente a democratização de informações, seja do inconsciente coletivo para o uno ou o contrário, logo, que atitude os legisladores devem adotar diante de um indesejado vazamento de dados e quais direitos podem ou não estar no acervo do apetrecho da justiça brasileira.

Assim, através de pesquisas bibliográficas, documentais e digitais de natureza exploratória e descritiva, esta pesquisa busca responder à problemática proposta a partir de quatro capítulos. No primeiro verifica-se o que de fato é o direito à privacidade e o seu surgimento, assim como a evolução do direito digital no Brasil, demonstrando que além da constituição federal assegurar o direito à privacidade, a primeira lei infra constitucional sobre o assunto surgiu em 2012, a lei Carolina Dieckmann, dispondo sobre a invasão de dispositivos informáticos, sendo, consequentemente a primeira a proteger a privacidade cibernética e os dados pessoais.

Posteriormente em 2011 a Lei do Cadastro Positivo e em 2014 o Marco Civil da Internet, sendo está uma lei que visa a consolidação de direitos, deveres e princípios para a utilização e o desenvolvimento da internet no Brasil.

O segundo capitulo deste trabalho terá por escopo demonstrar o conceito e o tratamento de dados pessoais, abrangendo também os dados sensíveis, de crianças e adolescentes, o que fazer ao término do tratamento e quais órgãos regularão a LGPD.

O terceiro capitulo verifica-se a abrangência da lei, os casos de transferência internacional de dados pessoais e o tratamento destes dados pelo poder público.

Por fim, o quarto capitulo expõe sobre a responsabilidade e o ressarcimento de danos, a responsabilidade civil do controlador e do operador de dados, como também as hipóteses de exclusão destas. Ainda dispõe sobre casos de irregularidades no tratamento e o ressarcimento de danos aplicados na primeira ação civil pública e na primeira sentença brasileira sobre o tema.

2 DIREITO À PRIVACIDADE E A EVOLUÇÃO DO DIREITO DIGITAL

Atualmente a polarização da internet está impactando o mundo como conhecemos, gerando transformações nas interações sociais. Tal polarização possui inquestionáveis avanços e benéficos para toda a sociedade, entretanto também possui maléficos se usada indevidamente, gerando riscos para direitos fundamentais e para a proteção de dados pessoais (RUARO; SOUZA, 2017, p. 197 apud GLITZ, 2019).

Ocorre que, a cada ano que se passa, devidos a esses avanços tecnológicos estamos mais conectados e transmitindo cada vez mais dados na rede e por conta disso torna-se inquestionável o direito de ter acesso à internet, sendo que quem opta por viver sem internet, deve estar ciente das possibilidades e direitos que não terá acesso (MAÑAS, 2017, p. 61e 69 apud GLITZ, 2019).

Muitas pessoas acreditam estar protegidas quando estão na internet devido estarem atrás de uma tela de computador, contudo tal sensação de invisibilidade é falha pois enquanto navegamos na internet ocorre a coleta de dados pessoais e devido a isso é que a privacidade cibernética deve ser seriamente tutelada. (MATOS, 2005).

Em decorrência desta coleta, os dados e informações pessoais tornaram-se matéria prima básica para um novo mercado, no qual toda utilização feita na rede deixa um rastro oculto de informações, permitindo que até mesmo terceiros tenham acesso a estes dados e consequentemente violação do direito à privacidade (RUARO; SOUZA, 2017, p. 198 apud GLITZ, 2019).

É preocupante o destino desses dados coletados por sites enquanto navegamos na internet, pois os *cookies* (arquivos de texto que armazenam as preferências de usuários sobre determinados sites (GUGIK, 2008)) são capazes de monitorar os sites que visitamos, quanto tempo permanecemos nele e qual a frequência de visitação. Coisa bem pior ocorre com outros meios eletrônicos como os satélites que tem a capacidade de focalizar a fachada de casas, podendo até espionar o fluxo de entrada e saída desta (MATOS, 2005).

Esta realidade, muitas vezes afronta a dignidade da pessoa humana que é o ideal máximo na Declaração Universal da ONU consagrada em seu artigo 1º (CANOTILHO, 2003, p. 225 apud GLITZ, 2019): “Artigo 1°-Todos os seres humanos

nascem livres e iguais em dignidade e em direitos. Dotados de razão e de consciência, devem agir uns para com os outros em espírito de fraternidade". (ONU, 1942)

A constituição brasileira, adota tal princípio em cujo conteúdo se insere o direito fundamental à privacidade, que se vê diante dos mais variados desafios para a sua tutela, ainda mais quando analisado sob a ótica da proteção de dados pessoais (DONEDA, 2006, p. 371 apud GLITZ, 2019).

Cabe ainda destacar a origem do direito à autodeterminação informativa, originada do julgamento da Lei do Censo de População, Profissão, Moradia e Trabalho realizado pelo Tribunal Constitucional alemão em 25 de março de 1982 (GLITZ, 2019).

> Nesse julgamento histórico, o Tribunal reforçou o conceito do livre controle do indivíduo sobre a circulação de suas informações pessoais, decidindo pela inconstitucionalidade parcial da lei em virtude da existência de um direito à "autodeterminação informativa", com base na Lei Fundamental que protege a dignidade humana e o livre desenvolvimento da personalidade (MENDES, 2014, p. 30 apud GLITZ, 2019).

O objetivo da referida lei era a coleta de informações dos cidadãos como suas profissões, moradia e trabalho, tendo como objetivo final fornecer ao estado informações sobre o crescimento populacional, distribuição espacial da população e atividades econômicas realizadas no país e que ocasionaria em multa caso o cidadão se recusasse a prestar informações, gerando violação direta ao livre desenvolvimento da personalidade. Tal sentença criou um marco, reconhecendo o direito à auto determinação informativa, influenciando normas nacionais e europeias em sequência "a reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados" (MENDES, 2014, p. 31 apud GLITZ, 2019).

A proteção da privacidade no atual contexto em que vivemos está diretamente ligado a proteção de dados pessoais, estendendo-se além do isolamento ou tranquilidade, mas com o fim de garantir um posicionamento adequado ao indivíduo perante a sociedade, trazendo como sua maior contribuição a caracterização deste direito como um direito fundamental (DONEDA, 2006, p. 25 apud GLITZ, 2019).

A caracterização da proteção de dados pessoais como um direito fundamental torna-se mais clara ao analisar a Convenção do Conselho da Europa de 1950 e a Carta dos Direitos Fundamentais da União Europeia de 2000. Em seu artigo 8º da

Convenção está disposto que “todos tem o direito de respeito à vida privada e familiar, seu domicilio e sua correspondência”. Já a Carta do Direitos Fundamentais evidência a diferença entre os convencionais direitos do artigo 7º, “direito de respeito da vida privada e familiar”, originários da Convenção, e insere o “direito à proteção de dados pessoais” em seu artigo 8º da Carta, tornando-se um direito fundamental autônomo (RODOTÀ, 2008, p. 16 apud GLITZ, 2019).

> O direito ao respeito da vida privada e familiar reflete, primeira e principalmente, um componente individualista: este poder basicamente consiste em impedir a interferência na vida privada e familiar de uma pessoa. Em outras palavras, é um tipo de proteção estático, negativo. Contrariamente, a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas – *i.e.* é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos. Adicionalmente, a supervisão e outros poderes não são somente conferidos às pessoas interessadas (os sujeitos de dados), mas são também entregues a uma autoridade independente. A proteção não é mais deixada somente aos sujeitos de dados, uma vez que existe um órgão público permanente responsável por isso (RODOTÀ, 2008, p. 17 apud GLITZ, 2019).

Neste novo cenário em que as informações circulam livremente, embora o Brasil já possuísse legislações que tratavam da privacidade e proteção de dados pessoais como a Constituição Federal de 1988, Código Civil, Código de Defesa do Consumidor, Lei do Marco Civil da Internet e a Lei de Acesso à Informação, até 2018 a matéria não era normatizada em Lei especifica. Entretanto com inspiração no Regulamento de Proteção de Dados Pessoais europeu – GDPR 2016/979 o Brasil modificou este cenário com a regulamentação da Lei Geral de Proteção de Dados em 2018 (GLITZ, 2019).

No dia 18 de setembro de 2020 a MP 959 foi convertida em lei 14.058/20, passando então a LGPD ter efeitos imediatos, mas com as sanções administrativas que só passaram a valer a partir do dia 01 de agosto de 2021.

2.1 Constituição Federal

Em meio as transformações socioeconômicas em que vivemos e como dito anteriormente, a Constituição Federal de 1988 consagra o direito à privacidade como um direito fundamental disciplinado em seu artigo 5º, incisos X, XI e XII: (PONTICELLI, 2018)

> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> XI - A casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
>
> XII - É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Alexandre de Moraes (2017, p. 97 apud PONTICELLI, 2018) esclarece que “os conceitos constitucionais de intimidade e vida privada apresentam grande interligação, porém podem ser diferenciados por meio da menor amplitude do primeiro, que se encontra no âmbito de incidência do segundo”. Para o autor, a intimidade diz respeito ao íntimo do indivíduo e suas relações familiares e de amizades, já a vida privada envolve todos os demais relacionamentos humanos.

Portanto, o direito à privacidade possibilita ao indivíduo possuir o domínio do que se encontra consigo, como seu corpo, casa, pensamentos, propriedades, segredos e tudo relacionado a si, tendo a liberdade para escolher o que deseja permitir que outras pessoas tenham acesso, tendo a garantia de que tem a capacidade de controlar a exposição e a disponibilidade de dados e informações sobre si mesmo (PONTICELLI, 2018).

Em conformidade ensina Diniz (2008, p. 157 apud CARVALHO *et al,* 2019) “direito à privacidade da pessoa (CF, art. 5º, X) contém interesses jurídicos, de maneira que o sujeito de direito pode impedir intromissões em sua esfera privada ou íntima (CF, art. 5º, XI), inclusive via internet”.

> Nesse diapasão, frisam-se aspectos referentes à publicidade, sob o ponto de vista jurídico, os quais se encontram positivados na CRFB/88, em vários momentos, notadamente, vinculado ao Poder Público, como forma de garantir a transparência dos atos governamentais (art. 37, *caput e* art.37, §1º), bem como, aos processos judiciais (art. 5°, inciso LX). Conquanto, para a presente pesquisa, realiza-se o corte epistemológico na violação gerada por meio da publicização de dados de caráter pessoal (CARVALHO *et al, 2019).*

Similar a constituição, o código do consumidor e o código civil brasileiro de 2002 também protegem a privacidade e a vida privada.

> Código de Defesa do Consumidor art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
>
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
>
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
>
> § 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

O código de defesa do consumidor (CDC) criou no artigo 43 o banco de dados dos consumidores e ainda o direito destes em ter o acesso aos próprios dados arquivados, trazendo inclusive sanções com a detenção de até 1 ano nos artigos 72 e 73 para quem impedir ou dificultar o acesso (COTS; OLIVEIRA, 2019).

Já o código civil ofereceu maior descrição aos direitos inerentes à personalidade, como a privacidade e a intimidade, prevendo ainda que o juiz deverá adotar as providências necessárias para cessar a violação da vida privada (COTS; OLIVEIRA, 2019).

> Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.
>
> Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.
>
> Art. 16. Toda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome.
>
> Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma (BRASIL, 2002).

2.2 Lei Carolina Dieckmann

O caso ficou conhecido quando a atriz Carolina Dieckmann teve seu computador invadido por hackers (alguém que tenha conhecimento suficiente de informática e segurança usando dessas técnicas para o roubo de informações e dinheiro alheio (SANTINO, 2019)) e consequentemente imagens íntimas vazadas na internet. Antes da lei crimes deste tipo eram decididos com adaptações de artigos existentes no código penal, entretanto, promulgada em 2012 a lei nº 12.737/12 foi a primeira lei brasileira a tratar sobre o assunto de invasão de dispositivos informáticos e consequentemente a primeira a proteger a privacidade cibernética e os dados pessoais (LOES, 2016).

A lei alterou o Decreto-Lei nº 2.848/1940 (Código Penal), acrescentando os artigos 154-A e 154-B tipificando os delitos informáticos e alterou a redação dos artigos 266 e 298 (CÂMARA DOS DEPUTADOS, 2012):

> **“Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.” (BRASIL, 2012).

“Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.” (BRASIL, 2012).

O artigo 266 do Código Penal, passou a vigorar com a seguinte redação:

“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”

Art. 266..

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (BRASIL, 2012).

Acrescentou o parágrafo único ao artigo 298 do código penal.

“Falsificação de documento particular

Art. 298.. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (BRASIL, 2012).

2.3 Marco Civil Da Internet

A lei 12.965/2014, conhecida como Marco Civil da Internet é uma lei que visa a consolidação de direitos, deveres e princípios para a utilização e o desenvolvimento da internet no Brasil. Com a expansão da internet no país e o crescente número de pessoas e empresas a utilizando criou-se novas questões e desafios acerca da proteção de direitos civis e políticos da população, tornando-se necessário a regulamentação e estabelecimento de condições mínimas e essenciais que permitissem o futuro da internet livre e a inovação continua, o desenvolvimento econômico e político e a emergência de uma sociedade culturalmente vibrante (CGI, 2013).

A lei surgiu de uma iniciativa da secretária de assuntos legislativos do ministério da justiça em parceria com o centro de tecnologia e sociedade da escola de direito da Fundação Getúlio Vargas no Rio de Janeiro, tendo como principal inspiração a Resolução de 2009 do Comitê Gestor da Internet no Brasil (CGI.br) intitulada “Os princípios para a governança e uso da Internet”, merecendo destaque 3 itens dentre os 10 (CGI, 2013):

> **1. Liberdade, privacidade e direitos humanos**
> O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.
> **2. Governança democrática e colaborativa**
> A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.
>
> **7. Inimputabilidade da rede**
> O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos (CGI, 2010)

O Marco Civil estabelece princípios acerca do uso da internet no Brasil em seu artigo 3º, dentre eles a proteção da privacidade e a proteção dos dados pessoais: (CGI, 2013).

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> **II - Proteção da privacidade;**

> **III – Proteção dos dados pessoais, na forma da lei;**
>
> IV - Preservação e garantia da neutralidade de rede;
>
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - Preservação da natureza participativa da rede;
>
> VIII - Liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (BRASIL, 2014).

A lei prevê ainda a garantia da privacidade e a proteção dos dados pessoais em cinco artigos: (CGI, 2013).

> **Artigo 9 §3º** Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo (BRASIL, 2014).

O dispositivo citado em concordância com a Resolução CGI.br/RES/2012/008/P veda o monitoramento, análise ou fiscalização de conteúdos por parte de prestadores de serviços ou redes sejam utilizados pela internet (CGI, 2013).

Já em seu artigo 7º e 8º a lei proclama os direitos dos usuários e garante a inviolabilidade da intimidade da vida privada e do sigilo das comunicações para todos os usuários o não fornecimento de dados pessoais a terceiros, salvo o consentimento do usuário, ou hipóteses prevista em lei, informações claras, completas e o consentimento expresso sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais e a exclusão definitiva dos dados que tiver disponibilizado na internet, a requerimento do usuário, no término da relação entre as partes e hipóteses previstas em lei: (CGI, 2013).

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - Não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - Manutenção da qualidade contratada da conexão à internet;

VI - Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - Não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - Informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) Justifiquem sua coleta;

b) Não sejam vedadas pela legislação; e

c) Estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - Exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - Publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - Acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - Aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet (BRASIL, 2014).

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
>
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput,** tais como aquelas que:
>
> I - Impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
>
> II - Em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil (BRASIL, 2014).

Já o artigo 10 estabelece que a guarda e a disponibilização dos registros de que trata a lei e de dados pessoais deve preservar a intimidade, vida privada, honra e a imagem das partes, determinando ainda que o responsável pela guarda dos dados somente será obrigado a disponibilizar informações que levem à identificação do usuário mediante solicitação judicial (CGI, 2013).

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
>
> § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais (BRASIL, 2014).

O artigo 11 estabelece que as operações com dados pessoais ou de comunicação por provedores de internet é obrigatório que sejam respeitados as legislações brasileiras e o direito à privacidade, à proteção dos dados pessoais e o sigilo das comunicações e registro (CGI, 2013).

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo (BRASIL, 2014).

O artigo 12 disponibiliza as sanções que podem ser adotadas em relação ao descumprimento dos artigos 10 e 11, podendo ser aplicadas isolada ou cumulativamente (CGI, 2013).

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - Advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - Multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> III - Suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
>
> IV - Proibição de exercício das atividades que envolvam os atos previstos no art. 11.
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País (BRASIL, 2014).

A lei deixa claro ainda em seus artigos 14 e 16, que é vedado guardar os registros de acesso a aplicações de internet, inclusive a guarda destes registros sem

que o titular tenha consentido previamente, conforme o artigo 7º já comentado aqui e os dados excessivos a finalidade para a qual o titular consentiu (HOSTERT, 2018).

> Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.
>
> Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
>
> I - Dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou
>
> II - De dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular (BRASIL, 2014).

2.4 Cadastro Positivo

A lei 12.414/11 conhecida como a lei do cadastro positivo trata-se de bancos de dados nos quais são armazenadas informações sobre comportamento financeiro do consumidor para uma formação de histórico de crédito sobre a quitação de suas dívidas, pontualidade destes pagamentos dentre outras características que o intitulem como um “bom pagador”, sendo que estes de acordo com sua pontuação possuem melhores chances de aprovação de crédito (KATARIVAS, 2019).

Do projeto de lei até a promulgação algumas mudanças aconteceram e a abertura do cadastro que estava condicionada a autorização prévia do usuário (modelo *opt-in)* passou a ser automática (modelo *opt-out),* fato esse que criou polêmica por tratar-se de quebra de privacidade dos consumidores devido a entrada em vigor da GDPR, o cenário mundial em torno deste novo direito fundamental da proteção de dados pessoais e a aprovação da Lei Geral de Proteção de Dados (LGPD) (KATARIVAS, 2019).

A LGPD visando a proteção de dados pessoais regula o tratamento e a transferência destes dados, afim de proteger os direitos fundamentais de liberdade e privacidade dos titulares. Contudo, apesar da necessidade do prévio e expresso consentimento dos titulares para o tratamento de dados, esta é apenas uma das dez hipóteses de autorização. O artigo 7º da LGPD traz um rol de hipóteses em que o tratamento poderá ser realizado e o inciso X é o tratamento para a proteção do crédito (KATARIVAS, 2019).

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> **X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).**

Portanto a inclusão dos dados pessoais de consumidores independente do consentimento expresso deste ao cadastro positivo poderá ser efetivada. Entretanto estes consumidores ainda possuem direitos de informação, privacidade e o livre acesso à informação que é garantido em ambas as leis (KATARIVAS, 2019).

Verifica-se ainda que o artigo 5º da lei 12.414/11 elenca os direitos dos cadastrados e dentre eles estão o direito de cancelar ou reabrir o cadastro, acessar a informações gratuitamente e independente de justificativa e dentre outros junto com o artigo 20 da LGPD concedem ao titular de dados o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem seus interesses (KATARIVAS, 2019).

> Art. 5º São direitos do cadastrado:
>
> I - Obter o cancelamento ou a reabertura do cadastro, quando solicitado;
>
> II - Acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado;
>
> III - Solicitar a impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 10 (dez) dias, sua correção ou seu cancelamento em todos os bancos de dados que compartilharam a informação;
>
> IV - Conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;
>
> V - Ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais;
>
> VI - Solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
>
> VII - Ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados (BRASIL, 2011).
>
> Art. 20 LGPD: O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (BRASIL, 2018).

Por fim, verifica-se que superada a ausência da necessidade de consentimento prévio do consumidor, hipótese autorizada pela LGPD, o gestor e a fonte do cadastro positivo devem se adequar a Lei Geral de Proteção de Dados e adotar medidas para o cumprimento desta, principalmente a segurança destes dados (KATARIVAS, 2019).

2.5 General Data Protection Regulation – GDPR

A lei com maior relevância no cenário internacional acerca da proteção de dados pessoais é o regulamento 2016/679 da união europeia mais conhecida como GDPR (HOSTERT, 2018).

A pesar de o Brasil já possuir legislações disciplinando e tratando os dados pessoais, como já observado neste capítulo, foi inspirado na GDPR que o Brasil normatizou uma lei especifica, a LGPD (GLITZ, 2019)

Regulamentada em 2016 pela União Europeia, a GDPR tem o objetivo de abordar a proteção de dados pessoais de pessoas físicas e a livre circulação destes dados conhecida pela expressão "*free data flow"* (PINHEIRO p. 18, 2020).

O regulamento Geral de Proteção de Dados Europeu nº 679 ocasionou um "efeito dominó", haja vista que começou a exigir outros países e empresas que possuíam interesse em manter relações comerciais com os países da U.E. deveriam possuir uma legislação do mesmo nível que o GDPR, devido ao Estado que não possuísse lei de mesmo nível passaria a poder sofrer sanções econômicas ou dificuldade de fazer negócios (PINHEIRO p. 18, 2020).

> Segundo o preâmbulo do GDPR, o regulamento tem como objetivo: a) contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas; b) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno; c) garantir a segurança jurídica e a transparência aos órgãos públicos e à sociedade como um todo; d) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais; e) possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros (PINHEIRO p.18, 2020).

Na Europa o direito fundamental do tratamento de dados pessoais já estava previsto na Carta dos Direitos Fundamentais da União Europeia e no tratado sobre o funcionamento da União Europeia (PINHEIRO p. 19, 2020).

Os efeitos da GDPR são especialmente econômico, social e político, tendo em vista que muitas regulamentações surgirão nesta linha que se busca mecanismos para controlar e equilibrar as relações em um cenário de negócios digitais (PINHEIRO p.19, 2020).

A lei brasileira está dividida em 10 capítulos, com 65 artigos, menor que a lei de sua referência (GDPR), que possui 11 capítulos, com 99 artigos. A versão nacional por ser mais enxuta deixa margens para uma intepretação mais ampla, que poderá trazer alguns pontos de insegurança jurídica. (PINHEIRO p. 21, 2020).

Tanto a LGPD e a GDPR trazem um rol de princípios que precisam ser atendidos, afim de garantir direitos fundamentais como a proteção de dados, fortalecendo a privacidade do titular de dados e proteger o desenvolvimento econômico e tecnológico. O artigo 5º da GDPR traz os princípios que norteiam, são eles: 1 licitude; 2 lealdade; 3 transparência; 4 limitação de finalidade; 5 minimização dos dados; 6 exatidão; 7 limitação da conservação; 8 integridade e confidencialidade (que são os mesmos da segurança da informação) e 9 responsabilidade (PINHEIRO p. 41 e 42, 2020).

Já a LGPD deve estar orientada pelos seguintes princípios conforme o artigo 6º da lei:

> Art. 6º 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 (BRASIL, 2018).

Importante destacar ainda que a GDPR pode ser aplicada a empresas brasileiras, devido sua aplicabilidade abranger os dados coletados de pessoas naturais que se encontram na união europeia (CARVALHO; SANTOS, 2019).

Por fim, várias são as semelhanças entre as leis, que tem como base legal o consentimento e sobre isto Carvalho e Santos (2019) afirmam que:

> O consentimento por escrito deverá constar em cláusula separada das demais; a prova do consentimento é um ônus do controlador/responsável, entre outras. Uma importante diferença entre as normas é que a GDPR não caracteriza como livre o consentimento quando este se mostra como um requisito para a prestação de um serviço, enquanto a LGPD apenas destaca que o titular dos dados pessoais deve ser informado quando o tratamento de dados é condição para obtenção de um produto ou serviço.

As diferenças entre as normas podem ser visualizadas na tabela 1 (ZYGON DIGITAL, 2019, apud CARVALHO; SANTOS, 2019):

GDPR		LGPD
Multa de até € 20 milhões ou 4% sobre a receita anual global da empresa, o que for maior.	Penalizações	Mais amenas, de advertências a 2% do faturamento total da empresa.
É necessário ter um representante estabelecido em um dos Estados-membros.	Representantes	Não existe nenhuma obrigatoriedade em relação ao local de estabelecimento.
São aceitas autorizações de menores com no mínimo 16 anos.	Dados de Menores de Idade	Dados de menores de 18 anos precisam de autorização do responsável para serem usados.
Obrigatório	Políticas Internas de Proteção de Dados	Opcional
Deverá ser realizado quando o tratamento dos dados oferecer risco elevado à privacidade dos mesmos. O GDPR detalha as informações que devem constar no documento.	Relatório de Impacto	Não há nenhuma especificação sobre a necessidade de um relatório do tipo.
Necessidade de um contrato que comprove o vínculo entre as duas partes.	Relação Controlador - Operador	Não é necessária a formalização do vínculo.
Regulamento específico para os dados tratados com esta finalidade.	Marketing Direto	Não possui uma previsão específica nas normas.

(FONTE: ZYGON DIGITAL, 2019).

3 CONCEITO E TRATAMENTO DE DADOS PESSOAIS

Não restam dúvidas quanto a importância do tratamento dos dados pessoais para o desenvolvimento econômico global de forma que ao mesmo tempo também se assegure os direitos do titular de dados que necessita saber sobre oque é um dado pessoal e a lei geral de proteção de dados disciplina isso em seu artigo 5º: (FIESP, 2019)

> Art. 5º, I: dado pessoal é informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2018).

A lei como vimos traz um conceito amplo e aberto, pois qualquer dado que isoladamente (dado pessoal direto) ou agregado a outro (dado pessoal indireto) possa permitir a identificação de uma pessoa natural, pode ser considerado como dado pessoal (FIESP, 2019).

Dados pessoais segundo Pinheiro (2020, p. 35) trata-se de toda informação relacionada a uma pessoa identificada ou identificável, informação esta que não se limita a somente nome, sobrenome, idade, endereço residencial, dados de localização, perfis de compra, entre outros. As informações estão sempre relacionadas a pessoa natural viva.

Os dados anonimizados (art. 5º, III: titular que não pode ser identificado) ou que passam por processo de anonimização (art. 5º, XI: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo) não são considerados dados pessoais. Da mesma forma, a lei não atinge diretamente os documentos confidenciais, segredos de negócios, fórmulas, direitos autorais ou propriedade industrial, que são protegidos por outras normas, sendo que somente eventuais dados pessoais que estejam dentro de tal tipo de conteúdo (FIESP, 2019), salvo quando o processo de anonimização for revertido, utilizando exclusivamente meios próprios, ou quando, puder ser revertido com esforços razoáveis (art.12 da LGPD).

Tal ressalva pode segundo Pinheiro (2020, p. 92) gerar interpretações subjetivas chegando à insegurança jurídica.

> Um estudo realizado por um grupo de pesquisadores do Media Lab do Instituto Tecnológico de Massachusetts (MIT) em 2014 apontou que, a partir da criação de alguns algoritmos matemáticos, é possível identificar uma pessoa baseando-se em seus hábitos de compra (PINHEIRO, 2020 p. 92).

Portanto a instituição de tratamento de dados deve demonstrar que o método utilizado impossibilita sua reversão para aquele que recepcionou o dado anonimizado (Pinheiro, 2020 p. 92).

O tratamento de dados assim como o conceito de dados pessoais é amplo, a LGPD traz um conceito aberto e um rol exemplificativo sobre oque é considerado como tratamento de dados pessoais: (FIESP, 2019)

> Art. 5º, X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

A lei em seu artigo 7º também traz um rol de requisitos necessários para o tratamento de dados pessoais, os quais as empresas deverão comprovar ao menos uma das hipóteses para que possam realizar o tratamento (FIESP, 2019).

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - Mediante o fornecimento de consentimento pelo titular;
>
> II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
>
> VII - Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII - Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

> IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
>
> § 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)
>
> § 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)
>
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
>
> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
>
> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
>
> § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
>
> § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei (BRASIL, 2018).

Antes do parágrafo 1º ser revogado pela MP 869/2018 e tal revogação mantida pela lei 13.853/19, o referido parágrafo exigia que o titular dos dados fosse “informado das hipóteses em que será submetido o tratamento de seus dados”, portanto o controlador deveria comunicar ao titular desta informação, entretanto a LGPD não previu nenhuma regra de como isso se daria. Além do parágrafo 1º a MP também revogou o 2º tornando então dispensável o cumprimento da obrigação de informação ao titular sobre o tratamento de seus dados (COTS; OLIVEIRA, 2019).

Segundo Pinheiro (2020, p. 84) a lei brasileira salienta ainda que o tratamento de dados pessoais deve observar a boa-fé e possuir finalidade, limites, prestação de contas, garantir a segurança por meio de técnicas e medidas de segurança, assim como a transparência e a possibilidade de consulta aos titulares.

A natureza jurídica de que trata o consentimento previsto no inciso I do artigo 7º da LGPD, sendo este uma base legal para o tratamento de dados está previsto no artigo 8º da lei e sua natureza é contratual, pois sendo bilateral temos de um lado a manifestação da vontade do titular que anui o tratamento e de outro em tratar os dados pessoais (COTS; OLIVEIRA 2019, p. 91,).

A LGPD ainda no artigo 8º possibilita que este consentimento seja também por outro meio que demonstre a manifestação de vontade do titular que não seja a forma escrita, entretanto este meio deve preservar a manifestação de vontade inequívoca, não permitindo a atuação passiva do titular (COTS; OLIVEIRA, 2019, p.92).

Este “outro meio” possibilita até mesmo a utilização de vídeos ou artes gráficas pelo titular com os termos do tratamento, devendo manifestar a vontade e não apenas informar, poderiam ser utilizados por exemplo os *tokens,* SMS, autenticação por e-mail, login, registros de áudios, vídeos ou ambos, dentre tantos outros. Oque não pode faltar para que a manifestação de vontade seja legitima é que seja preservada e inequívoca, compreensível e que esteja adequadamente atrelada aos termos do determinado tratamento de dados (COTS; OLIVEIRA, 2019, p. 92).

Segundo Cots e Oliveira (2019, p.95) o consentimento só é válido em casos em que se direcione a um tratamento específico ou determinado, portanto os termos como “melhorar a experiencia do usuário” ou “para formação de cadastro” não serão mais admitidos, se tornando nulos.

Também deverá haver um consentimento específico para que ocorra a comunicação ou o compartilhamento entre controladores distintos, devendo estar expresso e previsto no contrato (COTS; OLIVEIRA, 2019, p.95).

A revogação do consentimento se dará a qualquer momento, mediante manifestação expressa do titular por meios gratuitos e facilitados, o controlador ainda poderá enquadrar o tratamento de dados em outra base legal para continuar o tratamento, caso contrário deverá ser imediatamente interrompido e o tratamento realizado antes da revogação poderá ser mantido até que se tenha requerido a eliminação destes dados. A revogação deverá se dar através do mesmo meio pelo qual se deu o consentimento, possibilitando que o consentimento coletado pela internet deverá ser revogado também através de recursos *on-line* (COTS; OLIVEIRA, 2019, p.96).

Por fim, outra questão relevante a ser destacada é sobre a proteção de dados pessoais *post mortem* e a lacuna ainda existente no ordenamento jurídico sobre esse assunto que a LGPD não abordou (QUIRINO, 2019).

Vários usuários vêm a óbito por dia e consequentemente deixam um legado digital registrado em cada uma de suas redes sociais que utilizava, com isso muitos se perguntam sobre o direito destes falecidos e qual o regime jurídico para tratar do assunto (QUIRINO, 2019).

Segundo Leal (2019) o assunto ganhou relevância após os pais de uma menina de 15 anos, que morreu em uma estação de trem em 2012 na Alemanha, os genitores pleiteavam o acesso à conta do *facebook* da filha falecida, pretendendo investigar se a morte teria ocorrido por um acidente ou suicídio, através de conversas. Em primeira instância, o pedido foi deferido, entretanto o tribunal reformou a decisão e após um novo recurso no Tribunal Federal o acesso foi autorizado.

Já no Brasil, em 2013 a 1ª Vara do Juizado Especial Central do Estado de Mato Grosso do Sul deferiu o pedido em sede liminar, determinando a exclusão da página, após uma mãe pedir administrativamente que o *facebook* desativasse o perfil da filha falecida, que segundo a genitora havia se tornado um “muro de lamentações”, sendo negado pelo provedor (LEAL, 2019).

Atualmente, após inúmeras situações parecidas, o *facebook* possui fermentas em sua plataforma para esse tipo de situação. O usuário pode optar pela transformação da conta em memorial, indicando um herdeiro para administra-la ou optar pela exclusão da conta após o óbito (QUIRINO, 2019).

O GDPR exclui expressamente sua aplicação ao dados pessoais de falecidos, deixando tal regulamentação a cargo de cada Estado, a partir daí alguns países como a Bulgária que reconheceu que nestes casos os direitos serão exercidos através dos herdeiros, já na Estônia os dados referentes as pessoas falecidas somente é permitido com o consentimento por escrito de seu sucessor, cônjuge, descendente ou ascendente, irmão ou irmã, exceto nos casos de que não se exija consentimento do titular ou se já se passaram 30 anos de sua morte (LEAL, 2019).

A LGPD declara que o consentimento do titular é um requisito para o tratamento de dados, todavia não previu qual seriam os efeitos da morte do titular, ou se os direitos da proteção de seus dados seriam passados a seus familiares denominado de “herança digital” (LEAL, 2019). Posto isso resta a Autoridade Nacional de Proteção de Dados e ao Poder Judiciário Brasileiro interpretar este novo

dispositivo, haja vista que, a LGPD não possui disposição expressa que proíba sua aplicação aos falecidos (QUIRINO, 2019).

Conforme Quirino (2019) disciplina, o Brasil possui tendências legislativas com base no direito sucessório, tendo projetos de lei como o 1.331/15 que foi arquivada, mas previa que o cônjuge, ascendente e descendente fossem partes legítimas para exigir a exclusão dos dados pessoais do falecido.

3.1 Tratamento De Dados Pessoais Sensíveis

Dados pessoais sensíveis conforme a LGPD disciplina em seu artigo 5º, II trata-se 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”, ou seja, dados da pessoa natural identificada ou identificável que por consequência de os possuir possa ser discriminada e devido a isto estes dados devem ser considerados e tratados como sensíveis (FIESP. 2019).

O amplo conceito em que a lei traz os dados sensíveis já era conhecido pela Lei do Cadastro Positivo em seu artigo 3º, §3º, II, que proíbe anotações em bancos de dados para a análise de crédito de “informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas”, ou seja, é proibida a inclusão de quaisquer informações de natureza personalíssima que não se relacione com a finalidade almejada para a análise do crédito (Mulholland, 2018).

O princípio da não discriminação é o mais relevante tratando-se de dados sensíveis, uma vez que o ponto fundamental diante destes dados é a sua capacidade discriminatória, seja por entes privados ou públicos (Mulholland, 2018). Outro ponto importante a se destacar é o consentimento do titular de dados, que referindo-se ao tratamento de dados sensíveis é intrínseco à validade desta ação conforme o artigo 11, I da LGPD, entretanto o mesmo artigo em seu inciso II traz a ressalva de que em determinadas situações o consentimento pode ser relativizado (Pinheiro, 2020 p. 90).

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

> a) Cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
>
> e) Proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
>
> g) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018).

Nestas situações de dispensa do consentimento, o controlador (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI)) é obrigado a publicitar essa situação (PINHEIRO, 2020, p.90).

O regulamento europeu, o GDPR, também deixa claro a preocupação com os dados sensíveis em seu artigo 9º conforme explica Pinheiro (2020, p. 91) “o consentimento é essencial no tratamento de dados sensíveis, embora haja exceções cujos procedimentos devem respeitar com a mesma seriedade e garantia da segurança ao tratamento”. O regulamento ainda disciplina que as informações que o próprio titular tornou pública também dispensam o seu consentimento (Pinheiro p.91, 2020).

Os dados biométricos e genéticos também foram considerados sensíveis pela LGPD, conforme o artigo 5º, tendo em vista o grande aumento na utilização destes recursos no mundo globalizado, todavia, a fim de não atrapalhar o desenvolvimento de novas tecnologias, disciplinou uma base legar na alínea “g” do artigo 11 da lei, segundo esta é possível o tratamento de dados sensíveis para garantir a prevenção à fraude e à segurança do titular, sendo essas duas hipóteses limitadas aos processos de identificação e autenticação de cadastro de sistemas eletrônicos (COTS; OLIVEIRA, 2019, p. 112).

3.2 Tratamento De Dados Pessoais De Crianças E Adolescentes

Crianças e adolescentes da chamada geração Z (nascidos entre 1990 e 2010) e Alpha (nascidos a partir de 2010) já nasceram em meio a tecnologia e não é segredo que muita das vezes sabem mais sobre a tecnologia que seus pais e não é raro ver crianças que nem aprenderam a ler ainda, lidando normalmente com aparelhos eletrônicos. Pensando nesta coleta de dados digitais o legislador regulamentou no artigo 14 da LGPD o tratamento de dados pessoais da criança e do adolescente, determinando que deverão ser tratados em seu melhor interesse (ALBRECHT, 2019).

Primeiramente convém para um melhor entendimento esclarecer o conceito de criança e adolescente, que está previsto no Estatuto da Criança e do Adolescente (ECA), sendo considerado criança a pessoa de até 12 anos de idade incompletos e adolescente, aquela entre 12 e 18 anos (ALBRECHT, 2019).

A definição de melhor interesse de que trata o *caput* do artigo 14, deve se interpretar como um fundamento básico de toda e qualquer orientação ou decisão envolvendo crianças e adolescentes, devendo-se levar em conta o melhor e mais adequado para a satisfação de seus anseios (ALBRECHT, 2019).

No parágrafo 1º do artigo 14, a lei determina que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento especifico de pelo menos um dos pais ou responsável legal, silenciando-se quanto aos dados dos adolescentes. Dessa maneira, o consentimento parental previsto na LGPD é indispensável apenas quando se tratar de menores de 12 anos, de forma que os demais teriam capacidade para dispor sobre seus dados (B. F. F. YANDRA, A. C. A. SILVA, J. G. SANTOS, 2020).

Em contramão o Código Civil, define que são absolutamente incapazes os menores de 16, devendo ser representados por seus pais ou responsáveis legais e relativamente incapazes os maiores se 16 e menores de 18 anos que são assistidos pelos pais ou responsáveis, conforme os artigos 3º e 4º, inciso I. No primeiro caso o responsável toma as decisões pelo menor, respeitando seus interesses e no segundo caso o responsável apenas verifica a regularidade e a validade da decisão tomada pelo menor (B. F. F. YANDRA, A. C. A. SILVA, J. G. SANTOS, 2020).

Desta forma ao admitir que menores de 16 anos tenham capacidade para consentir sobre seus dados, a LGPD vai de encontro com o Código Civil, o qual afasta

a capacidade absoluta dos que se encontram nesta faixa etária (B. F. F. YANDRA, A. C. A. SILVA, J. G. SANTOS, 2020).

Nesta linha, nota-se que a União Europeia no artigo 8º do GDPR tem condições parecidas quanto a coleta de dados pessoais de crianças e adolescentes, destacando a necessidade de proteção especial a este grupo de pessoas. Um diferencial é que no regulamento no que concerne a oferta direta de serviços, é licito o consentimento dado por um adolescente de no mínimo 16 anos e os indivíduos com menos de 16 anos de idade necessitam do consentimento dos pais ou responsáveis legais e dependendo do Estado-Membro a idade mínima pode ser de 13 anos, ou seja, dependendo do país, os jovens poderão dar seu consentimento desde os 13 anos ou dos 16, ou mesmo precisar de consentimento para tanto. Destaca-se ainda que os menores de 13 anos sempre precisarão de consentimento de pais ou responsáveis (PINHEIRO, 2020 p. 96).

Portanto a finalidade do consentimento parental não é restringir o acesso de crianças e adolescentes aos meios digitais, mas sim protege-los e devido ao desenvolvimento incompleto dos adolescentes, ainda em fase de amadurecimento a LGPD deveria ter concedido a estes indivíduos um tratamento especial possibilitando o controle familiar (B. F. F. YANDRA, A. C. A. SILVA, J. G. SANTOS, 2020).

Posto isso, resta aos controladores o dever de empreender todos os esforços para atestar que o consentimento foi concedido, oque na pratica estes controladores deveram estar atentos, especialmente se utilizam a internet e passar a utilizar de recursos como audiovisuais para se comunicar com os responsáveis dos menores (COTS; OLIVEIRA, 2019).

O parágrafo 2º disciplina que a coleta de dados consentida por pelo menos um dos pais ou responsável legal deverão os controladores de acordo com sua obrigação manter publica a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos do titular de dados (FRANZÃO, 2018).

Como toda lei, a LGPD também traz exceções quanto a este consentimento de pais ou responsáveis, em seu paragrafo 3º a lei expõe a única exceção, sendo nos casos em que a coleta for necessária para contatar os pais ou o responsável legal e mesmo assim utilizados uma única vez e sem armazenamento e em nenhum caso poderão ser repassados a terceiros sem o consentimento de pelo menos um dos pais ou responsável (FRANZÃO, 2018).

Já no parágrafo 4 a lei declara que os controladores (pessoa natural ou jurídica, de direito publico ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI)) não deverão condicionar a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além da estritamente necessárias à atividade. Desta forma a LGPD sintetiza que os serviços ofertados ao fornecimento de informações pessoais, salvo os estritamente necessária a atividade e considerado abusivo em caso de desrespeito, mesmo que anteriormente pudesse haver consentimento (FRANZÃO, 2018).

Conforme Albrecht (2019) o grande desafio para o controlador será conseguir identificar que o consentimento foi cedido, de fato, pelo responsável pela criança ou adolescente.

A legislação ainda impõe ao controlador no parágrafo 5º que este deverá realizar todos os esforços razoáveis para verificar o consentimento de um dos pais ou responsável legal da criança, considerando as tecnologias disponíveis e que as informações referentes ao tratamento de dados tratado neste dispositivo deveram ser fornecidas de maneira simples, clara e acessível, conforme o parágrafo 6º (Albrecht, 2019)

> § 5º - O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (BRASIL, 2018).

3.3 Término Do Tratamento De Dados

O tratamento de dados pessoais possui um limite de atuação, sendo este um dos requisitos de sua validade, este limite é intrínseco ao princípio da finalidade do tratamento, pois quando a finalidade do tratamento chega ao fim não há motivos para que se continue com o procedimento, não podendo ser realizado por tempo indeterminado (PINHEIRO, 2020).

O término do tratamento de dados determina o encerramento da utilização de dados pessoais e a eliminação destes nos limites técnicos das atividades, sendo autorizada sua conservação somente nos casos elencados no artigo 16 da LGPD: (PONTICELLI, 2018).

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I - Cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II - Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
>
> IV - Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

As hipóteses para o término de tratamento de dados estão disciplinadas no artigo 15 da LGPD e o descumprimento após constatados um destes cenários acarreta na violação do direito fundamental à privacidade do titular (PONTICELLI, 2018).

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I - Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
>
> II - Fim do período de tratamento;
>
> III - Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
>
> IV - Determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

O primeiro inciso deste artigo se subdivide em três situações, sendo a primeira a análise de que a finalidade do tratamento tenha sido atingida, a segunda e a terceira apesar de abordadas separadamente o termo “pertinente” engloba o termo “necessário”, haja vista que o que é necessário consequentemente é pertinente Ponticelli (2018) ainda diz que “é viável ignorar a condição da necessidade dos dados

para o alcance da finalidade almejada, podendo apenas ser feita a indagação se é pertinente a continuidade deste tratamento".

A revogação do consentimento pelo titular é um de seus direitos elencados no artigo 18 da lei, o qual iremos tratar em outro capitulo (PONTICELLI, 2018).

De certa forma mesmo que tenha se preenchido um dos requisitos pra o término do tratamento de dados o artigo 16 abre a possibilidade para que desde que preenchidos os requisitos não chegue ao fim, como nos casos de dados anonimados em que o término do tratamento não se dará (PONTICELLI, 2018).

Uma das diferenças entre a legislação brasileira e a europeia é que na LGPD a limitação do tempo obriga o controlador a realizar o apagamento ou a revisão dos dados coletados, vinculando os prazos a necessidade do processo e o GDPR recomenda que os prazos sejam determinados de acordo com a finalidade do tratamento, tendo vinculação direta com a finalidade do procedimento (PINHEIRO, 2020, p.97).

Por fim, o preâmbulo do GDPR ainda diz que "a fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica" (PINHEIRO, 2020, p.98).

3.4 Órgãos Reguladores

O principal órgão regulador e fiscalizador da proteção de dados pessoais no Brasil é a ANPD (Autoridade Nacional de Proteção de Dados), entretanto o titular de dados, entidades de classe, PROCON, Ministério Público e qualquer agência reguladora da respectiva atividade também possuem um papel importante neste âmbito. (MENDES, 2019).

O titular de dados, além de seus direitos previamente constituídos no artigo 7º da LGPD, pode também realizar a avaliação da reputação da empresa em sites como o "Reclame Aqui", exercendo a função de fiscalizador. Os titulares de dados podem processar a empresa que não estivem adequados a lei, além dos eventuais danos morais e materiais. (MENDES, 2019).

A ANPD foi criada pela MP 869/2018 e convertida em lei 13.853/19, haja vista ter sido vetada do projeto de lei pelo presidente da república, devido a

inconstitucionalidade no processo legislativo, que afrontava os artigos 61, §1, II e 37, XIX da Constituição. (COTS; OLIVEIRA, 2019, p.219 e 220).

Ao contrário do que era previsto, a ANPD terá menos independência, pois, agora, faz parte da administração direta e não terá autonomia administrativa e nem personalidade jurídica própria, devendo observar as diretrizes da União, fato que muitos doutrinadores criticam. (COTS; OLIVEIRA, 2019, p.221).

Por outro lado, a agência estará sujeita a aplicação do artigo 37 da Constituição e deverá obedecer, entre outras obrigações, os princípios da administração pública. (COTS; OLIVEIRA, 2019, p.221). Alternativamente, foi assegurado a autoridade a autonomia técnica e decisória, conforme artigo 55-B.

Outro fato muito discutido é o de que a ANPD foi criada com a premissa de “sem aumento de despesa”, sendo que a princípio pode parecer uma boa coisa devido ao momento econômico em que foi criada e a onda de contenção das despesas públicas atualmente, entretanto alguns doutrinadores apontam um certo descaso do Governo para com o tema, tendo em vista a grande importância da agência. (COTS; OLIVEIRA, 2019, p.221).

No entanto, conforme COTS e OLIVEIRA (2019, p.22) relatam “a lei 13.853/19 prevê que a ANPD poderá, após 2 (dois) anos da “entrada em vigor da estrutura regimental” se tornar um órgão da administração indireta, por decisão do executivo”.

De acordo com o artigo 55-C a ANPD será composta por:

Conselho Diretor, órgão máximo de direção, que será formado por “5 membros, responsáveis por administrar, planejar e tomar decisões pertinentes ao bom funcionamento da LGDP. Um Diretor-Presidente será designado para encabeçar o Conselho”. (VARELLA, 2019).

Conselho Nacional de Privacidade de Dados Pessoais e da Privacidade, “possuindo uma formação de diversos nichos, será composto por 23 membros da sociedade, sem direito a voto nas tomadas de decisões da ANPD. Conforme o Artigo 58 da lei”. (VARELLA, 2019).

Corregedoria, “Setor especializado na apuração de erros ou práticas que não estejam em conformidade com a lei. Em caso de erros dos agentes públicos, o setor será o responsável por aplicar as penalidades necessárias”. (VARELLA, 2019).

Ouvidoria, “especializada em atender a população, é a ponte entre os titulares dos dados e a ANPD, responsável por atender a reclamações, dúvidas e mensagens, em geral”. (VARELLA, 2019).

Órgão de Assessoramento Jurídico Próprio, “é o setor especializado em consultoria e assistência jurídica na aplicação da LGPD, para pessoas físicas e jurídicas. É quem vai apoiar a implementação da lei esclarecendo as principais dificuldades que possam ser apresentadas durante os projetos de *compliance”*. (VARELLA, 2019).

Unidades administrativas e unidades especializadas “necessárias à aplicação da lei, Setor formado por diversos órgãos, que serão os responsáveis diretos pela aplicação do que dispõe a Lei Geral de Proteção de Dados”. (VARELLA, 2019).

As competências da Autoridade Nacional de Proteção de Dados Pessoais estão no artigo 55-J, elencadas em 24 incisos.

A ANPD é quem irá aplicar as sanções em caso de descumprimento da LGPD, conforme artigo 52 da lei. Vale lembrar que tais sanções são administrativas e não impedem eventuais processos na esfera judicial, sanções que poderão ter multa de até 50 (cinquenta) mil reais. (COTS; OLIVEIRA, 2019, p.236).

Entretanto, antes da aplicação de multas e outras sanções a autoridade observará cada caso, não se aplicando uma receita genérica para todos os segmentos, respeitando a ampla defesa, de forma gradativa, isolada ou cumulativamente. (LIMA, 2020).

4 ABRANGÊNCIA DA LEI

A LGPD disciplinou sua abrangência em seu artigo 3º garantido que qualquer operação de tratamento realizada, independente do meio, do país sede ou país onde esteja localizado os dados serão atingidos pela lei, a mesma lógica prevista pelo Marco Civil da Internet (PINHEIRO, 2020, p.75).

O artigo trouxe três hipóteses legais, as quais não são cumulativas, portanto, aplicadas independentemente uma da outra e a expressão “independente do meio” tratada no *caput* do artigo abrange além dos dados online, os offline também (COTS; OLIVEIRA, 2019, p.62).

> Art. 3º Esta Lei aplica-se a 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:
>
> I - A operação de tratamento seja realizada no território nacional;

> II - 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; ou
>
> III - Os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
>
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
>
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

A primeira hipótese de aplicação da lei que o artigo traz é sobre o tratamento que ocorre dentro do território nacional, seja por um controlador ou um operador. Não descartando as hipóteses em que o tratamento ocorra somente com pessoas estrangeiras, se o tratamento se deu em território brasileiro o mesmo será alcançado pela lei (COTS; OLIVEIRA, 2019, p.63).

A segunda hipótese de abrangência da lei ocorre com o tratamento para oferta ou fornecimento de bens ou serviços para qualquer pessoa que esteja em território brasileiro. Nesta hipótese o critério é a localização e não a nacionalidade, assegurando até mesmo estrangeiros que estejam no país mesmo que por um curto período (COTS; OLIVEIRA, 2019, p.63).

Neste caso com “ofertas de bens ou serviços” podemos citar casos de sites estrangeiros que apesar de seu idioma em português não significa que os produtos ou serviços estejam em território brasileiro (COTS; OLIVEIRA, 2019, p.63).

A terceira hipótese é através de dados coletados no território nacional, como exemplo Cots e Oliveira (2019, p.63) cita a empresa estrangeira que que envia prepostos para a coleta física de dados e encaminhamento destes ao exterior. Os autores ainda explicam que a coleta destes dados já está atribuída no conceito de tratamento, portanto, a terceira hipótese se equivale a primeira.

4.1 Transferência Internacional De Dados

Em 2014 o primeiro dispositivo brasileiro a disciplinar a transferência internacional de dados foi a Lei do Marco Civil em seu artigo 11, se apresentando como única lei infraconstitucional a tratar dados pessoais nas redes até a LGPD (VIEIRA, 2019).

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por

> provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo (BRASIL, 2014).

De acordo com o marco civil, mesmo que o tratamento de dados tenha sido realizado por pessoa jurídica estrangeira, se o serviço foi ofertado aos brasileiros ou a integrante de grupo econômico com estabelecimento no Brasil, a legislação é aplicável (VIEIRA, 2019).

A LGPD inspirou-se no GDPR ao tratar sobre as transferências internacionais de dados pessoais defendendo que os países que pretendem fazer este tipo de operação deverão conceder a garantia da proteção dos dados no mesmo nível que a LGPD protege (PINHEIRO, 2020, p.112).

Desta forma o Brasil conforme Pinheiro (2020, p.112) segue o movimento europeu de padronização internacional do fluxo de dados, assim como de proteção dessas informações, de maneira a garantir o desenvolvimento tecnológico e econômico.

A LGPD tratou sobre a transferência internacional de dados em seu artigo 33 e seguintes trazendo um rol de nove hipóteses tratada nos incisos (VIEIRA, 2019).

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> II - Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

> a) Cláusulas contratuais específicas para determinada transferência;
>
> b) Cláusulas-padrão contratuais;
>
> c) Normas corporativas globais;
>
> d) Selos, certificados e códigos de conduta regularmente emitidos;
>
> III - Quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
>
> IV - Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> V - Quando a autoridade nacional autorizar a transferência;
>
> VI - Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
>
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
>
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente está de outras finalidades; ou
>
> IX - Quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.
>
> Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional (BRASIL, 2018).

A primeira hipótese trata sobre o mesmo grau de jurisdição e esta prevista no inciso I do artigo, possibilitando, portanto, transferência de dados para outros países que proporcionem o mesmo grau de proteção previsto pela LGPD. Esta hipótese protege os dados de usuários, levando em consideração os tratados, convenções internacionais e legislações interna de cada país (VIEIRA, 2019).

A segunda hipótese de garantias que o controlador oferece, permitindo a transferência após o oferecimento e a comprovação destas garantias de que cumprirá a LGPD. Esta hipótese benéfica os controladores que estão localizados em países cuja proteção de dados não se equiparam a lei brasileira, como é o caso por exemplo dos Estados Unidos (COTS; OLIVEIRA, 2019, p. 164).

O compromisso do controlador deve se dar através de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; e, d) selos, certificados e códigos de conduta regularmente emitidos (COTS; OLIVEIRA, 2019, p. 164).

A terceira hipótese aborda a cooperação jurídica internacional, possibilitando dois tipos de colaboração: a comum, abordada no inciso VI, e a jurídica, tratada no inciso III, que ocorre apenas entre órgãos públicos, para objetivos específicos (COTS; OLIVEIRA, 2019, p. 164).

Esta hipótese tem por finalidade investigações conduzidas por outros países, sendo imprescindível para combater os crimes *cibernéticos,* haja vista que nestes tipos de crimes a prova da materialidade autoria pode se dar em qualquer computador e de qualquer outro país (VIEIRA, 2019).

A quarta hipótese visa a proteção da vida ou da incolumidade física do titular ou de terceiros, ainda que o nível de proteção de dados do local de destino seja inferior a LGPD, tendo como exemplo a transferência de registros médicos de um país que o titular tenha sofrido acidente e precisa de seu histórico para bom diagnostico (VIEIRA, 2019).

A quinta hipótese autoriza a transferência internacional desde que haja a autorização expressa da autoridade nacional para a transação que não esteja prevista em outo inciso. Os autores Cots e Oliveira (2019, p.164) apontam que esta hipótese permite uma “carta branca” á autoridade nacional pois deveria se ter acrescentado ao inciso que a autorização deveria se dar dentro do contexto da LGPD, não abrindo margem para transferências sem o mínimo oferecimento de garantias aos titulares.

A sexta hipótese prevista no inciso VII ocorre quando tratamos de política pública e atribuição legal, que além de justificar a transferência precisa ser objeto de publicidade conforme o artigo 23, inciso I da LGPD: (COTS; OLIVEIRA, 2019, p. 165).

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades,

> em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (BRASIL, 2018).

A sétima hipótese para transferência internacional prevista no inciso VII do artigo torna possível também o compartilhamento nos casos em que ocorre o consentimento do titular, devendo este se de forma previa e destacada quanto ao tratamento e a finalidade deste (COTS; OLIVEIRA, 2019, p. 165).

Os autores Cots e Oliveira (2019, p. 165) defendem que ainda que a transferência traga riscos ao titular será valida desde que este tenha sido informado com clareza e precisão.

Assim, é importante destacar os famosos “Termos e Condições de Uso” que muitas vezes possuem textos enormes e extremamente técnicos que na maioria das vezes são ignorados por usuários, permitindo a plataforma acessar os dados do titular. Por conta disto, sendo o consumidor hipossuficiente e este um tipo de contrato de consumo, aceitar os termos não significa que o titular se manifestou livremente, que foi informado e que esta manifestação é inequívoca. Para que isto ocorra deverá a plataforma destacar esta clausula das demais e não a possuir apenas na forma implícita (OLIVEIRA, 2019).

Na oitava hipótese prevê o tratamento de dados pessoais para as hipóteses dos incisos II, V e VI do artigo 7º da LGPD, devendo ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador, quando necessária a execução do contrato, a pedido do titular ou para o regular exercício de direitos em processos judiciais (VIEIRA, 2019).

O nível de proteção de dados estrangeiros mencionado no inciso I por ser difícil e custoso para os agentes de tratamento analisarem as legislações estrangeiras e compara-las, esta será avaliada pela autoridade nacional de acordo com o artigo 34 que levará em consideração (COTS; OLIVEIRA, 2019, p.166):

> I - As normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
>
> II - A natureza dos dados;
>
> III - A observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
>
> IV - A adoção de medidas de segurança previstas em regulamento;

> V - A existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
>
> VI - Outras circunstâncias específicas relativas à transferência (BRASIL, 2018).

4.2 Tratamento De Dados Pelo Poder Público

As pessoas jurídicas de direito público do mesmo modo que as privadas tem o dever de apresentar para o tratamento de dados possuir uma finalidade clara e transparente, tendo a de direito público finalidade e interesse público (PINHEIRO, 2020).

Estes mesmos órgãos deverão ainda obedecer aos princípios constitucionais (COTS; OLIVEIRA, 2019, p.141).

> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:(BRASIL, 1988).

Além disso, a LGPD determinou requisitos para o tratamento de dados pelo poder público: (1) o ente público deverá publicar de forma clara e precisa de preferência em seu site informações relativas ao tratamento, como a previsão legal, finalidade, procedimentos e praticas utilizadas no tratamento, entre outras informações do inciso I; (2) seja indicado um encarregado (COTS; OLIVEIRA, 2019, p.145).

Destaca-se ainda que de acordo com o artigo 7º, inciso III o poder público pode tratar dados por meio de base legal especifica, não dependendo do consentimento ou enquadramento em outras hipóteses, exceto se mais especifica, como no caso de tutela à saúde (COTS; OLIVEIRA, 2019, p.145).

Ao contrário das instituições privadas, as públicas poderão ainda segui prazos e procedimentos das leis nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) (PINHEIRO, 2020, p.106).

Ressalte-se que a LGPD destacou em seus parágrafos 4º e 5º que terão o mesmo tratamento os serviços notariais, devendo fornecer a administração publica o acesso aos dados por meio eletrônico (BONFIM, 2019).

Já no artigo 24 da lei dividiu-se a matéria sobre empresas publicas e sociedade de economia mista, no caso de estas entidades atuarem em regime de concorrência com empresas privadas, deverão obedecer às mesmas obrigações incidentes sobre estas, sendo o contrário nos casos em que essas entidades publicas operacionalizarem politicas públicas e do âmbito da execução destas, deverão obedecer à disciplina estabelecida para órgãos públicos (COTS; OLIVEIRA, 2019, p.149).

Conforme o artigo 25 que estabeleceu regras especificas para o compartilhamento de dados pelo poder público, vedando este tipo de ação para as entidades públicas aos particulares, possuindo 4 exceções no parágrafo primeiro: I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei de Acesso à Informação; II – se o ente privado indicar um encarregado e restringir o tratamento realizado às instruções recebidas do controlador; III - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou IV - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades (COTS; OLIVEIRA, 2019, p.153).

O caput do artigo 27 determinou que a comunicação ou compartilhamento de dados entre as pessoas de direito público e privado necessitam de ser informados a autoridade nacional, conforme regulamentação da ANPD, além disso instituiu a obrigatoriedade do consentimento do titular para o devido compartilhamento e comunicação de dados pessoais. Entretanto o mesmo artigo determina exceções: I - nas hipóteses de dispensa de consentimento previstas na LGPD; II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 da LGPD; ou III - nas exceções constantes do § 1º do art. 26 da LGPD (COTS; OLIVEIRA, 2019, p.155).

Os órgãos públicos assim como os privados estão sujeitos a sanções, por conta disso, cabe a autoridade nacional garantir que sejam adotadas medidas cabíveis e também proporcionais para o cumprimento da lei (PINHEIRO, 2020).

A seção II do capítulo em que se trata sobre o tratamento de dados pelo poder público não aborda quaisquer responsabilidades civis ou penais, mas continua a descrever atribuições e prerrogativas a autoridade nacional, muito menos menciona vinculação com o artigo 52 que escabece sanções administrativas (COTS; OLIVEIRA, 2019, p.158).

Por fim, o artigo 31 da lei prevê que a autoridade nacional, no caso de infração da lei, enviar “informe com medidas cabíveis para fazer cessar a violação”, dependendo da boa-fé das ações governamentais corrigir procedimentos que violem a LGPD (COTS; OLIVEIRA, 2019, p.158).

5 RESPONSABILIDADES E RESSARCIMENTO DE DANOS

Hoje, os dados pessoais se tornaram um dos ativos mais importantes e podem, sem dúvida, ser considerados uma fonte de riqueza no século XXI. Nesse caso, existe uma realidade que precisa de atenção, pois todas as empresas realizam determinados tipos de operações sobre dados pessoais, seja na coleta, armazenamento, transmissão ou utilização, sendo isso, inerente à atividade empresarial. Portanto, a fim de trazer maior segurança ao titular nesta realidade em que vivemos, a LGPD trata sobre a responsabilidade dos controladores e operadores nos artigos 42 a 45 da seção III. (MOREIRA, 2020).

5.1 Responsabilidade Civil

A responsabilidade civil é tratada principalmente no artigo 42 da LGPD, discorrendo sobre a responsabilidades dos agentes de tratamento, isso é, controlador e operador. (COTS; OLIVEIRA, 2019, p.180).

O controlador é aquele que possui todos os poderes de tomada de decisão para o processamento de dados, e o operador executa as instruções fornecidas pelo primeiro, por meio de contratos de prestação de serviços, parcerias, sociedade, entre outros. (COTS; OLIVEIRA, 2019, p.180).

A LGPD tem por característica os seguintes elementos necessários para a responsabilização civil dos agentes de tratamento: i) realização do tratamento; ii) violação à legislação de proteção de dados pessoais; iii) nexo de causalidade e; iv) dano a outrem. (DRESCH, 2020).

Neste caso, a violação à legislação de proteção de dados pessoais (o elemento básico da responsabilidade civil dos agentes de processamento), pode ocorrer através ilícitos específicos, que se caracteriza por contradizer as responsabilidades de tratamento de dados previstas na lei. Mas também na forma de um ilícito geral, normalmente na forma do sistema de proteção. (DRESCH, 2020).

O ilícito geral na LGPD pode ser entendido como uma falta de disciplina jurídica semelhante ao “Código de Defesa do Consumidor” (CDC) para assumir a responsabilidade civil por obrigações de segurança em termos de fatos de serviço. No direito do consumidor, a responsabilidade geral pela segurança está baseada no elemento defeito, pois o produto ou serviço é considerado defeituoso, portanto,

quando o produto ou serviço não apresentar a segurança razoavelmente esperada, haverá a responsabilidade civil do fornecedor. (DRESCH, 2020).

A premissa do artigo 42 é que o controlador ou operador serão responsáveis pelos danos materiais ou morais, pessoais ou coletivos causados pela violação da LGPD. A utilização da palavra “ou” entre o controlador e o operador evidencia a ideia de que todos são responsáveis pelos seus atos e pelos danos causados e, geralmente, não existe responsabilidade solidária entre eles. (COTS; OLIVEIRA, 2019, p.180).

A responsabilidade civil dos agentes de tratamento segue as regras gerais estabelecidas nos artigos 186, 187 e 927 do Código Civil:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
>
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.
>
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. (BRASIL, 2002).

A causalidade do dano está intrinsecamente relacionada às violações de LGPD. Se não houver violação, o artigo 42 não se aplicará e as violações não serão consideradas ato ilícito. (COTS; OLIVEIRA, 2019, p.180).

Cots; Oliveira (2019, apud CAVALIERI FILHO, 2012), preconizou que o nexo causal é o "elemento referencial entre a conduta e o resultado. É através dele que poderemos concluir quem foi o causador do dano".

No entanto, a LGPD propõe duas premissas de responsabilidade solidária, na qual, o operador será responsável junto com o controlador, pelos danos causados. É possível visualizar isto no parágrafo 1º do artigo 42, a saber: (i) quando o operador violar a LGPD; (ii) quando o operador não seguiu as instruções de tratamento estabelecidas pelo controlador. Essas duas premissas não são cumulativas, embora na maioria dos casos, o não cumprimento das instruções afetará diretamente os princípios estabelecidos na LGPD, ou seja, indiretamente violarão a lei (por exemplo, o operador que diferentemente das instruções, compartilhou os dados pessoais em vez de apenas os armazenar, violou o principio da finalidade e adequação). (COTS; OLIVEIRA, 2019, p.181).

Sendo então a responsabilidade solidária, o credor poderá exigir a dívida toda de qualquer dos responsáveis, conforme artigo 264 do Código Civil:

> Art. 264. Há solidariedade, quando na mesma obrigação concorre mais de um credor, ou mais de um devedor, cada um com direito, ou obrigado, à dívida toda. (BRASIL, 2002).

De acordo com o inciso I, parágrafo 1º, o operador que não segue as instruções do controlador, significa que ele usurpou o poder de decisão do processamento de dados, assumindo assim a responsabilidade. (COTS; OLIVEIRA, 2019, p.181).

O primeiro pressuposto, destaca a importância da compreensão e aplicação da LGPD por parte do operador, e do ponto de vista do cumprimento da lei não se pode confiar no controlador para determinar o seu comportamento. Esse aspecto legal pode levantar as seguintes questões: Se as instruções do controlador violam o LGPD, o operador deve se recusar a cumprir? Sim, a menos que você deseje correr o risco junto com o controlador para o tratamento irregular. (COTS; OLIVEIRA, 2019, p.181).

A segunda suposição de responsabilidade solidaria do operador é devido ao não cumprimento das instruções do controlador sobre o processamento de dados, o que aumenta a relevância da precisão e exatidão de tais instruções, não permitindo a obscuridade ou dúvidas. (COTS; OLIVEIRA, 2019, p.181).

Portanto, a comunicação de instruções será um marco na relação jurídica entre o controlador e o operador no que diz respeito ao tratamento de dados pessoais. (COTS; OLIVEIRA, 2019, p.181).

Por fim, caso mais de um controlador pelo tratamento esteja envolvido no tratamento de dados, nos termos do artigo 934 e do seu §4º do Código Civil, ambos serão solidariamente responsáveis pelo reembolso dos dados, podendo haver ação de regresso entre os dois. (COTS; OLIVEIRA, 2019, p.182).

5.2 Exclusão da Responsabilidade Civil

Em seu artigo 43 a LGPD tratou sobre as hipóteses em que os agentes de tratamento (controlador e operador) não serão responsabilizados. (COTS; OLIVEIRA, 2019, p.184).

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
>
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
>
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (...)

A primeira hipótese trata sobre quando o agente não executou o processamento de dados atribuído a ele. Em outras palavras, o processamento de dados foi realizado, mas o réu não tem nada a ver com ele. (CAPANEMA, 2020). Isso é muito próximo da ilegitimidade passiva, LGPD vê isso como uma vantagem. Se não houve o tratamento, não há nexo causal. (COTS; OLIVEIRA, 2019, p.184).

A segunda hipótese exclui a responsabilidade no caso em que o agente realiza o processamento dos dados, mas “não houve violação à legislação de proteção de dados”. Aqui, o dano ocorreu por meio de ato ilícito. (CAPANEMA, 2020).

“Conforme artigo 42 da lei, só há responsabilização se houver descumprimento da LGPD que gere dano ao titular” (COTS; OLIVEIRA, 2019, p.184).

Por exemplo, a tomada de decisão automática baseada em padrões transparentes, informados (existentes em termos de uso) e sem viés, que negue um empréstimo para um consumidor em potencial. Este inciso prevê expressamente apenas as circunstâncias que não houve violação a proteção de dados. (CAPANEMA, 2020).

Já na terceira hipótese, ocorre quando, o dano é causado por culpa exclusiva do titular, de terceiro ou pela atuação conjunta do titular e do terceiro. (CAPANEMA, 2020).

> No entanto, ainda haverá alguns problemas, conforme disciplina CAPANEMA, 2020, imagine a situação em que houve a invasão da conta de e-mail de um usuário, com a destruição de todas as suas mensagens. Tal fato só ocorreu porque a senha utilizada pelo titular era fraca, com apenas quatro caracteres, e foi facilmente descoberta. Poder-se-ia aqui falar em culpa exclusiva do titular? Caberia aos agentes de tratamento verificar a segurança da senha criada pelo usuário e impedir o uso daquelas que fossem frágeis? Existe norma técnica estabelecendo essa obrigação?

5.3 Irregularidade no Tratamento e Ressarcimento de Danos

Para que o tratamento de dados esteja dentro da lei, precisa estar dentro das hipóteses do artigo 7º da LGPD, tratando-se, portanto, da necessidade de uma base legal para que isso ocorra.

No entanto, ainda que o enquadramento seja formulado com base jurídica, tendo em conta as circunstâncias relevantes, se o tratamento dos dados não proporcionar a segurança que o titular espera, o tratamento dos dados também será

considerado irregular. Entre eles, o rol exemplificativo do artigo 44, (i) o modo pelo qual é realizado; (ii) o resultado e os riscos que razoavelmente dele se esperam; (iii) as técnicas de tratamento de dados disponíveis à época em que foi realizado (COTS; OLIVEIRA, 2019, p.186).

Primeiramente, as considerações que se faz é sobre a expectativa de segurança que é criada para o titular pelo controlador. Atender a essa expectativa é essencial para o processamento regular dos dados (COTS; OLIVEIRA, 2019, p.186).

> Exemplos uteis que são dados por COTS e OLIVEIRA (2019, p. 186) é de quando o titular que abre conta bancária tem uma expectativa alta de segurança de seus dados pessoais. Se o faz na agência bancária ou por meio de aplicativo pode fazer essa expectativa variar, mas continua, em ambos os casos, sendo alta. Por outro lado, o titular que fornece dados pessoais, como seu nome e telefone, para participação em um sorteio realizado por um açougue de sua rua, tem uma expectativa de segurança completamente diferente daquela verificada no primeiro exemplo.

Um questionamento que os autores fazem é de que se o açougue deve usar todas as ferramentas técnicas normalmente contratada pelos bancos para coletar dados pessoais para o sorteio? E chegam à conclusão de que é obvio que não, e não se pode esperar que isso aconteça, ou seja, a relação entre o açougue e o titular não tem grandes expectativas quanto à segurança dos dados pessoais (COTS; OLIVEIRA, 2019, p.186).

Portanto, a expectativa deverá ser realizada sempre sobre circunstancias especificas, como em um caso concreto, usando conceito de que se espera do homem-médio em relação a determinado tratamento de seus dados (COTS; OLIVEIRA, 2019, p.186).

De outro modo, a lei pondera que as técnicas de tratamento disponíveis à época devem ser consideradas. Esta regra é importante, especialmente porque usa a palavra “disponíveis”, ao invés de “existentes", pois são coisas totalmente diferentes. Por exemplo, imagine que um sistema de segurança muito eficiente está sendo testado na Noruega, mas ainda não foi vendido em mercados fora do país. O sistema já existe, mas não pode ser usado por controladores brasileiros. Por outro lado, suponha que o sistema seja vendido no Brasil depois de algum tempo, mas o valor da licença é de US $ 50 milhões de dólares. Os escritores COTS e OLIVEIRA (2019, p. 186) questionam se isso faz com que o sistema esteja disponível para os controladores brasileiros? Chagando a conclusão de que não. O termo “disponíveis” deve levar em consideração a possibilidade de o controlador acessar determinado

sistema, e não o simples fato de o controlador existir ou ser vendido fora do padrão econômico sob análise (COTS; OLIVEIRA, 2019, p.186).

De acordo com a redação do artigo 44 da LGPD, há quem questione se os legisladores criaram um sistema diferente do sistema de responsabilidade civil adotado no artigo 42 da LGPD. Este problema é causado pelos fatos de que no artigo 44 da LGPD usa-se o termo "tratamento irregular" condicionando a responsabilidade civil em seu parágrafo único, à qualificação de irregularidade definidas no artigo 46 da LGPD. Neste artigo 46 é inserido o Capítulo 7, “Segurança e Boas Práticas”, onde são incluídas na seção I “Da Segurança e Sigilo de Dados”, que menciona medidas de segurança e boas práticas, que devem ser adotadas pelos agentes de tratamento para prevenir os danos decorrentes de incidentes de segurança (MULHOLLAND, 2020).

Diante disso, enquanto o artigo 42 da lei estipula a obrigação de indenização "em razão do exercício de atividade de tratamento de dados pessoais", o artigo 44 e seu parágrafo único estabelece a obrigação de indenização por tratamento irregular de dados pessoais, considerado a fonte deste o comportamento de "violação de segurança de dados". Nesta hipótese, aponta MULHOLLAND (2020), os legisladores parecem querer identificar situações lesivas especificamente causadas por incidentes de segurança, que por sua vez estão relacionados com os riscos inerentes ao desenvolvimento das atividades de processamento de dados, como vazamentos acidentais e invasões de sistemas e base de dados por terceiros autorizados. Nesta logica, esses riscos devem ser considerados como inerentes às atividades de tratamento de dados, portanto, em última análise, esses riscos devem ser considerados como pressupostos acidentais internos, que não podem eliminar a obrigação dos agentes de indenizar os danos causados pelos incidentes, concluindo, portanto, que tanto o artigo 42, quanto o 44 da Lei Geral de Proteção de Dados, aderiram ao fundamento da responsabilidade civil objetiva, exigindo, dos agentes de tratamento a obrigação de indenizar os danos causados aos titulares, retirando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador (MULHOLLAND, 2020).

Portanto, a Agência Nacional de Proteção de Dados desempenhará um papel de destaque na definição do nível de segurança diretamente, por meio do poder normativo do agente regulador ou indiretamente, delegando o poder de determinar os

padrões de segurança à autorregulação de vários departamentos do mercado (DRESCH, 2020).

Em se tratando de ressarcimento de danos, a Lei Geral de Proteção de Dados possui 6 (seis) tipos de sanções previstas, sendo elas: (1) Advertência; (2) Multa de até R$50.000.000,00 por infração; (3) Multa diária; (4) Divulgação da infração ao público; (5) Bloqueio dos dados pessoais relativos à infração; (6) Eliminação dos dados pessoais relativos à infração e para a aplicação efetiva, a ANPD, deverá analisar como por exemplo, o impacto do incidente e quais dados ele afeta; o motivo do tratamento de dados; o dano gerado e a proporção da gravidade, entre outros (GROCHWSI, 2020).

Em decorrência disto o Ministério Público do Distrito Federal propôs a primeira ação civil pública após a entrada em vigor da lei, contra uma empresa com sede em Belo Horizonte (MG). Em setembro de 2020 o MP ajuizou a ação, acusando a Infortexto de vender bancos de dados para envio de publicidade digital e mala direta (DEMARTINI, 2020).

De acordo com a ação movida, os 500 mil moradores de São Paulo (SP) faziam parte de uma enorme quantidade de dados que inclui milhões de pessoas de todo o Brasil. No entanto, o número citado na ação parece baixo: um pacote contendo apenas dados de cabeleireiros, esteticistas e demais profissionais de beleza de todo o país custa R$ 212,90 reais, enquanto escritório de contabilidade e contadores de São Paulo custava R$ 52,90 reais. No entanto, alguns usos específicos são mais caros por exemplo, um conjunto para envio de mensagens de texto de propaganda política custava R$ 462,90 reais (DEMARTINI, 2020).

A investigação ocorreu através da unidade Especial de Proteção de Dados e Inteligência Artificial do MP (Espec), concluindo que os bancos de dados eram vendidos livremente, como em um *marketplace* comum, onde compradores escolhiam os conjuntos e critérios com garantia de 95% de endereços reais, 65% dos telefones fixos e 50% dos e-mails (DEMARTINI, 2020).

A ação apontou que a Infortexto tratou indevidamente as informações pessoais que possuía, comercializou-as indiscriminadamente e prejudicou a intimidade e privacidade de seu titular (DEMARTINI, 2020).

Entretanto, por se encontrar com o *marketplace* fora do ar, o TJDFT julgou a ação sem mérito e sem interesse processual. O MP recorreu da decisão e utilizou o serviço *Wayback Machine*, que armazena cópias antigas do site da Internet, incluindo

screenshots, dados da URL do lembrete digital e informações do CNPJ da Infortexto para subsidiar o processo, encontra-se novamente aguardando decisão para prosseguir (proc. nº 0730600-90.2020.8.07.0001) (DEMARTINI, 2020).

Posto isso, em outubro de 2020 é possível observar a primeira empresa condenada por descumprir a LGPD.

O processo tratava sobre um cliente que havia adquirido um imóvel em novembro de 2018 e, posteriormente, começou a receber ligações indesejadas de instituições financeiras e empresas de decoração que prestam serviços relacionados à aquisição de imóveis. Na visão da juíza, da 13ª Vara Cível de São Paulo, a empresa Cyrela não só violou as regras da LGPD, como também violou os direitos do Código de Defesa do Consumidor e da própria Constituição. Na explicação da magistrada, a construtora violou normas como a honra e privacidade do reclamante, não só repassando seus dados pessoais, mas também revelando informações detalhadas sobre a compra do imóvel, violando assim sua privacidade (DEMARTINI, 2020).

Além da indenização efetiva de R$ 10.000 reais, a decisão também condenou a construtora por não mais ceder os dados pessoais ou financeiros de seus clientes a terceiros, cobrando 300 reais para cada contrato indevido cuja má utilização de informações seja confirmada, entretanto, a decisão ainda está sujeita a apelação (proc. nº 1080233-94.2019.8.26.0100) (DEMARTINI, 2020).

6 CONSIDERAÇÕES FINAIS

Em primeiro lugar, percebe-se que com o advento da internet o mundo em que conhecemos muda constantemente, assim, consequentemente, o mercado de valores. Ao observar quais as empresas se tornaram as mais valiosas do mundo, percebe-se que todas tem relação com o mundo digital.

Todas as empresas precisam vender o seu produto, seja ele ao consumidor final ou não, em decorrência disso, a fim de oferecer a cada vez mais pessoas, refina-se a busca do consumidor ideal ao seu produto e aí entra o dado pessoal, possibilitando as empresas a divulgarem aos seus públicos específicos e a terem um maior retorno, tornando os dados pessoais, o bem mais valioso para uma empresa.

Como resultado de tudo isso, vemos esses dados serem alvos de hackers e a criação de um comércio para a venda dos mesmos, em virtude da alta procura e rentabilidade.

Com o propósito de proteger esses dados e os direitos fundamentais dos indivíduos, começaram a surgir no Brasil e no mundo, leis para amparar a privacidade de cada um.

Destacando no primeiro capítulo deste trabalho o julgamento da Lei do Censo de População, Profissão, Moradia e Trabalho realizado pelo Tribunal Constitucional alemão em 25 de março de 1982, realçando a origem do direito a auto determinação afirmativa, tendo em vista que a referida lei previa a coleta de informações pessoais dos cidadãos para o Estado e no caso de recusa, ocasionaria multa ao cidadão.

Tal sentença criou um marco, reconhecendo o direito à auto determinação informativa, influenciando normas nacionais e europeias em sequência “a reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados” (MENDES, 2014, p. 31 apud GLITZ, 2019).

No Brasil a Constituição Federal de 1988 já previa o direito à privacidade como um direito fundamental disciplinado em seu artigo 5º, incisos X, XI e XII. Possibilitando ao indivíduo possuir o domínio do que se encontra consigo, como seu corpo, casa, pensamentos, propriedades, segredos e tudo relacionado a si, tendo a liberdade para escolher o que deseja permitir que outras pessoas tenham acesso (PONTICELLI, 2018).

Ademais, o Brasil, além da Constituição possui outras leis infraconstitucionais que também asseguram este direito aos indivíduos, como por exemplo o Código de Defesa do Consumidor em seu artigo 43, criando o banco de dados dos consumidores o direito destes em acessar estas informações, como também o Código Civil em seus artigos 11, 12, 16, 17 e 21, dando maior descrição aos direitos da personalidade, privacidade e a intimidade.

Posteriormente a algumas outras leis brasileiras que enfatizaram uma maior segurança ao indivíduo em relação a proteção de seus dados, o Brasil inspirado no regulamento europeu denominado *General Data Protection Regulation* ou GDPR, criou a Lei Geral de Proteção de Dados estudado no presente trabalho.

O Brasil assim como muitos outros sofreram o efeito dominó que a União Europeia ocasionou após começar a exigir que outros países e empresas que possuíam interesse em manter relações comerciais com os países da U.E. deveriam possuir uma legislação do mesmo nível que o GDPR e no caso do Estado que não possuísse lei de mesmo nível, passaria então a poder sofrer sanções econômicas ou dificuldade de fazer negócios e em decorrência disso a lei brasileira é praticamente

idêntica a GDPR, entretanto conforme PINHEIRO (2020, p. 21) A versão nacional por ser mais enxuta deixa margens para uma intepretação mais ampla, que poderá trazer alguns pontos de insegurança jurídica.

No segundo capitulo, observa-se a conceituação de dado pessoal, dados anonimizados e o processo de anonimização, o conceito e os tipos de tratamento e as suas hipóteses, sendo o principal o consentimento do titular.

O tratamento de dado sensível por exemplo é aquele que trata sobre origem racial ou étnica, convicção religiosa, opinião política, dado genético ou biométrico, ou seja, todo aquele que a pessoa possa ser discriminada.

Além disso, no tratamento de dados pessoais de crianças deverá ser realizado com o consentimento especifico de pelo menos um dos pais ou responsável legal, silenciando-se quanto aos dados dos adolescentes. Dessa maneira, o consentimento parental previsto na LGPD é indispensável apenas quando se tratar de menores de 12 anos, de forma que os demais teriam capacidade para dispor sobre seus dados (B. F. F. YANDRA, A. C. A. SILVA, J. G. SANTOS, 2020).

Já o termino do tratamento de dados ocorre quando verificado que a finalidade do tratamento foi alcançada, pelo fim do período de tratamento, a comunicação do titular revogando o consentimento e a determinação de autoridade nacional.

Os órgãos que fiscalizam a devida aplicação da lei no Brasil são o Ministério Público, PROCON, agências reguladoras, o próprio titular de dados e principalmente a Autoridade Nacional de Proteção de Dados, aplicação que posteriormente no quarto e último capitulo observamos as primeiras atividades da justiça brasileira e investigar, processar e condenar empresas que inadimpliram com as normas da LGPD.

No terceiro capitulo tratamos sobre o artigo 3º da lei e a abrangência da LGPD que garante que qualquer operação de tratamento realizada, independente do meio, do país sede ou país onde esteja localizado os dados serão atingidos pela lei, a mesma lógica prevista pelo Marco Civil da Internet (PINHEIRO, 2020, p.75).

De acordo com o marco civil, mesmo que o tratamento de dados tenha sido realizado por pessoa jurídica estrangeira, se o serviço foi ofertado aos brasileiros ou a integrante de grupo econômico com estabelecimento no Brasil, a legislação é aplicável (VIEIRA, 2019).

A LGPD inspirou-se no GDPR ao tratar sobre as transferências internacionais de dados pessoais defendendo que os países que pretendem fazer este tipo de

operação deverão conceder a garantia da proteção dos dados no mesmo nível que a LGPD protege (PINHEIRO, 2020, p.112).

Explanamos ainda neste capitulo que as pessoas jurídicas de direito público, assim como as privadas, devem apresentar para o tratamento de dados possuir uma finalidade clara e transparente, além de cumprir com os requisitos estabelecidos.

No quarto capítulo abordamos a responsabilidade civil do controlador e do operador de dados, sendo essa a objetiva e suas hipóteses de exclusão. Abordou-se ainda como dito anteriormente as irregularidades e os ressarcimentos destes danos em casos práticos.

De todo o exposto, conclui-se que com o advento da Lei Geral de Proteção de Dados o Brasil deu mais um passo rumo a efetiva proteção de dados e a privacidade de seus cidadãos, apesar de ainda estarmos no início na vigência da lei, observa-se que a mesma já se torna efetiva apesar de algumas lacunas.

7 REFERÊNCIAS

ALBRECHT, Lucas Cé. **O que crianças e adolescentes ganham com a nova lei?.** 2019. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/criancas-adolescentes-lgpd-lei-geral-protecao-de-dados-pessoais>. Acesso em: 15/03/2020.

BRASIL, **Lei nº 12.414, de 9 de junho de 2011**. Disciplina A Formação E Consulta A Bancos De Dados Com Informações De Adimplemento, De Pessoas Naturais Ou De Pessoas Jurídicas, Para Formação De Histórico De Crédito, Brasília, DF, 2011. Disponível Em: <Http://Www.Planalto.Gov.Br/Ccivil_03/_Ato2011-2014/2011/Lei/L12414.Htm>. Acesso Em:15/02/2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, Brasília, DF, abril 2014. Disponível em: < HTTP://WWW.PLANALTO.GOV.BR/CCIVIL_03/_ATO2011-2014/2014/LEI/L12965.HTM >. ACESSO EM: 15/03/2020.

BRASIL. **Constituição da república federativa do brasil de 1988**, Brasília, DF, 1988. Disponível em: HTTP://WWW.PLANALTO.GOV.BR/CCIVIL_03/CONSTITUICAO/CONSTITUICAO.HTM. Acesso em: 15/03/2020.

BRASIL, **Lei nº 10.406, DE 10 de janeiro de 2002**. Institui o código civil, Brasília, DF, 2002. Disponível em: <HTTP://WWW.PLANALTO.GOV.BR/CCIVIL_03/LEIS/2002/L10406COMPILADA.HTM>. Acesso Em: 16/03/2020.

BRASIL, **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o decreto-lei no 2.848, de 7 de dezembro de 1940 - código penal; e dá outras providências, Brasília, DF, 2012. Disponível em: <HTTP://WWW.PLANALTO.GOV.BR/CCIVIL_03/_ATO2011-2014/2012/LEI/L12737.HTM>. Acesso em: 16/03/2020.

BRASIL, **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil. Brasília, DF, 2014. Disponível em: <HTTP://WWW.PLANALTO.GOV.BR/CCIVIL_03/_ATO2011-2014/2014/LEI/L12965.HTM> Acesso Em: 16/03/2020.

BRASIL, **Lei nº 13.709, de 14 de agosto de 2018**. Lei geral de proteção de dados pessoais (LGPD), Brasília, DF, 2018. Disponível em: < HTTP://WWW.PLANALTO.GOV.BR/CCIVIL_03/_ATO2015-2018/2018/LEI/L13709.HTM>. Acesso Em:16/03/2020.

BRASIL, **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF, 1990. Disponível em: <HTTP://WWW.PLANALTO.GOV.BR/CCIVIL_03/LEIS/L8078.HTM>. Acesso Em: 16/03/2020.

B. F. F. YANDRA, A. C. A. SILVA, J. G. SANTOS. **Lei Geral De Proteção De Dados E A Tutela Dos Dados Pessoais De Crianças E Adolescentes: A Efetividade Do Consentimento Dos Pais Ou Responsáveis Legais**. Revista internet&sociedade, n.

1 ⁄ v. 1 ⁄ fevereiro de 2020 páginas 230 a 249. Disponível em:< https://revista.internetlab.org.br/lei-geral-de-protecao-de-dados-e-a-tutela-dos-dados-pessoais-de-criancas-e-adolescentes-a-efetividade-do-consentimento-dos-pais-ou-responsaveis-legais/>. acesso em: 17/03/2020.

CARVALHO, Gisele Primo. PEDRINI, Taina Fernanda. **Direito à privacidade na lei geral de proteção de dados pessoais.** *Revista da ESMESC.* Florianópolis, v. 26, n. 32 (2019). Disponível em <HTTPS://REVISTA.ESMESC.ORG.BR/RE/ARTICLE/VIEW/217>. Acesso Em 17/03/2020.

CARVALHO, Fellipe Freire De; SANTOS, Carlos Eduardo Lessa. **PRIVACIDADE E PROTEÇÃO DE DADOS NA ERA DO BIG DATA**. 2019. Trabalho de conclusão de curso apresentado ao curso de bacharelado em sistemas de informação da universidade federal fluminense como requisito parcial para conclusão do curso. Disponível em: < https://app.uff.br/riuff/handle/1/13054>. Acesso em: 17/03/2020.

CÂMARA DOS DEPUTADOS, Projeto De Lei Da Câmara N° 35, De 2012 (Lei Dos Crimes Cibernéticos / Carolina Dieckmann), Disponível Em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/105612>. Acesso Em:17/03/2020.

COMITÊ GESTOR DAINTERNET NO BRASIL (CGI.BR). **O cgi.br e o marco civil da internet**, março de 2013. Disponível em <https://www.cgi.br/publicacao/o-cgi-br-e-o-marco-civil-da-internet/91>. Acesso em: 24/10/2020.

CAPANEMA, Walter Aranha. **A Responsabilidade Civil na Lei Geral de Proteção de Dados,** 2020. Disponível em: <http://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em 24/10/2020.

Declaração Universal Dos Direitos Humanos. Assembleia geral das nações unidas em paris. 10 dez. 1948. Disponível em: <http://www.dudh.org.br/wpcontent/uploads/2014/12/dudh.pdf>. Acesso em 21/04/2020.

DEMARTINI, Felipe. **Cyrela é a 1ª empresa condenada por descumprir a LGPD e deve pagar R$ 10 mil,** 2020. Disponível em: https://canaltech.com.br/juridico/cyrela-e-a-1a-empresa-condenada-por-descumprir-a-lgpd-e-deve-pagar-r-10-mil-172465/#:~:text=A%20Cyrela%20%C3%A9%20a%20primeira,compartilhados%20com%20parceiros%20sem%20autoriza%C3%A7%C3%A3o. acesso em 29/10/2020.

DEMARTINI, Felipe. **Ministério Público abre primeira ação civil pública baseada na LGPD,** 2020. Disponível em: https://canaltech.com.br/legislacao/ministerio-publico-abre-primeira-acao-civil-publica-baseada-na-lgpd-171930/. Acesso em: 29/10/2020.

DRESCH, Rafael. **A especial Responsabilidade Civil na Lei Geral de Proteção de Dados,** 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados. Acesso em: 24/10/2020.

FRANZÃO, Ana. **Nova LGPD: tratamento dos dados de crianças e adolescentes,** 2018. Disponível em: <https://www.ab2l.org.br/nova-lgpd-tratamento-dos-dados-de-criancas-e-adolescentes/>. Acesso em: 24/10/2020.

GLITZ, Gabriela Pandolfo Coelho. **Da privacidade à proteção de dados pessoais: o caminho para uma lei geral de proteção de dados pessoais**. 2019. Trabalho apresentado como requisito de avaliação à disciplina direito privado e sociedade (mestrado em direito) - Pontifícia Universidade Católica Do Rio Grande Do Sul, (local), 2019.

GUGIK, Gabriel. **O que são cookies?.** 2008. Disponível em: <https://www.tecmundo.com.br/web/1069-o-que-sao-cookies-.htm>. Acesso em: 15/03/2020.

GROCHOWSKI, André Vieira. **Critérios para aplicação de multas e sanções previstas na LGPD,** 2020. Disponível em: https://www.portnet.com.br/criterios-para-aplicacao-de-multas-e-sancoes-previstas-na-lgpd/. Acesso em: 29/10/2020.

HOSTERT, Ana Cláudia. **Proteção de dados pessoais na internet: a necessidade de lei específica no ordenamento jurídico brasileiro**. Monografia apresentada à universidade federal de Santa Catarina para obtenção do título de bacharel em direito, Florianópolis – SC, 2018.

KATARIVAS, Nicole. **A lei do cadastro positivo e a lei geral de proteção de dados: conflito ou sinergia?.** 2019. Disponível em <https://www.migalhas.com.br/depeso/298656/a-lei-do-cadastro-positivo-e-a-lei-geral-de-protecao-de-dados-conflito-ou-sinergia>. Acesso em: 15/03/2020.

LOES, João. **Lei Carolina Dieckmann: apenas o primeiro passo**. 2016. Disponível em:<https://istoe.com.br/288575_lei+carolina+dieckmann+apenas+o+primeiro+passo/>. Acesso em: 16/03/2020.

LEAL, Lívia. **Proteção post mortem dos dados pessoais?**. 2019. Disponível em: <https://www.ab2l.org.br/protecao-post-mortem-dos-dados-pessoais/> acesso em 27/05/2020.

LIMA, Mariana. **A Autoridade Nacional De Proteção De Dados: o que você precisa saber sobre a ANPD**. 2020. Disponível em: https://triplait.com/anpd/. Acesso em: 17/09/2020.

MATOS, Tiago Farina. **comércio de dados pessoais, privacidade e internet.** *revista de doutrina da 4ª região* publicação da escola da magistratura do TRF da 4ª região - EMAGIS, n. 7, 18 jul. 2005.

MENDES, Cleyton. **Quem Vai Poder Fiscalizar A LGPD**. Disponível em: <https://www.youtube.com/watch?v=MYopbQx7Bw0&list=WL&index=24&t=0s>. Acesso em: 15/09/2020.

MOREIRA, Fernanda Monteiro. **A LGPD e a Responsabilidade das Empresas,** 2020. Disponível em: <https://olivre.com.br/a-lgpd-e-a-responsabilidade-das-empresas>. Acesso em: 24/10/2020.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18).** R. Dir. Gar. Fund., vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

PONTICELLI, Murilo Meneghel. **O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da lei geral de proteção de dados.** 2018. Monografia apresentada ao curso de direito da Universidade Do Sul De Santa Catarina como requisito parcial à obtenção do título de bacharel em direito. Tubarão, 2018.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD).** 2. Ed. São Paulo: saraiva educação, 2020. 152 p.
QUIRINO, Alberto Talma Catão. **Legados digitais e proteção de dados post mortem.** Disponível em: <https://www.migalhas.com.br/depeso/315790/legados-digitais-e-protecao-de-dados-post-mortem>. Acesso em 27/05/2020.

SANTINHO, Renato. **Glossário hacker: 20 termos para entender melhor o mundo do cibercrime.** 2019. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/glossario-hacker-20-termos-para-entender-melhor-o-mundo-do-cibercrime/87176>. Acesso em: 17/05/2020.

VARELLA, Luisa. **ANPD: entenda o órgão gestor da LGPD**. 2019. Disponível em: https://www.compugraf.com.br/anpd-entenda-o-orgao-gestor-da-lgpd/ Acesso em: 17/09/2020.

VIEIRA. Victor Rodrigues Nascimento. **Lei Geral De Proteção De Dados: Uma Análise Da Tutela Dos Dados Pessoais Em Casos De Transferência Internacional. 2019.** Monografia apresentada ao curso de direito da Universidade Federal de Uberlândia, como requisito parcial à obtenção do título de bacharel em direito. Uberlândia, 2019.

ZYGON. Digital. **GDPR x LGPD Whitepaper**. Disponível em: <https://zygon.digital/2019/04/11/gdpr-x-lgpd/>. Acesso em: 25 de abril de 2020.