CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A PROTEÇÃO DE DADOS PESSOAIS NA INTERNET NO BRASIL: REGIME JURIDICO E RESPONSABILIDADE DOS AGENTES SOB A ÓTICA DA LEI Nº 13.709 DE 14 DE AGOSTO DE 2018

Giovana Pizzato Bruno

Presidente Prudente/SP

2019

CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A PROTEÇÃO DE DADOS PESSOAIS NA INTERNET NO BRASIL: REGIME JURIDICO E RESPONSABILIDADE DOS AGENTES SOB A ÓTICA DA LEI Nº 13.709 DE 14 DE AGOSTO DE 2018

Giovana Pizzato Bruno

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação do Prof. Luis Fernando Nogueira.

Presidente Prudente/SP

2019

A PROTEÇÃO DE DADOS PESSOAIS NA INTERNET NO BRASIL: REGIME JURIDICO E RESPONSABILIDADE DOS AGENTES SOB A ÓTICA DA LEI Nº 13.709 DE 14 DE AGOSTO DE 2018

Trabalho de Monografia aprovado como requisito parcial para obtenção do Grau de Bacharel em Direito.

_____

Luís Fernando Nogueira

_____

Ana Carolina Greco Paes

_____

Wilton Boigues Corbalan Tebar

Presidente Prudente, 03 de novembro de 2019

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”

(Marthin Luther King)

AGRADECIMENTOS

E mais uma etapa da vida se conclui. Um período de 5 anos, que vale dizer, se passaram voando. Eu não seria a pessoa que vos escreve sem os aprendizados, convívios, aulas, puxões de orelha e conselhos que recebi durante esse tempo. Nada disso seria possível sem as pessoas que tanto me ajudaram.

Em breves palavras, agradeço a Deus, Ele que nunca me abandona, Ele que foi meu amparo e consolo em todos os meus dias difíceis nesta caminhada na faculdade, Ele que sempre me levantou quando eu não achava que era mais capaz, sem Ele não seria nada.

Agradeço, também, aos meus pais, Dileusa e Luis Henrique, e meus avós, por toda confiança, incentivo e dedicação ao longo do curso. Esse trabalho, assim como qualquer conquista, é consequência direta de seus esforços por todos esses anos, e de todo amor e carinho que depositaram em mim. Não foi nada fácil estar longe deles por todos esses anos, tanto pra mim, quanto pra eles, mas eu sei que os alegro em perceber que todo sofrimento da distancia, hoje valeu a pena.

Agradeço ao meu irmão, Luis Henrique, que, além de meu companheiro de vida, se tornou meu companheiro de faculdade. Não tenho palavras pra descrever o quanto é importante ter a presença dele no meu dia-a-dia.

Aos meus amigos, em especial meus amigos de caminha de faculdade, Andressa, Bianca, Vitor e Luiza, e a todos meus outros amigos que sempre acreditaram no meu potencial e me encorajaram, mesmo quando eu não acreditei em mim mesma, meu grande e eterno agradecimento.

Por fim, e não menos importante, agradeço a todos os professores da Toledo Prudente, por todo ensinamento passado, em especial ao meu orientador, professor Luis Fernando Nogueira, por me acompanhar nessa caminhada difícil, com paciência e motivação, não medindo esforços em sua assistência. Ainda agradeço ao professor Wilton Tebar e professora Ana Carolina Paes que, com tanto carinho, aceitaram o convite de compor a banca examinadora deste trabalho.

A todos vocês, meu imenso agradecimento, pois sem cada um descrito a cima, eu não conseguiria chegar aonde cheguei, e nem ser o que sou hoje.

RESUMO

O presente trabalho é dedicado ao estudo da proteção de dados pessoais no contexto tecnológico, analisando as principais legislações pertinentes à matéria, em especial a nova Lei do Brasil, conhecida como Lei de Proteção de Dados Pessoais. Para isso, é exposto o conceito amplo do que seria os dados pessoais protegidos em lei, sua vulnerabilidade no atual modelo societário, passando, então, pela análise de direitos fundamentais, como o da privacidade e o da informação, sob a ótica da proteção destes dados pessoais. Em seguida, faz-se uma análise de toda a evolução histórica envolvendo a proteção dos dados pessoais na internet, destacando as principais legislações, tanto na norma Europeia, quanto no Brasil. Por fim, o trabalho aborda a Lei nº 13.709 de 14 de Agosto de 2018, conhecida como Lei de Proteção de Dados Pessoais, trazendo suas novas previsões acerca do tratamento dos dados pessoais, e suas possíveis consequências para os agentes responsáveis por esse tratamento. Busca-se com este estudo traçar um panorama de como a evolução tecnológica, sob a ótica da divulgação de dados pessoais na internet, resultou na necessidade de elaboração de legislações para regular o tratamento destes, atuando em caráter protetivo diante de infração à privacidade e liberdade dos cidadãos.

Palavras-chave: LGPD. Proteção de Dados Pessoais. Responsabilidade Civil. Sociedade de Informação.

ABSTRACT

The present paper is dedicated to the study of protection of personal data in the technological context, analyzing as main pertinent legislations to the matter, in particular a new Law of Brazil, known as Law of Protection of Personal Data. For this, the broad concept of serious data protected by law, its vulnerability in the current social model is exposed, passing through the analysis of fundamental rights, such as privacy and information, from the perspective of data protection personal. It analyzes all the historical evolution involving the protection of personal data on the Internet, standing out as the main legislations, both in the European standard and in Brazil. Finally, the paper addresses Law n. 13,709, of August 14, 2018, known as the Personal Data Protection Act, brings its new considerations on the processing of personal data and its possible consequences for the agents involved in the processing. Look for this study to track a panorama of technological evolution, from the perspective of the disclosure of personal data on the Internet, resulting in the need to draft legislation for regular or regular treatment, acting in front protective characters of privacy violation and freedom of citizens.

Keywords: Protection of Personal Data. Information society. LGPD. Civil responsability.

SUMÁRIO

1 INTRODUÇÃO

A sociedade, a partir do século XX, vem sofrendo grades mudança nas formas de sua organização social. O atual modelo social, conhecida como contemporâneo, vive em uma era em que a computação eletrônica e a internet são suas principais ferramentas, marcado pelo protagonismo da propagação de informação pessoal nos meios de comunicação.

Nesse sentindo, pela alta revolução tecnológica e, consequentemente, a propagação de informação, criou-se uma sociedade no qual há um aumento diário na produção de dados pessoais, pelos próprios usuários, sendo estes sendo cada vez mais utilizados para as mais variadas atividades.

Em 2009, a comissária da União Europeia Meglena Kuneva falou a frase “dados pessoais são o novo petróleo da Internet e a nova moeda do mundo digital”. Essa afirmação destaca a importância dos dados pessoais na era digital, isto, pois, a sociedade contemporânea sofreu um processo de transformação, no qual a informação tornou-se insumo essencial para o desenvolvimento social, econômico e tecnológico (BRANCHER; BEPPU, 2019, p. 64).

Contudo, essa nova era não trouxe apenas vantagens, trouxe, também, alguns aspectos negativos, como a utilização dos dados pessoais dos indivíduos, com ou sem seu consentimento, no qual estes não possuem conhecimento da quantidade de informações que despejam na internet, e muito menos o que acontece posteriormente.

A manifesta crise na proteção de dados pessoais não é mais novidade no mundo contemporâneo, e do mesmo modo a relevância do problema.

Vem crescendo bastante a preocupação de juristas pela ampla disponibilização dos dados pessoais e informações, voluntariamente ou sem seu conhecimento, na rede mundial de computadores, aliada com o gradativo aumento da ameaça de graves lesões a direitos, como o da privacidade (SAUAIA, 2018, p. 01).

Não se pode esquecer que o direito e a sociedade estão intimamente ligados, sendo necessária uma adequação do primeiro à sociedade, para que se regule e possibilite a evolução e segurança do ser humano em todas as eras da sociedade (MIRANDA, 2018, p.13).

Desse modo, tornou-se inegável a necessidade de legislação a cerca do tema. Vale dizer que, a proteção dos direitos pessoais já era tratada como direito fundamental em diversas legislações. Na Europa, por exemplo, já está previsto no Regulamento Geral de Proteção de Dados Pessoais da União Europeia, Regulamento nº 2016/679. No Brasil, algumas leis, como, o Marco Civil da Internet, já possuíam algumas previsões, mas não era suficiente.

À medida que essa necessidade cresceu, diversos Projetos de Lei foram criados. Um deles deu origem à Lei Geral de Proteção de Dados, a Lei Federal nº 13.709/2018, que dispõe acerca do tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, com o objetivo de proteger os direitos fundamentais de privacidade e liberdade, como também o livre desenvolvimento da personalidade da pessoa natural.

Assim, o presente trabalho tem como escopo analisar a evolução social e tecnológica na era contemporânea sob a ótica do Direito, destacando as principais legislações que influenciaram diretamente o legislador brasileiro. Ademais, analisar-se-á a legislação hoje terminada no Brasil e sua efetiva tutela judicial dos conflitos entre direitos fundamentais. Tais questões serão levantadas por meio de revisão bibliográfica, doutrinária e legislativa da matéria.

2 DADOS PESSOAIS

Esse capítulo tem o precípuo objetivo de permitir a compreensão básica do que sejam os dados pessoais, quais suas espécies e por qual motivo se fez a necessidade de proteção maior a esses.

Ademais, pretende-se demonstrar que direitos, como, à privacidade e ao acesso à informação, são direitos fundamentais e garantidos à todo ser humano, e a problematização se enquadra em como ponderar essas suas diretrizes, quando houver conflito sob a ótica da proteção de dados pessoais.

Pode-se afirmar, por fim, que vivemos em um constante fornecimento de dados e conteúdos pessoais, fomentada por esta intensa revolução tecnológica, e que está permitindo que nessa sociedade de informação e líquida os sujeitos sejam constantemente monitorados, e, estejam ou não de boa-fé, vem trazendo sérios problemas quanto à garantia efetiva de direitos fundamentais, como o da privacidade, e à proteção dos dados expostos.

2.1 Conceituação

Dados pessoais são aquelas informações relativas a uma pessoa natural identificada ou, pelo menos, identificável, sendo considerado pessoa identificável aquela que consiga ser identificada, direta ou indiretamente, como, por exemplo, pelo nome, dados de localização, dados acadêmicos ou, até mesmo, por elementos de identificação física, genética, mental, social ou cultural da pessoa.

Nesse sentido, conforme entendimento de Catarina Castro (2005, p. 70), dado pessoal é “[...] qualquer informação (numérica, alfabética, gráfica, fotográfica, acústica), independentemente do suporte (som e imagem), referente a uma pessoa identificada ou identificável”.

Ressalta-se que, hoje em dia, são as redes sociais – especialmente o *Instagram* e *Facebook* – que predominam como plataformas coletoras de tais dados, e que por meio da conta do usuário, têm acesso livre a diversas informações, inserida em um banco de dados. Tal banco de dados compreende informações sobre o nome, e-mail, idade, e todas as fotos no perfil deste.

Antes de aprofundarmos em seu conceito, cabe, em um primeiro momento, saber que há uma grande diferente entre “dado”, que é todo e qualquer tipo informação, e “dados pessoais”, já conceituados a cima.

Segundo Ana Helena Fragomeni (1986, p. 161), considera-se que dado são os “elementos básicos passiveis de serem expressos como uma determinada combinação de sinais que têm significado através de um código, e que, estruturados, podem conter informação”.

Quer dizer, então, que dado propriamente dito, são atos que necessitam de interpretação antes de adquirirem algum sentido específico, servindo como uma pré-informação, no qual é desprovido de significação imediata, sendo até perceptível, porem de baixo valor semântico, até que algo o defina, dando origem a significações mais complexas.

À vista disso, consoante ao regulamento mencionado à cima – GDPR –, este não regula o dado propriamente dito, mas tão somente os “dados pessoais”, significando que, obrigatoriamente, além dos dados servirem pra prestar informações, devem estar intrinsecamente vinculados a uma pessoa natural, identificada ou identificável.

Os dados pessoais podem ser classificados e dentre outros destacam-se os chamados dados biométricos, dados sensíveis e dados anônimos.

Por dados biométricos compreende-se, em primeiro momento, nos termos da normatização a Lei Europeia de Proteção de Dados Pessoais, em seu artigo 4º (14), que são aqueles dados:

> Resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

Nesse contexto, esses dados contêm características únicas de cada pessoa, como, por exemplo, a sua impressão digital ou reconhecimento facial, sendo estes não variáveis com o tempo e sempre acessíveis. Por consequência, permitem a identificação do sujeito.

Conforme mencionado, outro dado pessoal é os dados sensíveis, também chamados de dados especiais, e podem ser encontrados na GDPR

(*General Data Protection Regulation)*, não a sua definição propriamente dita, mas uma referencia, em seu nº 51:

> Merecem proteção específica os **dados pessoais** que sejam, pela sua natureza, **especialmente sensíveis** do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão **incluir-se neste caso** os dados pessoais que revelem **a origem racial ou étnica**, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. [...] (grifou-se)

O fragmento do texto normativo acima mencionado, indicam uma conceituação indireta, decorrente de caráter apenas exemplificativo. Nesse sentido tais dados poderão ser considerados como sensíveis, pois, também o são considerados:

> Aqueles referentes à origem racial ou étnica, às opiniões políticas, as convicções religiosas ou filosóficas, à filiação sindical ou associativa, bem como os relativos à saúde ou sexualidade (LIMBERG, 2007, p. 203).

Nesse sentido, pelo entendimento de Laura Schertel Mendes (2014, p. 74), extrai-se que a particularização de alguns dados conferida pela lei se fez pela necessidade de proteção maior a esses, pois a categoria que os dados sensíveis se enquadram está diretamente relacionada à percepção de que o armazenamento e a circulação destes podem gerar um alto risco de exposição, ferindo diretamente os direitos fundamentais do individuo, especialmente se utilizados com intuito discriminatório.

Ressalta-se que essa classificação especial – dados sensíveis – compreende também os dados biométricos.

Por fim, dados anônimos são, conforme ensina Leandro Alvarenga Miranda (2018, p.131), “as informações que não digam respeito a uma pessoa singular identificada ou identificável, nem a dados pessoais tornados a tal modo anônimo, que o seu titular não seja ou não possa ser identificado”.

Pelo Regulamento 2016/679 da União Europeia, os dados anônimos são considerados opostos ao que os dados pessoais produzem, sendo estes os dados que se referem a pessoas que não podem ser identificadas. Isto é,

considera-se um dado anônimo aquele que, mesmo que seja referente a uma pessoa, não permite a identificação de seu titular.

O fenômeno da anonimização dos dados se torna um meio eficaz para o tratamento dos dados sensíveis, aqueles que têm o condão de identificar diretamente o titular, não os expondo e mantendo a segurança desses dados na Internet. Para que isso aconteça, será necessário, sempre que possível, eliminar os elementos identificadores, exibindo apenas as iniciais dos nomes ou até mesmo não divulgar a idade exata dos titulares, como exemplo, garantido maior proteção ao titular (BIONI, 2015, p. 25).

À vista disto, valendo-se dos conceitos grafados a cima, para os dados serem qualificados como anônimos, devem ser livres de qualquer informação de identificação, os quais torna impossível particularizar o titular.

Desse modo, esgotados os estudos acerca da definição genérica de dados pessoais, passa-se a discorrer neste trabalho a respeito da modernidade líquida e sociedade de informação, e, por conseguinte, acerca da vulnerabilidade dos dados pessoais inseridos nesta sociedade, porquanto o uso e a interpretação do significado desses dados se dão em um contexto diluído da privacidade em grande parte por conta do alto uso das redes sociais.

2.2 A Modernidade Líquida e a Sociedade de Informação

O uso da tecnologia na sociedade do século XXI reforça o enquadramento dos fenômenos sociais que caracterizam uma geração de pessoas que nascem em um contexto digital. A forma como as pessoas se relacionam, como interagem, como contratam, como vendem e compram, como realizam-se em seus projetos de vida está intimamente ligado ao uso da tecnologia e da informação.

A viragem para o novo milênio foi marcada por grande alteração paradigmática e os efeitos da globalização aceleraram e potencializaram diferentes mudanças nos comportamentos das pessoas. No início do ano 2000 as pessoas nem sequer utilizavam seus celulares para tirar fotos ou interagirem por meio de compartilhamento instantâneo dessas imagens. A internet não discada (de banda larga) dava seus primeiros passos.

Em que pese tal cenário, uma coisa é passível de observação. A tecnologia avançou de forma exponencial, isto é, a tecnologia do século XXI não respeita os passos lineares que eram dados nos séculos passados, mas de forma previamente programada se sustentam nos passos largos de uma progressão geométrica que dobra sua velocidade a cada passo dado.

Em termos de Direitos Fundamentais o cenário apresentado revela uma síndrome de inefetividade estatal que não consegue acompanhar o frenético avanço provocado pelo uso das novas tecnologias (inteligência artificial, por exemplo).

Na sociedade atual, tem-se a autodeterminação como coercitiva e obrigatória, isto é, os direitos democráticos e suas liberdades são garantidos na teoria, porem inalcançáveis na prática.

Para exemplificar, o filósofo francês Jean-Paul Sartre (1986, p. 39) um direcionamento quanto à liberdade como direito fundamental, fazendo um paralelo entre a liberdade e a sua alienação, firmando que:

> Acho que, por ora, o homem é livre para ser alienado. Alienação e liberdade não são, em absoluto, conceitos contraditórios. Muito pelo contrario: se não fosses livres como poderia transformar-te em escravo? Não se escraviza um pedregulho ou uma maquina: só se escraviza e se aliena a um homem que, primeiramente, é livre: não há alienação a não ser de um homem livre.

O que o autor aqui explicita é o fato de que, pela alta revolução tecnológica e, consequentemente, dos meios de comunicação, está presenciando uma realidade no qual há um aumento diário na produção de dados pessoais, pelo próprio ser humano, e a captação destes por quem quer tenha interesse, tornando a todos colaboradores e sujeitos desse processo de apropriação de conteúdo informacional.

É importante enfatizar que nesse mundo líquido, isto é, conforme ensina o sociólogo e filósofo polonês Zygmunt Bauman (2000, p. 48), o qual tudo vem se tornando maleável e incerto, isto é, tudo poderá ser feito, e o que quer que aconteça, provavelmente chegará sem anunciar-se e fluirá sem prévio aviso.

Por essa razão, na realidade contemporânea, o que mais se encontra são novas oportunidades e possibilidades, como quando ele exemplifica com o uso da metáfora de uma mesa de bufê, no qual há diversos

pratos, porém ninguém é capaz provar todos. Ainda assim, tentam encher seus pratos com o máximo de opções, por mais que, em algum momento, abandone parte delas, entrando em constância duvida se optaram pela escolha certa ou não em suas escolhas. Por essa ótica, infelicidade, hoje, segundo ensina, está atrelada ao excesso de escolhas que devemos fazer, e não pela falta de opção.

De acordo com a autora Anna Lucia King (2014, p. 34), devemos ter a compreensão de como esta sendo a formação do sujeito, enquanto membro desta sociedade de informação, na comunidade global, porquanto há de se convir que o “mundo virtual é um mundo de deslumbramento e as redes sociais são palcos para que possamos nos apresentar para uma plateia de espectadores assíduos por atender à necessidade de compartilhamento”.

Seguindo o mesmo raciocínio, alerta ainda, para os supostos efeitos da exposição mútua a esses meios virtuais (*digital)*, e assim:

> temos o dever de orientar e esclarecer a sociedade e as pessoas menos preparadas sobre a cultura da fantasia virtual, para que ela não seja privilegiada em detrimento do aprendizado dos valores reais” (KING, 2014, p. 34).

Como afirmado, vivemos em uma modernidade líquida, ou pós-modernidade, onde há extrema necessidade de autoexposição, no qual o ser humano se tornou dependente em permanecer vinculado aos meios digitais, principalmente pela Internet, no qual, consequentemente e involuntariamente, estão disponibilizando uma quantidade massiva de dados pessoais (SAUAIA, 2018, p. 27).

Para Tatiana Malta Viena (2007, p. 156):

> [...] a expressão sociedade de informação define uma nova forma de organização social, política e econômica que recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações.

No mesmo sentido, Leandro Miranda (2018, p. 50) denomina nossa atual Sociedade de Informação sendo aquela que “tem como principal característica a valorização do conhecimento e da informação, em especial daqueles adquiridos com a coleta e tratamento de dados”.

Urge ressaltar que nessa realidade, o grande papel da Internet, principalmente com suas redes sociais, é servir com modelo perfeito para a vida cotidiana, seja a exposição verídica ou não, no todo conteúdo publicado dos meios digitais estão à disposição dos internautas vinte e quatro horas por dia.

Tão grandiosa esta sendo a revolução social e digital na nossa sociedade, que o que era apenas um meio de disponibilização de dados impessoais, vem se tornando um grande armazenador de dados pessoais, servido com um cérebro global que capta e transmite nossas relações, nossas intenções e nossas vontades.

Como pontua Hugo Sauaia (2018, p. 20), há uma potencialidade de alcance das informações que é alcançada inconscientemente porque os:

> Dossiês sobre o individuo não estão mais em gavetas de algum órgão, ele são autobiográficos, postados para o mundo inteiro, quando, muitas vezes, sequer a intenção era promover divulgação tão ampla daquela informação da vida.

Tendo em vista tais fatores, mormente da ausência de barreiras, ou de controle severo quanto ao fluxo de dados pessoais, é que se consolida uma nova era de pós-modernismo, nos quais tais dados aparecem com o bem mais valioso e procurado.

É neste cenário que se pretende discutir o tema central da presente monografia, porquanto o estudo da lei de proteção de dados no Brasil (e em outros países) não pode estar desgarrada dessa visão em que os dados pessoais, muitas vezes sensíveis e biométricos, identificam o sujeito e por causa da sua dependência tecnológica se aproveitam da utilização do alto índice de exposição a que as pessoas se submetem nessa sociedade líquida.

2.3 A Vulnerabilidade dos Dados Pessoais da Sociedade de Informação

Diante do alto tráfego de dados pessoais a sua vulnerabilidade é sintomática e, assim, abra-se margem para discussões quanto à necessidade de sua proteção.

Tem-se como principal resultado da Internet e dos outros meios de navegação, a globalização e uma profunda mudança da vida em sociedade. Os

próprios cidadãos tiveram que se ajustar à nova realidade, no qual precisam se atentar aos dados que disponibilizam, associando ao grande aumento do numero de mecanismos aptos a capturar, com ou sem o seu consentimento, toda espécie de dados pessoais.

Nesse sentido, ressalta Hugo Moreira Sauaia (2018, p. 44):

> Os avanços tecnológicos têm permitido ainda o desenvolvimento de tecnologias das mais diversas, que permitem à rápida e massiva captação de imagens pessoais, gerando grave incerteza quanto a seus fins e utilizações [...].

Um dos pontos principais a ser discutido e apresentado é o fato de que, apesar de haver pesquisas demonstrando preocupação publica sobre a eventual deturpação da privacidade do individuo, são tímidas – de certa forma – as atitudes são tomadas a respeito. A contradição desse comportamento se encontra na baixa capacidade de conhecimento dos riscos de compartilhamento de dados simplórios, ou, igualmente, quando consumidores na internet aceitam fornecer seus dados pessoais, por modelos persuasivos de convencimento, mesmo que estes valorizem sua privacidade.

Sendo assim, conclui Hugo Sauaia (2018, p. 37), a respeito da contradição comportamental e seu efeito:

> Sendo assim, ainda que disponível o completo acesso a avaliações quanto aos riscos de violação à privacidade,e meios de proteção, esses dados muito possíveis não serão adequadamente utilizados.

No mesmo sentido, o autor Richard Warner (2011, p. 1084) afirma que, mesmo que seja disponível clausulas de privacidade em contratos ou políticas de privacidade, a maioria massiva dos consumidores não gasta seu tempo os lendo, pois, para compreensão da leitura, requer que tenha um mínimo de conhecimento sobre as informações que estão conditas nesses avisos de privacidade, não sendo este o caso da maioria dos consumidores.

Prosseguindo nesse contexto, a captação e o processamento de informações ocorrem por meio do denominado “mineração de dados”, nada mais sendo uma atividade para descobrir informações relevantes, fundado em um grande armazenamento de dados, tornando possível à disponibilização de enormes

quantias de dados em meio digital. Isto é, essa mineração de dados é um procedimento para identificação e captação de padrões em dados pessoais disponíveis dos indivíduos, com ou sem seu consentimento (SAUAIA, 2018, p. 41).

Para exemplificar, quando se navega sites como o *Facebook,* logo após realizar seu *login* na pagina, surgem, a todo o momento, propagandas sobre o ultimo produto que foi pesquisado na Internet. Isto, pois, a mineração de dados, explicados acima, capta dados pessoais e analisa as informações do individuo, permitindo essa interação, com intuito de ampliar o consumo.

Ainda, há exemplo da utilização do mecanismo de mineração de dados em conjunto com estratégias comerciais de discriminação de preços. Isto é, são oferecidos, pelo produto, diferentes preços, a certos indivíduos, de acordo com seu perfil, aptidão para consumo do referido produto.

Acerca desse contexto de ausência de proteção dos dados pessoais, atrela-se o alerta em “proteger” o titular dos dados, isto, pois, diante da vulnerabilidade dos dados pessoais em relação aos responsáveis pelo tratamento deste, e assim fica claramente caracterizada uma relação de hipossuficiência. Ensina Limberger (2007, p. 140-141):

> Diante das novas tecnologias da informática, a intimidade adquire outro conteúdo: visa-se a resguardar o cidadão com relacao aos dados informatizados. Um arquivo informatizado pode guardar um numero quase ilimitado de informações. Assim, o individuo que confia seus dados deve contar com a tutela jurídica para que estes sejam utilizados corretamente. [...] Pretende-se evitar, outrossim, que o cidadão seja transformado em números, tratado como se fosse uma mercadoria.

À luz desses estudos, resta claro que as facilidades tecnológicas e os novos meios de comunicação e a ideologia de “propiciar o fluxo de informações e permitir o compartilhamento do conhecimento” ultrapassa essa concepção idealista e, diante do monopólio de capacidade técnica dos responsáveis pela guarda dos dados fornecidos, em conjunto com os interesses em jogo, nos leva para a noção de que não há equilíbrio entre os interesses dos usuários e os demais atores nessa relação.

Em breve e conclusiva síntese, diante do poder sobre o paradeiro, nesta sociedade de informação, pelos responsáveis ao tratamento dos dados que a eles são fornecidos, no qual o individuo sequer é resguardado de mínimos filtros em

relação a lesão de seus direitos com a divulgação de seus dados, é que se proclama uma proteção efetiva à esses dados, protegendo, principalmente, sua dignidade e sua privacidade.

2.4 Do Direito Fundamental à Privacidade e o Conflito com o Direito à Informação sob a Ótica da Proteção de Dados Pessoais

O legislador constituinte, ao preocupar-se em reconhecer, no texto constitucional, uma maior gama possível de direitos fundamentais, incluiu em seu artigo 1º, a proteção da dignidade da pessoa humana, na qual se encontra inserido tanto o direito à informação, quanto o direito à privacidade do cidadão.

Cabe, em um primeiro momento, dizer que o direito à privacidade, que se encontra inserido entre os principais direitos fundamentais, tem como fundamento "[...] o direito de todo indivíduo de ser respeitado como pessoa e não ser prejudicado na sua existência e em sua dignidade" (DELPECH, 2004, p. 279).

Por outro lado, conceitua o autor Leandro Miranda (2018, p. 44) que o direito de informação é tão fundamental quanto qualquer outro para o próprio cidadão e a sociedade, e deverá ser contemplado e protegido, pois "a informação é uma ferramenta essencial para proteção de um país e para a inserção de um individuo em uma sociedade e formação de sua própria personalidade".

Diante disso, não restam hesitações quanto o direito à informação e o direito à privacidade serem reconhecidos como direitos fundamentais de todo e qualquer cidadão.

Sob a ótica do avanço tecnológico em está se vivendo, sabe-se que informações contidas nos dados pessoais estão cada vez mais acessíveis e, com base na vida cotidiana deste século, é certo que a maioria da população que possui acesso à internet está exposta quanto aos seus dados, que de alguma forma foram disponibilizados neste meio, e adquire informações sobre outras pessoas.

Observa-se, entretanto, que o ponto crucial que causa turbulência é que, com a nossa realidade atual de coleta e o tratamento dos dados pessoais, a velocidade e a quantidade então fazendo com que abusos e excessos estejam presentes.

Nesse sentido, explica Leandro Miranda (2018, p. 49)**:**

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

Importante realçar que, com a formação de bancos de dados pessoais, estas possuem um papel importantíssimo tanto para o desenvolvimento do ser humano em uma sociedade, quanto para o viés comercial e político.

Todavia, por deterem um poder em atingir intimamente a vida do individuo, deverá ser tratado de maneira onde haja uma cautelosa responsabilidade social dos agentes responsáveis.

Visto isso, entende-se que, para a utilização correta e devida das informações advindas de dados pessoais, o autor Leandro Miranda (2018, p. 46) leciona que:

> Por isso, sua atuação deve-se restringir ao objetivo para que foi criado, ou seja, que não haja qualquer desvio de finalidade da informação que foi coletada e tratada, a qual somente poderá ser transmitida, ainda que de forma onerosa, atendendo os preceitos legais para a qual foi coletada, sendo evidenciado o legítimo interesse.

Há um crescente ponto de convergência e contrariedade paradoxais entre o público e o privado. De qualquer forma, faz-se necessário, então, um efetivo combate à intromissão social na vida particular, onde apenas será resguardado o legitimo interesse social e legal para a coleta e transmissão das informações presentes nos dados pessoais disponíveis.

No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

A Constituição Brasileira contempla o problema da informação inicialmente por meio das garantias à liberdade de expressão e do direito à

informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade.

Além disso, a Constituição considera invioláveis a vida privada e a intimidade (art. 5º, X), veja-se especificamente a interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de habeas data (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais.

De suma importância entender o que leciona o Ministro do Supremo Tribunal Federal, Luis Roberto Barroso (Revista da EMERJ, v.6, n.23, 2003) que nenhum dos princípios constitucionais encontra-se imune a limitação, incluindo o direito à privacidade e o direito à informação, afirmando, este, a necessidade, então, de estipular alguns padrões de analise, incluindo o da existência real de interesse público.

Afirmar o equilíbrio entre esses direitos faz com que nenhum seja equivalente perante o outro, consagrando-se a técnica de ponderação como a maneira mais adequada para resolução de conflitos que haja entre princípios. Tartuce (2019, p. 167), assim, define a ponderação como sendo:

> A aplicação da ponderação nada mais é do que a solução do caso concreto de acordo com a máxima da proporcionalidade. [...] a pesagem deve ser fundamentada, calcada em uma argumentação jurídica com solidez e objetividade, para não ser arbitrária e irracional. Para tanto, deve ser bem clara e definida a fundamentação de enunciados de preferências em relação a determinado valor constitucional.

Após as referidas observações, fica certo que, tratando de direitos fundamentais à privacidade e à informação, deverá sempre realizar uma proporcionalidade entre ambos, no qual evite a intromissão nas informações que não sejam do interesse social, ou que possam ocasionar algum prejuízo ao próprio titular, preservando, desta maneira, a vida e a intimidade privada de cada sujeito.

O cidadão, certamente, é a vítima mais contumaz das violações de direitos ocorridas por meio da Internet, principalmente no que tange aos direitos à privacidade, porque, até sem ter ciência, suas informações podem ser coletadas, repassadas e comercializadas.

Sendo assim, tendo em vista os grandes impactos trazidos pelas novas tecnologias, no qual facilitaram a coleta e o armazenamento de dados pessoais,

tem-se que uma legislação que regulamente o tratamento de dados e proteja o cidadão é imprescindível, principalmente porque dirão respeito a direitos garantidos na Constituição, quando a proteção da privacidade vier em confronto com o direito à informação.

3 PROTEÇÃO DE DADOS PESSOAIS: EVOLUÇÃO LEGISLATIVA E O DIREITO COMPARADO

A rede mundial de computadores tornou-se o principal meio de cambio de informações da atualidade por meio de dados pessoais e, apesar de ter propiciado inúmeros avanços benéficos para a nossa sociedade, situações de ameaça aos usuários surgiram, sendo assim, passou a ser indispensável uma regulamentação.

Sendo assim, o presente capítulo tem como escopo uma compreensão melhor da proteção normativa dos dados pessoais. Para isso, serão analisados, de antemão, como que surgiu a Internet e, consequentemente, a dissipação de dados pessoais nesta.

Em um segundo momento, serão analisados as normas de proteção de dados pessoais, verificando, no ordenamento brasileiro, o que tange à construção legal da proteção de dados pessoais, analisando se é oferecida proteção suficiente aos dados pessoais em nosso país.

Por fim, será estudada especificamente a concentração das normas de proteção dos dados pessoais dos titulares dadas pela regulamentação da União Europeia.

3.1 Evolução Histórica dos Dados Pessoais na Internet

A evolução da tecnologia e consequente multiplicação de mecanismos automatizados para tratamento de informações estimularam um aumento significativo no fluxo de dados na atual sociedade (SCHREIBER, 2014, p. 137).

Constata-se, assim, que nada em nossa história evoluiu tanto quanto a tecnologia, em um espaço tão curto de tempo. É a partir do século XX que contamos com as grandes mudanças.

O surgimento da internet veio na década de 60, no qual nos mostra que a transmissão de informações não é tão recente, e que a Era da Informação – fase histórica posterior à segunda guerra mundial, desde já nos propiciou a pesquisa de diversas tecnologias e aparatos que aumentaram a mecanização em diferentes áreas da sociedade, inclusive com grande ênfase nos dados pessoais.

Seguindo a mesma evolução tecnológica do século XX, o autor Hugo Sauaia (2018, p. 93) pontua que:

> [...] o desenvolvimento tecnológico rápido, nas décadas de 60 e 70, trouxeram as primeiras preocupações sobre o armazenamento e a utilização desses dados, à medida que computadores passariam a ser usado por indivíduos, em todo mundo, com a capacidade de armazenamento fácil, rápido e amplo de informações, algo nunca antes testemunhado pela humanidade.

Por sua vez, o autor Leandro Miranda (2018, p. 87) entende que:

> A evolução tecnológica vem efetivando a combinação de diversas técnicas automatizadas, as quais permitem a captação de um grande número de dados de diversas pessoas simultaneamente, facilitada pela rede mundial de computadores.

Desse modo, pela primeira vez na história, a capacidade de reunir e analisar dados e informações de forma fácil e rápida se tornaram viável, mas, com isso, surgiam novas situações que poderiam colocar seus usuários em prejuízo, fazendo com que, assim, inúmeros Estados começassem a se mobilizar para regula-las.

Por muito tempo a controvérsia se baseou em como poderia ter uma regulamentação, dentro de espaço virtual que vai além dos limites territoriais do Estado, vigorando a ideia, por muito tempo, de que seria impossível esse tipo de regulamentação dar certo.

A autora Ana Cristina de Azevedo (2014, p. 91), em seu livro “Marco Civil da Internet no Brasil”, então, nos explicou que:

> No Brasil, a discussão envolvia ‘se’ e ‘como’ o espaço virtual devia ser regulado e, nesse sentido, como a utilização da rede surgiu antes de qualquer previsão legal e rapidamente se expandiu e ocupou lugar de destaque no mundo, a primeira providencia para suprir a lacuna jurídica foi lançar mão da analogia, com o uso de velhas regras criadas tendo em vista outras situações, quando possível encontrar alguma semelhança entre as duas realidades, a prevista na lei e a ocorrente na telemática.

À vista disso, embora o Brasil só tenha aprovado uma lei especifica para a proteção de dados ano passado, não nos é permitido dizer que o ordenamento jurídico nacional, até então, era silente a respeito do tema (BRANCHER; BEPPU, 2019, p. 23).

A Constituição Federal de 1988 trouxe, em seus artigos, como direito fundamental inviolável, a intimidade, a vida privada, a honra e a imagem dos individuo. E, para Laura Mendes (2014, p. 171), do art. 5º, X da Constituição, foi possível:

> [...] extrair uma tutela ampla da personalidade e da vida privada do cidadão, nas mais diversas situações em que ele se encontra. Não faria sentindo excluir exatamente as situações em que a sua vida privada está sujeita a uma maior violação, como é o caso do processamento de dados pessoais. Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e à vida privada do homem médio do que os perigos "tradicionais", [...]. Assim, não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos.

Seguindo na mesma linha da autora acima citada, constata-se que a Constituição Federal deverá sempre abrir suas possibilidades de interpretação, isto é, se fazer viável localizar em seus dispositivos algum regulamento sobre a proteção de dados, mesmo em esta foi elaborada anteriormente às grandes mudanças tecnológicas.

Posto isso, pode-se confirmar que a Constituição Federal de 1988 dá inicio às diretrizes das futuras leis de proteção de dados no Brasil, mas não apenas. Ou seja, não havendo uma legislação específica sobre o tema, como já dito, ocasionou o dever de se fazer uma ampla interpretação dos dispositivos espalhados tanto na Constituição Federal, mas também em legislações infraconstitucionais, como o Código Civil e do Consumidor, com o propósito de sempre ser preservada a privacidade e a personalidade do indivíduo.

Desde então, o Brasil busca aprovar uma Lei de proteção de dados pessoais, haja vista que há diversos problemas que poderão ser ocasionados pela transmissão indevida de dados, em especial pela internet, e que, por isso, precisam de soluções, tendo em vista a ausência de fronteiras definidas (MIRANDA, 2018, p. 89).

No contexto, Vinicius Fortes (2016, p. 12), estudioso do tema, demonstrou que a carência de uma legislação sobre o assunto faz com que as situações específicas relacionadas à proteção de dados fiquem a "mercê da

consciência jurisdicional” de cada juiz, causando uma insegurança jurídica e não alcança uma resposta uniforme e adequada aos problemas.

Para mais, é notório que a carência de uma regulamentação específica deixa o país em uma insegurança jurídica, em que desde a garantia dos direitos de seus cidadãos, até mesmo os acordos internacionais, são prejudicados pela sua inexistência.

3.2 A Proteção de Dados Pessoais no Brasil: Marco Civil da Internet

Mesmo a internet tendo começado a ser operada no Brasil nos anos 90, parte de sua regulamentação apenas surgiu só em 2014, com o Marco Civil da Internet, nome popular da Lei no 12.965, de 23 de abril de 2014, que depois foi regulamentada e complementada pelo Decreto no 8.771/2016.

O Marco Civil da Internet pode ser considerado o primeiro avanço sobre o tema da proteção de dados na Internet no nosso ordenamento jurídico, proporcionando maior clareza à questão, com dispositivos sobre a proteção de dados pessoais, tomando como influencia leis vigentes em outros países à época de sua elaboração.

Nota-se que no escopo do Marco Civil da Internet reflete os princípios e direitos fundamentais garantidos previstos no artigo 5º da Constituição Federal, visto, desde logo, no início da Lei, em seu artigo 3º, onde se encontra a vontade do legislador em proteger a privacidade do usuário da internet e, especificamente, aprecia a proteção de dados na medida em que reafirma os princípios constitucionais relacionados a respeito da privacidade.

A Lei se preocupou de tal forma com a proteção dos dados pessoais expostos na internet, que criou um capítulo inteiro, o “CAPITULO II DOS DIREITOS E GARANTIAS DO USUÁRIO”, no qual, já em seu artigo 7º, reconhece a essencialidade do acesso à internet para o pleno exercício da cidadania e, para que haja o pleno exercício deste direito, necessário assegurar à inviolabilidade dos dados por meio dos princípios de proteção da privacidade, da inviolabilidade e a proteção da intimidade e da vida privada (MIRANDA, 2018, p. 260).

Seguindo a breve análise da Lei, a seção II trata especificamente “da proteção aos registros, aos dados pessoais e às comunicações privadas”,

determinando as formas legais para disponibilização de conteúdos de comunicação privada.

Observa-se, com a leitura dos dispositivos do Marco Civil da Internet, que este também buscou garantir a autodeterminação informacional, para que o cidadão tenha conhecimento sobre o fluxo de seus dados, podendo, assim, controla-los, por meio deu seu consentimento (BIONI, 2019, p. 132).

Não há dúvidas que o Marco Civil da Internet foi avanço significativo para a regulamentação da internet no Brasil, concluindo Fortes (2016, p. 126) que:

> Mais do que estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, estabeleceu que a disciplina do uso da internet no Brasil tem como fundamentos o respeito à liberdade de expressão; o reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; a finalidade social da rede.

Em suma, apesar de ser composto de alguns dispositivos que regulam a proteção de dados, isto é, ter contribuído de maneira significativa para uma efetiva proteção de dados na rede mundial de computadores, não elide a necessidade de uma Lei geral específica sobre o assunto, para que assim se efetive uma real proteção aos dados pessoais (MIRANDA, 2018, p. 269).

Assim, cita-se (MENEGUETTI; GIACCHETTA, 2014, p. 390):

> Ainda que o Marco Civil da Internet contenha alguns dispositivos e princípios esparsos e genéticos relacionados ao tema, a inexistência de um diploma legal especifico sobre a proteção de dados pessoais, é, frequentemente, um empecilho à efetividade do principio constitucional da intimidade e da vida privada (artigo 5º, inciso X, da Constituição Federal), assim como para a correta e clara delimitação das atividades e ações que são permitidas, desde que consentidas pelos usuários.

À vista do exposto, temos que o Marco Civil da Internet trouxe em seu propósito, fundamentos jurídicos e princípios relativos à proteção dos dados pessoais expostos na internet, entretanto, não conseguiu regularizar da forma plena. Há ainda lacunas vazias, e para uma efetiva proteção, estas deverão ser preenchidas.

3.3 Do Plano Normativo Internacional de Proteção dos Dados Pessoais – Regulamento Geral de Proteção de Dados da União Europeia

A busca por regulamentar a proteção de dados acontece por todo o mundo. Centenas de países já positivaram suas regras e trouxeram uma maior segurança, tanto para o titular dos dados, quanto para os responsáveis pelo tratamento.

O Brasil, por meio do Marco Civil da internet, já estudado a cima, trouxe uma regulamentação significativa com relação à proteção de dados na Internet, porém demonstrou que há a necessidade de ser regulamentada por meio de dispositivo legislativo específico.

A Europa possui longo histórico em regulamentar a proteção de dados pessoais, no qual as primeiras legislações a respeito vieram de seus membros, no qual constantemente vem se atualizando, adequando as normas às novas evoluções na tecnologia e na sociedade (MIRANDA, 2018, p. 96).

Por suposto, apesar da proteção de dados já ser tema de discussão a temos pelos membros União Europeia, somente em 27 de abril de 2016 promulgaram o Regulamento nº 2016/679, também conhecido como "*General Data Protection Regulation*" (GDPR), no qual houve a concentração das normas de proteção dos dados pessoais dos titulares.

O Regulamento dispõe em sua ementa que é "relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" e ressalta que "revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).".

Posto isso, o atual Regulamento nº 679 de 2016 revogou a Diretiva nº 95/46/CE, formulada em outubro de 1995, visto que alguns de seus aspectos se mostraram ineficientes, pois à época de sua criação, o quadro tecnológico e social não eram tão desenvolvidos, necessitando, assim, de uma adequação e modernização às novas realidades (MIRANDA, 2018, p. 124).

Sobre a GDPR, o Presidente do Parlamento Europeu Jean-Claude Juncker dissertou (COMISSÃO EUROPEIA, 2016):

> Ser europeu significa ter o direito a que os nossos dados pessoais sejam protegidos por legislação europeia eficaz. [...] É por esse motivo que o

> Parlamento, o Conselho e a Comissão chegaram a acordo, em maio deste ano, quanto a um regulamento europeu em matéria de proteção de dados. [...] Porque, na Europa, as questões da privacidade são importantes. Trata-se de uma questão de dignidade humana.

Ainda a respeito da criação da GDPR, o autor Leandro Alvarenga Miranda (2018, p. 123-124) pontua que “se fez necessária para padronizar e resguardar de forma mais eficiente a privacidade, bem como criar condições igualitárias para a transmissão de dados entre os Estados-Membros”.

A GDPR veio com três novidades mais significantes, sendo elas as alterações da forma de consentir dos titulares, alterações para reformar as competências das Autoridades de Proteção de Dados e as alterações para induzir certos comportamentos por parte dos responsáveis pelo tratamento.

Para tanto, destaca-se as considerações abarcadas pelo Guilherme B. de Campos Guidi (2018, p. 92-93):

> Em primeiro lugar, em relação aos direitos individuais, a forma de expressão do consentimento e a relevância do adjetivo “informado” foram reforçados, exigindo-se que o titular dos dados tenha acesso facilitado às informações sobre o tratamento, expressas de modo simplificado (ao invés da linguagem geralmente hermética dos contratos), e que seu consentimento seja expressado de modo destacado – com igual facilidade para a sua revogação. Ainda para reforçar direitos dos titulares, os direitos de acesso e de eliminação dos dados (na forma do ‘direito do esquecimento‘‘) são reelaborados e expandidos, dando maior segurança ao titular e ao mercado.
> No que toca o reforço das Autoridades de Proteção de Dados, podemos citar a especificação de sanções que podem ser impostas aos responsáveis por tratamentos de dados que não respeitem as regras do GDPR, a responsabilização também do agente processador dos dados e a nova obrigação de notificação de violações de segurança de dados. Assim, empresas que sofreram ataques para roubo de dados ou que tiverem dados pessoais de seus clientes vazados, por exemplo, deverão agora notificar os titulares dos dados e a Autoridade de Proteção de dados sobre tal fato.
> [...]
> Por fim, o regulamento também traz algumas práticas que servem como incentivo ao responsável pelo tratamento dos dados pessoais para que este zele pelo cumprimento do regulamento e pela garantia da privacidade dos titulares dos dados.
> A primeira mudança vem pela consolidação dos conceitos de *privacy by default* e *privacy by design* como obrigações do responsável pelo tratamento. Nesse sentido, o responsável deve sempre construir seus produtos, serviços e processos tendo em mente a preservação da privacidade e os princípios gerais da matéria, além de utilizar como padra de operação a escolha pela preservação da privacidade em detrimento da publicidade na ausência de um posicionamento expresso do titular de dados.
> A segunda mudança, de igual importância, vem na reafirmação dos programas de incentivo ao cumprimento do Regulamento, pela criação de selos e sistemas de certificação relacionados ao grau de zelo da empresa com a privacidade de seus usuários.

Insta realçar que o Regulamento recorre para qualquer pessoa localizada na União Europeia, e não só a cidadãos europeus.

Nesse sentido:

> Há de se ressaltar que a GDPR se aplica em todos os casos de tratamento de dados de pessoas singulares que se encontrarem na União Europeia, mesmo que o responsável ou subcontratante não esteja estabelecido no bloco comunitário, desde que o tratamento esteja relacionado à oferta de bens ou serviços, ainda que gratuitos (MIRANDA, 2018, p. 129).

A aplicação da extraterritorialidade da GDPR pode alcançar, por exemplo, empresas brasileiras, no caso destas coletarem dados e controlarem-nos de titulares de dados na UE. Estão sujeitas a lei as empresas brasileiras que efetuem o oferecimento de produtos, serviços ou que coletem, monitorem, processem e tratem dados de qualquer pessoa identificada, ou, pelo menos, identificável, que se encontrarem fisicamente no território Europeu.

Em relação aos sujeitos responsáveis pelo tratamento e suas responsabilidades, cita-se:

> O processador data (processador de dados) é a empresa ou organização que, claro, trata os dados. Ela responde ao controlador. Mas há responsabilidade solidária. Exemplo: uma cervejaria terceiriza o salário dos funcionários a uma empresa de pagamentos, que oferece o sistema de tecnologia e de armazenamento de dados dos trabalhadores. A cervejaria é o controlador e a terceirizada é o processador. Há situações em que uma entidade exerce as duas funções (SOPRANA, 2018, p.1).

Desse modo, resta claro que o objetivo da GDPR, de acordo com o autor Leandro Miranda (2018, p. 124) leciona:

> Desse modo, a GDPR veio com o objetivo de assegurar uma proteção coerente e elevada às pessoas singulares, eliminando, ainda, os obstáculos à circulação de dados pessoais, criando por meio desta norma uma proteção efetiva e equivalente em todos os Estados-Membros.

Assim sendo, entende-se que o Regulamento 2016/679 da União Europeia (*General Data Protection Regulation* – GDPR) não só verte para a efetiva proteção dos dados pessoais, mas estabelece procedimentos claros e insere em seu conteúdo também soluções tecnológicas para tanto.

Portanto, tem-se que é um modelo de lei apropriado para se vislumbrar os direitos, os conceitos, e as direções para uma lei específica brasileira acerca da proteção dos dados pessoais.

4 REGIME JURÍDICO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

Recentemente foi sancionada no Brasil sua própria Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Sua elaboração foi oriunda, principalmente, da reunião de dois projetos de leis antigos que tramitaram pelo Congresso Nacional – o PL 4.969/2912 e PL 5.276/2916.

Teve, também, grande inspiração da mais importante normativa sobre o tema da proteção de dados no mundo, a GDPR (*General Data Protection Regulation*), já mencionada em tópico específico.

Como visto, a GPDR é uma legislação editada pela União Europeia - já produzindo seus efeitos na esfera jurídica -, na qual ditou regras de como devem resguardar com os dados pessoais que estão nos meios digitais.

Resta claro que a nova LGPD filiou-se ao modelo europeu de proteção de dados pessoais, pois este estabelece dois pilares centrais: apreciar o princípio fundamental da dignidade e da proteção da pessoa humana; e, também, garantir o princípio da livre circulação, mas controlada dos dados pessoais (BRANCHER; BEPPU, 2019, p.256).

É uma Lei que trouxe em seus dispositivos: princípios, direitos e obrigações sobre a proteção de dados pessoais, visando garantir à efetividade dos direitos fundamentais do ser humano para o tratamento de dados, na tentativa de assegurar a sua aplicação da melhor maneira possível.

4.1 Lei Federal nº 13.709 de 14 de Agosto de 2018

Diante da nossa realidade tecnologia, já exposta até agora, é que, então, houve a necessidade de editar uma legislação nacional, como explica a autora Patrícia Pinheiro (2018, p. 317):

> A necessidade de uma lei específica sobre proteção de dados pessoais decorre da forma como está sustentado o modelo atual de negócios da sociedade digital, na qual a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências.

No mesmo sentido, leciona o autor Paulo Marcos Brancher que (2019, p. 65):

> A disciplina da proteção de dados pessoais emerge no âmbito da sociedade em rede justamente como uma possibilidade de proteger o indivíduo dos potenciais riscos oriundos do tratamento de dados a partir da moderna tecnologia da informação.

Pode-se extrair da Lei que a sua aplicabilidade é para todos aqueles que realizam o tratamento de dados pessoais, sejam órgãos públicos ou privados, pessoas jurídicas ou físicas, independente do meio. Tal regra se encontra no artigo 3º da LGPD.

Importante ressaltar que, de acordo com o parágrafo primeiro do artigo supracitado, a Lei é direcionada a todo tratamento de dados pessoais coletados em território nacional, isto é, quando o titular desses dados se encontrarem no país no instante que foi coletado seus dados, em meios digitais, ou até fora dele, objetivando a proteção de direitos fundamentais, como o da liberdade e de privacidade, e o livre desenvolvimento da personalidade do indivíduo.

Além disso, esta estabelece uma série de regras que estas empresas e outras organizações atuantes no Brasil sigam para permitir que o cidadão tenha mais controle sobre o tratamento que é dado às suas informações pessoais.

Interessa, em primeiro momento, compreender que a Lei, conforme seu artigo 1º faz menção aos seus objetivos, no qual seja a proteção e garantia de direitos fundamentais e individuais dos titulares dos dados.

Por outro lado, mesmo que a LGPD seja regida por fundamento jurídico e seus objetivos, o legislador, a fim de nortear a sua aplicação, incluiu dez princípios gerais de proteção de dados pessoais, em seu artigo 6º, que devem ser observados para qualquer tratamento dos dados pessoais.

Importante destacar que, em nosso ordenamento jurídico, os princípios possuem uma grande força, servindo como colunas sobre os quais o legislador se inspirou para dar luz às normas. Nesse sentido, pela doutrina, Celso Antônio de Mello (2007, p. 115) define princípio como:

> Principio, é por definição, mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e servido de critério para sua exata

> compreensão e inteligência exatamente por definir a lógica e a racionalidade do sistema normativo.

Pertinente observar, também, a definição fornecida pela De Plácido e Silva (2001, p. 639), que define:

> Princípios, no plural, significam as normas elementares os requisitos primordiais instituídos como base, como alicerce de alguma coisa [...] revelam o conjunto de regras ou preceitos, que se ficam para servir de norma a toda espécie e ação jurídica, traçando, assim, a conduta a ser tida em qualquer operação jurídica [...] mostram-se a própria razão fundamental de ser das coisas jurídicas, convertendo-as em perfeitos axiomas [...] significam os pontos básicos, que servem de ponto de partida ou de elementos vitais do próprio Direito.

Assim sendo, a intenção do legislador da LDPG foi reunir fundamentos jurídicos, seus objetivos e princípios, no qual todos deverão ser interpretador harmonicamente, a fim de dar coesão e adequação à sua aplicação (COTS; OLIVEIRA, 2018, p. 59).

Para fins da Lei nº 13.709/2018, a definição do que vem a ser dado pessoal, com fulcro no parágrafo I de seu artigo 5º, é ser alguma informação relacionada à pessoa natural identificada ou, pelo menos, identificável.

À vista disto, tem-se ser qualquer informação, de quaisquer naturezas, sendo condicionado o titular dos dados pessoais ser distinguível direto ou indiretamente – preferencialmente por referencia a um identificador, como o próprio nome, cadastro de pessoa física, registro de identidade.

No que concerne à classificação, encontra-se no mundo jurídico uma vasta variedade de rótulos para diferentes dados pessoais. Entre eles, a legislação atribuiu relevância à conceituação de dados pessoais sensíveis.

Por dados sensíveis, já conceituados acima nos parágrafos anteriores, entende-se como os referentes à de origem racial ou étnica, convicções religiosas, opiniões políticas, saúde ou à vida sexual.

Por decorrência de sua essencialidade, o doutrinador Têmis Limberger (2007, p. 203) afirmou que tais dados possuem “[...] potencialidade maior de causar ofensa aos direitos fundamentais, não somente no tocante ao direito à intimidade, mas, especialmente ao princípio da igualdade”.

Por fim, é de extrema importância ressaltar que, além da classificação de dados pessoais sensíveis, encontram-se na legislação aqueles em que a pessoa não é identificada ou identificável, chamado de dados anônimos. Essa terminologia encontra fulcro no artigo 5, inciso III, e artigo 12 da lei.

Antes da normatização da proteção de dados, pouco se falava destes dados, pois eram considerados dados não detentores do direito de proteção, por serem considerados completamente anônimos, e, consequentemente, não permitindo, em hipótese alguma, a identificação de seu titular.

Tais disposições da lei inovaram a respeito do absoluto anonimato, caindo por terra o pensamento em que há possibilidade de conseguir completa não identificação do individuo, mesmo que isto seja benéfico a ele.

Isto, pois, a lei, em consonância com a Constituição Federal, trouxe uma razoabilidade quanto o anonimato, pois, a própria Magna Carta, pela leitura do seu artigo 5º, inciso IV, expressa que “É livre a manifestação do pensamento, sendo vedado o anonimato”.

Sustenta-se, em suma, que o anonimato possui condão de proporcionar uma maior proteção ao titular dos dados, resguardados quando tiverem a intenção de proteger intimidade, a vida privada, a honra e a imagem das pessoas.

Pode-se dizer, em síntese, que a nova regulamentação traz uma padronização para a tutela dos diversos tipos de dados pessoais, especialmente no âmbito da *web*, por ser o meio de maior captação de tais dados, necessitando, assim, conceder ao titular maior controle sobre a divulgação de seus dados, e maior garantia de que este terá resguardado todos os seus direitos e liberdades ao dispor qualquer informação pessoal, sem que, de alguma forma, possa ser prejudicado.

Devido a isso, a LGPD traz alterações e inovações de grande relevância jurídica, como a forma que será tratado os dados pelos responsáveis, quais são os direitos dos titulares dos dados, e as responsabilizações dos agentes de tratamentos e consequentes sanções, nos quais serão tratados a seguir no presente artigo, com o único objetivo de garantia e eficácia da proteção do titular dos dados.

4.2 Dos Direitos dos Titulares de Dados Pessoais

A LGPD, sendo uma Lei que objetiva a proteção dos dados pessoais, tem como finalidade assegurar a garantia dos direitos fundamentais, como a liberdade e privacidade da pessoa natural e, com isso, assegurar também às pessoas naturais à titularidade de seus dados pessoais que estão disponíveis.

Visto isso, para fins de regulamentar os direitos assegurados aos titulares dos dados pessoais, a LGPD dedica-se, no seu Capítulo III, aos direitos dos titulares de dados pessoais, nomeado de “DOS DIREITOS DO TITULAR”.

Já em seu artigo 17, é estabelecido que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.”.

A redação deixa claro que os dados pessoais são de titularidade da pessoa natural a quem estão relacionados, isto é, a quem dizem respeito, pertencendo sempre a ela (BRANCHER; BEPPU, 2019, p. 90).

Dentre todas as hipóteses dos direitos previstos aos titulares dos dados pessoais, algumas delas então elencadas a partir do artigo 18, no qual interessante destacar alguns principais direitos, pela importância do assunto, quais sejam:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> [...]
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> [...]
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

É interessante notar que, nos termos dos incisos do artigo 18, em conjunto com o § 3º do referido artigo, prevê que “os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.”. Conclui-se, então, que esses direitos que detêm os titulares dos dados estão direcionados aos agentes de tratamento - englobando tanto os controladores, como os operadores.

Garantir ao titular o direito de ter a confirmação da existência de tratamento, acesso aos dados tratador e os corrigi-los, quando incompletos, inexatos ou desatualizados, esclarece-nos de que, como a própria lei, em seu artigo 6º, traz princípios básicos para a proteção de dados pessoais, praticamente todos os direitos listados, já haviam sido mencionados.

Daí por que o artigo 18 da LGPD apresenta uma função sistematizadora, no qual os princípios irradiam seu conteúdo estimativo sobre as demais normas, imprimindo-lhes unidade e coerência.

À vista disso, para melhor explicação, dar ao titular o direito à confirmação da existência de tratamento, ou seja, direito de saber se os seus dados estão ou não sendo objeto de tratamento, interliga diretamente este direito ao principio da transparência, no qual está previsto no mesmo regramento legal, em seu artigo 6º, inciso VI, garantindo ao titular “informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, [...]” (BRANCHER; BEPPU, 2019, p. 91).

No que concerne ao direito de acesso, este também deriva de um dos princípios elencados pela LGPD, no qual seja o princípio do livre acesso, vide artigo 6º, inciso IV. Isto quer dizer que, o titular terá o direito de “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralização de seus dados pessoais”.

Nesse sentido, pontua o autor Paulo Brancher (2019, p. 91-92):

> Ou seja, o titular pode exigir do controlador copia de seus dados pessoais de sua titularidade que são objeto de tratamento por esses controladores.
> [...]
> Nesse contexto, controladores devem estar preparados para atender a solicitação dessa natureza de imediato.

Diante da importância crescente dos dados para a vida das pessoas, é fundamental estabelecer uma espécie de devido processo legal em relação aos dados, possibilitando aos titulares o direito de correção de informações a seu respeito, quando essas se encontrarem incompletas, inexatas ou desatualizadas.

Esse direito citado é um corolário do principio da qualidade dos dados, pelo qual já da a garantia de “exatidão, clareza, relevância e atualização dos dados,

de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (BRANCHER; BEPPU, 2019, p. 93).

Salienta-se que, garantindo a plena eficácia do direito citado, a previsão do § 6º do art. 18 da LGPD nos traz que o responsável pelo tratamento tem a obrigação informar a correção prontamente aos agentes de tratamento com os quais tenha.

Por fim, vale a pena ressaltar dois dos direitos do titular dos dados pessoais que então relacionados: o direito da revogação do consentimento, e o direito de eliminar os dados pessoais tratados com o consentimento do titular.

Estão relacionados, pois, pelo parágrafo 5º do artigo 8º, este estipula que:

> O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificando os tratamentos realizados sob amparo do consentimento anteriormente manifestado, enquanto não houver requerimento de eliminação, nos termos do inciso IV do caput do art. 18 desta Lei.

Sempre que os agentes de tratamento utilizarem com base para controlar os dados pessoais, o consentimento, estes devem facilitar a suposta revogação desse consentimento, normalmente dando informações de fácil entendimento, pois, vale observar que os titulares devem poder sempre revogar seu consentimento, sem qualquer prejuízo.

Todavia, ao interpretarmos o artigo acima descrito, compreende-se que, não basta a revogação para que os dados sejam eliminados, isto é, para que a eliminação aconteça, deverá ser requisitada expressamente pelo titular que revogou seu consentimento.

Importante realçar que, nos termos do parágrafo 2 do artigo 18 da Lei, toda vez que a base legal de tratamento de dados pessoais não tiver a necessidade de manifestação de consentimento do titular, este, poderá se opor, exigindo a interrupção de qualquer atividade que suas informações estejam relacionadas, se houver algum descumprimento da LGPD.

Diversos dos direitos dos titulares de dados pessoais decorrem diretamente dos princípios que a LGPD contempla - como visto a cima -.

Tão somente com uma visão conjunta e sistemática da LGPD é que se pode compreender a exata proporção do seu Capítulo III, que, ao versar dos direitos dos titulares, repesca uma série de previsões e de conceitos já definidos preliminarmente, e, assim, garantindo a plena eficácia de suas normas.

4.3 Do Tratamento dos Dados Pessoais

A definição de tratamento de dados pessoais, na LGPD, é extremamente abrangente, englobando varias possibilidades manuseio dos dados na internet.

Esta definição esta prevista no artigo 5º, inciso X, da lei mencionada:

> Art.5º Para fins desta Lei considera-se:
> [...]
> 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 de informação, modificação, comunicação, transferência, difusão ou extração;

Insta salientar que este é um rol é considerado exemplificativo, isto é, não taxativo e exauriente. Isto, pois, a leitura da expressão “toda operação”, em conjunto com o entendimento da expressão “como”, nos da à ideia de que o previsto são apenas exemplos de como poderá ser feito o manuseio e controle de dados, na internet, tornando o conceito extremamente abrangente.

Também importa mencionar que as hipóteses descritas não são cumulativas. Leciona Márcio Cots e Ricardo Oliveira (2018, p. 94), que:

> [...] Uma única atividade da lista já se inclui no conceito de tratamento, por mais simples que seja. Armazenar dados pessoais sem utiliza-los, por exemplo, já é considerado tratamento de dados.

Para fins de regulamentar o tratamento de dados pessoais, a Lei Geral de Proteção de Dados Brasileira (LGPD) elaborou requisitos necessários para advir esse tratamento, além de categorizar e tutelar, de forma diferenciada, os dados pessoais e os dados pessoais sensíveis, abordando dentro do Capitulo II, nomeado de “DO TRATAMENTO DE DADOS PESSOAIS”.

Interessante, em primeiro momento, destacar os requisitos para o tratamento de dados.

Esse tratamento deverá ser feito mediante o enquadramento em um dos requisitos previsto no artigo 7º, no qual é considerado pelos juristas como um rol taxativo, isto é, não será requisito o que não estiver previsto em lei.

Dentre as hipóteses previstas, destacam-se duas, pela complexidade do assunto, e pela diversidade que pode ser tratada, quais sejam:

> Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> [...]
> 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;

Pela expressão “fornecimento de consentimento”, entende-se que, de um lado, há a manifestação de vontade de uma parte em tratar os dados pessoais para alguma finalidade e, do outro, há alguém que anui com tal tratamento.

Na própria LGPD, encontramos um conceito do que seria o consentimento, no qual, de acordo com o inciso XII do artigo 5º, o consentimento é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.”.

Quanto à forma, a Lei mencionada estabelece que alguém só poderá coletar ou tratar dados pessoais pertencentes ao titular, se este permitir, fornecendo seu consentimento por escrito ou por qualquer outro meio capaz de evidenciar a sua manifestação de vontade, vide o *caput* de seu artigo 8º, sendo “ o consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.”.

Ensina Patrícia Pinheiro (2018, p. 65) o porquê da necessidade do consentimento:

> Ao longo dos anos, a necessidade do consentimento na coleta de dados, principalmente no ambiente virtual, foi ganhando importância em razão da sensibilidade e vulnerabilidade que as informações pessoais foram adquirindo com o desenvolvimento da tecnologia.

Ainda, a mesma conclui seu pensamento para qual a finalidade da manifestação desse consentimento do titular dos dados (PINHEIRO, 2018, p. 65):

> Nesse sentido, garantir que as pessoas/usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para assegurar a liberdade e a privacidade.

Outro ponto significativo abordado pela Lei Geral de Proteção de Dados é o do tratamento de dados específicos, em especial, os chamados sensíveis.

A referida lei prevê uma definição de dados sensíveis, no inciso V do seu artigo 5º, sendo aqueles:

> sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genérico ou biométrico, quando vinculado a uma pessoa natural.

Em complementação, a LGPD estabelece restrições importantes quando diante do tratamento de dados sensíveis, inclusive a relação do consentimento nesse caso, abordado na redação de seu artigo 11, no qual devem ser dados de forma especifica, para finalidades especificas.

O legislador, ao tratar de maneira diferenciada os dados sensíveis, pretendeu impedir que estes pudessem causar prejuízo ou desvantagens ao titular, isto é:

> Os dados sensíveis merecem tratamento especial, porque em algumas situações a sua utilização mostra-se indispensável, porem o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa (PINHEIRO, 2018, p. 70).

Em sentido semelhante, explica Stefano Rodotà (2008, p. 90) que, é reconhecido que o consentimento do titular de dados sensíveis deve ser diferenciado, na medida em que está a diante de um “contratante vulnerável”, caracterizado justamente por sua ausência de liberdade substancial no momento ta determinação da vontade.

Fazendo uma primeira análise, conclui-se que a base legal de tratamento propriamente dito é a manifestação do consentimento do titular de dados, já tratado acima. E, diante de dados sensíveis, o consentimento necessita ser manifestado “de forma específica e destacada”, de acordo com o inciso I, do artigo 11.

Ressalva-se que, no artigo 7º da LGPD, em seu inciso IX, a própria base legal possibilitou o tratamento de dados pessoais sem a necessidade de manifestação de consentimento do titular dos dados, isto é, utilizando-se de um juízo de ponderação, no qual coloca lado a lado os interesses legítimos do controlador ou de terceiros e os direitos e liberdades fundamentais do titular dos dados.

Para melhor explicação, o autor Paulo Marcos Brancher (2019, p. 110) leciona que:

> O tratamento de dados pessoais com base no *legitimo interesse do controlador ou de terceiros* coloca-se, nos termos da lei, como alternativa ao consentimento, podendo o controlador decidir pela via dos “legítimos interesses” mesmo quando a obtenção da autorização do titular seja uma alternativa possível, desde que estejam presentes, no caso concreto, circunstâncias que coloquem tais interesses em posição de prevalência *vis-à-vis* os direitos fundamentais dos titulares.

Ainda na mesma linha de raciocínio, em um estudo no Grupo de Trabalho instituído pela Comissão Europeia, entendeu-se que, um interesse será considerado legítimo, desde que:

> o responsável pelo tratamento possa prosseguir esse interesse em conformidade com a legislação em matéria de proteção de dados e a demais legislação aplicável. Por outras palavras, um interesse legítimo deve ser admissível nos termos da lei.

Para aplicarmos devidamente o sopesamento e proporcionalidade entre o legítimo interesse e os direitos fundamentais do titular dos dados, visando sempre a proteção desses, o Robert Alexy (2017, p. 117) nos trouxe três regras cruciais a serem observadas:

> (i) adequação, isto é, o meio deve ser apto para alcançar o resultado pretendido;
> (ii) necessidade, ou seja, a finalidade não pode ser alcançada por outro ato que limite, em menor medida, o direito atingido; e
> (iii) proporcionalidade em sentido estrito, consistente no sopesamento entre a intensidade da restrição ao direito atingido e a importância da realização do direito que com ele colide.

Fato é que a LGPD se preocupou em trazer outras hipóteses de legitimação do tratamento de dados pessoais, dentre os quais, a de legitimo interesse. Isto, pois, mesmo que o objetivo desta Lei seja de proteger o titular dos dados, o exercício de sopesamento para o tratamento de dados, com base no legítimo interesse à vista de outros direitos fundamentais, deverá sempre ser assegurado em uso justo e ético dos dados, consubstanciado na adequação, necessidade e proporcionalidade (BRANCHER; BEPPU, 2019, p. 121).

Tendo em vista os aspectos observados, conclui-se que a Lei Geral de Proteção de Dados Pessoais abordou o tratamento dos dados pessoais em consonância com a observação de direitos fundamentais e garantias do titular dos dados, como a boa-fé e, ainda, concederam finalidades, limites e garantias de segurança ao extrapolar o tratamento de tais.

O consentimento, embora continue se apresentando com principal e mais seguro meio para legitimação do tratamento dos dados pessoais, este deixa de ser o único meio apto, abrindo espaço, pela LGPD, para o exercício de sopesamento e juízos de ponderação, onde se leva em conta os legítimos interesses de pessoas que não titulares dos dados.

5 DA RESPONSABILIDADE DOS AGENTES DE TRATAMENTO NA LEI GERAL DE PROTECAO DE DADOS

Dando continuidade às disposições da Lei Geral de Proteção de Dados Pessoais, estas nos trazem os agentes de tratamento, isto é, aqueles responsáveis por todo meio de tratamento dado aos dados pessoais da Internet. Ademais, normatizam sobre suas responsabilidades e obrigações quanto aos cargos que exercem, e possíveis sanções a serem aplicadas como consequência punitiva prática a eles, se descumprirem a norma.

5.1 Dos Agentes de Tratamento

A LGPD trata, também, da responsabilidade dos agentes de tratamento, sendo eles o controlador e o operador, definidos na própria lei nos termos do artigo 5º, VI e VII, respectivamente:

> Art.5º [...].
> [...]
> VI – controlador: pessoa natural ou jurídica, de direito publico ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII – operador: pessoa natural ou jurídica, de direito publico ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> [...]
> IX – agentes de tratamento: o controlador e o operador;

Outro conceito dos agentes de tratamento é dado pela Patrícia Pinheiro (2018, p. 27), diferenciando-os em:

> o controlador é aquele que recepciona os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção, e o operador é aquele que realiza algum tratamento de dados pessoais motivado por contrato ou obrigação legal.

É crucial a distinção de um controlador e um operador de dados pessoais, pois a diferença entre eles se encontra no poder de decisão. O operador realizará o tratamento dos dados pessoais, mas ocorre a partir das ordens de um controlador, que, por sua vez, apresenta-se como o “dono” ou responsável por essas

informações. É o controlador que está no topo da cadeia de tratamento de dados (VENTURA, 2019, p. 1).

Antes de adentrarmos no tema principal propriamente dito, cabe falar das obrigações desses agentes de tratamento previstas no artigo 37 da LGPD.

Entende-se que, como já abordado a cima, todo tratamento de dados pessoais poderá ser feito, desde que seja para atingir determinada finalidade, esta que consta em um dos principais princípios da LGPD, como seu artigo 6º prevê:

> 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;
> [...].

Para que se atinja a finalidade, os agentes de tratamento, normalmente, utilizarão mais de uma atividade.

Fazendo uma interpretação do artigo 37 da referida lei, Márcio Cots e Ricardo Oliveira (2018, p. 213) entenderam o seguido sentido pra norma:

> O artigo 37 estabelece a obrigação do controlador e do operador de manterem registro das operações de tratamento que realizarem o que pode se dar das mais diferentes formas. Dados como a atividade desenvolvida, data, horário, identificação da pessoa natural que realizou o processo, meios tecnológicos utilizados, como sistemas e *softwares*, entre outras informações, serão uteis.

Vale mencionar, ainda, que a própria Lei instituiu o chamado relatório de impacto à proteção de dados pessoais, tal como está definido pelo artigo 5º, inciso XVII, sendo a:

> documentação do controlador que contem a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardadas e mecanismos de mitigação de risco.

Na prática, o relatório poderá ser requisitado a qualquer tempo pela Autoridade Nacional, e será elaborado pelo controlador para descrever todo o tratamento dado aos dados pessoais, avaliando a necessidade e proporcionalidade, para que ajude o controlador a monitorar os riscos que esse tratamento poderá

causar a direitos e liberdades do titular. Isto é, no RIPDP, constará a descrição dos dados coletados, a metodologia utilizada para esta coleta e, para a garantia da segurança do titular dos dados, os mecanismos de mitigação de riscos adotados pelo controlador (BRANCHER; BEPPU, 2019, p. 288).

Tal qual, é de extrema importância à determinação de quem será o controlador ou operador do tratamento dos dados pessoais, pois a estes são encarregados várias obrigações a serem cumpridas em relação ao tratamento dos dados pessoais e, ademais, a estes poderão ser atribuídos responsabilidade civil pelos danos que causarem, por violação de qualquer norma da LGPD.

5.2 Da Responsabilidade Civil dos Agentes de Tratamento

Ainda que no nosso ordenamento jurídico já tenha a regulamentação sobre a Responsabilidade Civil, como prevê o Código Civil, em seus artigos 186 e 187, combinados com o artigo 927, a Lei Geral de Proteção de Dados optou por reforçar sobre o assunto na Seção III, chamada “Da Responsabilidade e do Ressarcimento de Danos”.

O tratamento de dados feito pelos agentes de tratamento, isto é, o controlador e o operador, será considerado irregular quando deixar de observar a LGDP, sendo consequência para os responsáveis à reparação pelos danos causados a essa inobservância, como prevê o *caput* do artigo 42:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> [...].

Aclarando mais sobre o tema, a premissa do artigo 42 é dizer que os agentes de tratamento responderão pelos danos que próprios causarem, seja eles materiais ou morais, individuais ou coletivos, por violação à LGPD. Insta ressaltar que, de regra, cada um responde pelos atos praticados e por eventuais prejuízos causados (COTS; OLIVEIRA, 2018, p. 225).

Para os agentes serem responsabilizados civilmente, é elemento necessário estar evidenciado o nexo de causalidade entre a conduta ilícita à LGPD e

o dano. Nexo causal, segundo Sergio Cavalieri Filho (2012, p. 67), é definido como o "elemento referencial entre a conduta e o resultado. É através dele que poderemos concluir quem foi o causador do dado".

Maria Helena Diniz, citando Giorgio Giorgi, doutrinador italiano, determina a impossibilidade de se falar em responsabilidade civil "sem a existência de um dano a um bem jurídico, sendo imprescindível a prova real e concreta da lesão" (2013, p. 77).

Nesse mesmo sentido, afirma o doutrinador José de Aguiar Dias (1983, p. 177) que é necessário demonstrar, para excluir a responsabilidade civil, ao propor alguma ação de reparação que, sem o fato alegado, o dano não teria ocorrido.

Excepciona-se a regra pela previsão do parágrafo 1 do artigo 42 da LGPD, quando será considerada responsabilidade solidária pelo ressarcimento "a fim de assegurar a efetiva indenização ao titular dos dados".

O doutrinador Silvio Venosa (2006, p. 63-64) nos explica que "se unicamente os causadores dos danos fossem responsáveis pela indenização, muitas situações de prejuízo ficariam irressarcidas". A responsabilidade solidária, portanto, é mais uma das formas de responsabilidade, no qual visa que a vítima não seja prejudicada.

A Lei, então, elaborou duas hipóteses de responsabilidade solidária entre o controlador e o operador, pelos danos causados.

À vista das duas hipóteses previstas, pela primeira entende-se que é crucial o operador conhecer e aplicar sempre as regras da LGPD, mesmo que for contra as instruções passadas pelo controlador. E, pela segunda hipótese de responsabilidade solidária, frisa a ideia de que a comunicação e a instruções passadas do controlador ao operador devem ser claras e precisas, no que versar sobre tratamento de dados (COTS; OLIVEIRA, 2018, p.226).

Posto isso, o titular dos dados pessoais, no qual será o credor da indenização, poderá cobrar a dívida total tanto do controlador, como do operador, dentre qualquer uma das duas hipóteses, pois nestes casos ambos seriam responsáveis solidários.

Ainda, em termos de responsabilidade civil, há outros pontos que também merecem atenção.

A Lei definiu expressamente três exceções à responsabilização descritas nos incisos do artigo 43, isto é, situações em que os agentes de tratamento poderão afastar o dever de indenizar. Nesses casos, incumbe aos agentes provarem: (i) que não realizarão o tratamento dos dados; (ii) embora efetuado o tratamento, não violaram a lei; e, por fim (iii) o dano decorreu de culpa exclusiva do titular dos dados ou de terceiros (COTS; OLIVEIRA, 2018, p. 229).

Por fim, importa trazer o artigo 44 da referida Lei, no qual nos da as condições de demonstração da ilicitude do tratamento de dados pessoais, isto é, quais atos de fato praticado pelos agentes de tratamento serão considerados irregulares de acordo com a LGPD.

Será considerado irregular, e, portanto uma ilicitude, o tratamento dos dados pessoais quando os agentes de tratamento violar qualquer disposição da Lei Geral de Proteção de Dados ou, tendo o dever quanto ao fornecimento de segurança dos dados do titular, deixarem de observa-lo.

Dado o exposto, destaca-se que a LGPD emerge como norma fundamental para a tutela, dentro do escopo de dados pessoais, da privacidade, da dignidade e da imagem das pessoas. Esta, ao buscar o tratamento dos dados de forma legitima, traz a responsabilização dos agentes encarregados tratamento, quando não atingirem suas funções, determinadas em lei, para o fim de conceder maior segurança e garantia aos titulares dos dados, esses que, como já concluído nos parágrafos acima, são a parte vulnerável e hipossuficiente da relação.

5.3 Da Relevância das Sanções Administrativas para a Eficácia da LGPD

Não há como se falar em plena eficácia da norma, se para o descumprimento desta não existir sanção, pois sem qualquer consequência punitiva, resta apenas o dever moral do cumprimento da norma. Isto é, se alguém é compelido a se comportar de determinada maneira ou passar a assumir certa obrigação, logo buscara saber quais esforços deverá empreender, e qual será a sua consequência caso não atinja êxito nos seus esforços (BRANCHER; BEPPU, 2019, p. 295).

No caso da Lei Geral de Proteção de Dados, esta trouxe, no texto de seu artigo 52, um rol exaustivo de sanções descritas como de natureza administrativa, quais sejam:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração

A sanção administrativa, a titulo de conceituação, é dita pelo autor Fabio Medina Osório da seguinte maneira (2015, p.106 e 107):

> Consiste a sanção administrativa, portanto, em um mal ou castigo, porque tem efeito aflitivo, com alcance geral e potencialmente pro futuro, imposto pela Administração Publica, materialmente considerada, pelo Judiciário ou por corporações de direito publico, a um administrador, jurisdicionado, agente publico, pessoa física ou jurídica, sujeitos ou não a especiais relaciones de sujeição com o Estado, como consequência de uma conduta ilegal. Tipificando em norma proibitiva, com uma finalidade repressora ou disciplinar, no âmbito de aplicação formal e material do Direito Administrativo.

Ainda, importante salientar que existe duas principais espécies de sanções administrativas, que possuem dois objetivos distintos, quais sejam: ressarcimento de danos ou retribuição.

A sanção administrativa de ressarcimento de danos possui fundamentação no Código Civil, e esta sanção é destinada aos titulares ou terceiros prejudicados (COTS; OLIVEIRA, 2018, p. 258).

Por outro lado, a respeito do segundo tipo de sanção, o Rafael Mello (2007, p. 76) ensina que:

> a sanção administrativa retribuitiva se destina a imputar um mal ao infrator de acordo com o ato ilícito praticado. Esse tipo de sanção não está voltado ao ressarcimento dos danos causados. A sua finalidade é evitar a repetição de novos atos ilícitos.

Conforme visto, conclui-se que a sanção imposta pela LGPD trata-se de sanções administrativas retributivas, constituindo-se um mal ou castigo, a fim de desestimular condutas similares, pois a importância dessas medidas para a eficácia da legislação que envolve a proteção de dados pessoais é tamanha.

Voltando à temática principal, a LGPD estabelece por quais sanções sujeitam-se as infrações dos agentes de tratamento e o que se deve ser observado pela autoridade sancionadora na aplicação da respectiva sanção.

Na esfera administrativa, na a aplicação de sanções, é possível estabelecer o responsável pela infração. Segundo o referido artigo, as sanções são direcionadas aos agentes de tratamentos, isto é, ao controlador e ao operador de dados pessoais, já conceituados à cima.

No tocante a dosimetria das sanções administrativas, qualquer decisão sancionatória tomada pela Administração Publica deve estar munidas, dentre outros, pelo principio da proporcionalidade, sendo o qual toda ação administrativa deve conduzir a um resultado razoável e proporcional à finalidade da lei e ao interesse publico, devendo sempre existir razoabilidade entre a medida adotada e a finalidade que se pretende alcançar (BRANCHER; BEPPU, 2019, p.303).

A respeito da aplicação do principio da razoabilidade, explica o doutrinador Antonio José Resende (2009, p. 55-56):

> A razoabilidade é um conceito jurídico indeterminado, elástico e variável no tempo e no espaço. Consiste em agir com bom senso, prudência, moderação, tomar atitudes adequadas e coerentes, levando-se em conta a relação de proporcionalidade entre os meios empregados e a finalidade a ser alcançada, bem como as circunstancias que envolvem a pratica do ato.

Dessa forma, a autoridade nacional responsável pela gradação das sanções, pela LGPD, deverá levar em consideração as peculiaridades do caso concreto, sob à luz do principio da proporcionalidade e razoabilidade, para que as penalidades aplicadas não sejam excessivas e desproporcionais à conduta praticada (COTS; OLIVEIRA, 2018, p. 266).

Em conclusão, a LGPD, no que diz respeito às sanções administrativas, apresenta elementos suficientes para que se inicie a execução de seus regramentos de proteção de dados no território nacional e, ainda, é oportuno

salientar que a sanção cumprirá papel educativo, por isso deverá sempre empregar a razoabilidade e a proporcionalidade pela autoridade sancionadora.

A partir da data em que a Lei de Proteção de Dados iniciar sua aplicação no plano prático, todos que vinham realizando suas atividades neste mercado, sem qualquer regramento, ou se adaptam à nova realidade legislativa, ou poderão estar sujeitas a sanções, de acordo com os dispositivos da nova lei.

6 CONCLUSÃO

As benesses oriundas da Lei Geral de Proteção de Dados são evidentes, principalmente, quando tomados parâmetros globais atuais de captação e transmissão de dados pessoais, mormente de barreiras territoriais.

O presente trabalho procurou discorrer acerca da problemática atual dos dados pessoais e de seu tratamento na Internet, através da leitura de artigos, doutrinas e legislações, analisando o desenvolvimento da nossa sociedade sob a ótica dos direitos à privacidade e à informação até o entendimento da proteção dos dados pessoais como um direito autônomo e fundamental.

Inicia-se o primeiro capítulo definindo dados, enquanto qualquer informação sobre o sujeito, pessoa física ou jurídica, que permita identifica-lo naquele ou momento ou, pelo menos, ser um dado identificável, também acerca dos dados sensíveis, como aqueles referentes à origem racial ou étnica, às opiniões políticas, às convicções religiosas, bem como os referentes à saúde ou sexualidade, os quais, por serem considerados mais íntimos do ser humano, os tornam mais suscetíveis a atitudes discriminatórias e outros fins ilícitos.

Dando continuidade ao capítulo, desenvolveram-se as noções de modernidade liquida e sociedade de informação, sob a ótica da vulnerabilidade dos dados neste atual modelo societário. Pôde-se afirmar vivencia-se uma realidade onde seu combustível é a Internet e a as inúmeras informações que nela contem, no qual vem se produzindo e transmitindo incontrolavelmente, fluxo esse que não obedece qualquer barreira. Inegável que a Internet possui papel fundamental, entretanto os próprios cidadãos precisam se atentar aos dados que disponibilizam, pois muito possivelmente seus dados não serão utilizados no todo de forma adequada.

No segundo capitulo, discorre acerca da evolução tecnológica, no qual trouxe consequências acerca do aumento significativo no fluxo de informações e dados pessoais dos usuários. Ademais, entendeu-se que, essa transmissão de dados desenfreada poderá ocasionar diversos riscos, necessitando de uma legislação pertinente a matéria. Restou evidencia da necessidade de proteção dos dados pessoais diante do evidente potencial lesivo à dignidade da pessoa humana decorrente da manipulação de dados pessoais pelos bancos de dados

automatizados, sem esquecer-se de buscar o equilíbrio com o direito fundamental ao acesso à informação, visto que este é vetor de relevância social.

Prosseguiu-se analisando uma evolução legislativa em relação a proteção dos dados pessoais, no qual, no Brasil, observou-se que o Marco Civil foi o principal avanço legislativo a respeito da proteção dos dados pessoais na Internet, utilizando como pilar os direitos fundamentais presentes em nossa Constituição, como o da privacidade. Na seção subsequente, discutiu-se a proteção de dados no direito comparado, com enforque no Regulamento Geral de Proteção de Dados (GDPR), norma da União Europeia, que serviu de base para a nossa atual Lei Geral de Proteção de Dados Pessoais, no qual também dispõe sobre o tratamento de dados e sua efetiva proteção no âmbito da Internet.

No terceiro capítulo, partiu-se para a análise branda da nova Lei de Proteção de Dados Pessoais do Brasil, a Lei nº 13.709/18. Verificou-se que a LGPD foi uma conquista legislativa de tamanha importância, pois nesta veio a regulamentação específica, de maneira ampla e sistemática, a respeito dos direitos, obrigações e sanções aplicáveis na proteção de dados pessoais, bem como a forma de deverão serem tratados esses dados pessoais pelos responsáveis, seguindo conforme a Lei.

No quarto e ultimo capítulo, dando continuidade às disposições da LGPD, discorreu sobre questões relativas às responsabilidades e obrigações dos agentes responsáveis por todo o tratamento dos dados pessoais. Tais agentes, como posto, deverão sempre te ater as disposições da Lei quanto suas obrigações, além de que, para tratamento dos dados, deverão atingir a finalidade que está imposta, pois, a estes, em razão do exercício de atividade de tratamento de dados pessoais, poderão ser atribuídos responsabilidade civil pelos danos que causarem, com a finalidade de conceder maior segurança e garantia dos direitos aos titulares dos dados.

Por fim, acentuou-se, ainda, a aplicabilidade de sanções administrativas trazidas na LGPD, para eficácia plena das disposições contidas na norma. Entendeu-se que, sem sanção, não haveria uma real finalidade das disposições, pois, para quem cometeu o ato ilícito, só restaria o dever moral do cumprimento da norma. Nesse contexto, além da LGDP trazer um rol exaustivo sobre quais são as sanções que poderão ser impostar, trouxe também para quem

serão imputadas, visto ser apenas para os agentes de tratamento, bem como quem terá o poder de dosar as sanções administrativas para sua aplicabilidade, qual seria a Administração Publica. Esta, para qualquer decisão sancionatória, devera estar munida pelos princípios da razoabilidade e proporcionalidade, para sempre aplicar as punições proporcionalmente às condutas ilícitas praticadas.

Em suma, conclui-se que a Lei Geral de Proteção de Dados Pessoais veio como de natureza protetiva, com o intuito de dar maior segurança aos titulares dos dados quando esses disponibilizam suas informações na Internet. Isto é, veio estabelecendo os devidos direitos dos titulares, instituindo obrigações e deveres aos agentes responsáveis pelo tratamento dos dados, bem como uma autoridade fiscalizadora para que se torne eficaz a proteção dos dados pessoais.

Conforme exposto no primeiro capitulo, a captação e transmissão desenfreada de dados pessoais, em especial os dados sensíveis, possui a necessidade de proteção maior, pois podem gerar um alto risco de exposição, ferindo diretamente os direitos fundamentais do individuo, especialmente se utilizados com intuito discriminatório.

A LGPD passará a ter plena eficácia em agosto de 2020. Isso significa que, a partir da data, é de rigor haja o enquadramento dos agentes de tratamento quanto às normatizações, mudando suas formas de atuação, sob a luz da proteção da privacidade do usuário, de mantê-lo informado do tratamento de seus dados, bem como utiliza-los sempre para a finalidade pretendida, para que a Lei consiga trazer no plano concreto os avanços esperados e necessários para a devida proteção dos dados pessoais no Brasil.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais.** Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2017.

AZEVEDO, Ana Cristina Carvalho. **Marco Civil da Internet no Brasil**. Rio de Janeiro: Alta Books, 2014.

BARROSO, Luís Roberto; BARCELLOS, Ana Paula de. **O começo da história:** A nova interpretação constitucional e o papel dos princípios no direito brasileiro. Revista da EMERJ, v.6, n.23, 2003. Disponível em: http://www.emerj.tjrj.jus.br/resitaemerj_online/edicoes/revista23/revista23_25.pdf. Acesso em: 02 nov. 2019.

BAUMAN, Zygmunt. **Modernidade líquida.** Rio de Janeiro: Zahar, 2000.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

_____. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil.** São Paulo: GPoPAI/USP, 2015.

BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia. **Proteção de dados pessoais no Brasil:** uma nova visão a partir da Lei nº 13.709/2018**.** Belo Horizonte: Fórum, 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 out. 2019.

_____. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil Da Internet.** Brasília, 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em: 29 out. 2019.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014**. Diário Oficial da União, Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 27 mai. 2019.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Edições Almedina, 2005.

CAVALIERI FILLHO, Sérgio. **Programa de responsabilidade civil**. 10ª Ed. São Paulo: Atlas, 2012.

COMISSÃO EUROPEIA. **Discussão sobre o Estado da União 2016:** Por uma Europa melhor: uma Europa que projeta, defenda e dê maior intervenção.

Estrasburgo, 14 set 2016. Disponível em: https://europa.eu/rapid/press-release_SPEECH-16-3043_pt.htm. Acesso em: 22 out. 2019.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. São Paulo: Thomson Reuters Brasil, 2018.

DELPECH, Horácio Fernandez. ***Internet*****:** Su Problemática Jurídica. 2 ed. Buenos Aires: Abeledo-Perrot, 2004.

DIAS, José de Aguiar. **Responsabilidade Civil em Debate.** Rio de Janeiro: Editora Forense, 1983.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro.** São Paulo: Saraiva, 2013.

FORTES, Vinicius Borges. **Os direitos de Privacidade e a proteção de dados pessoais da internet.** Rio de Janeiro: Editora Lumen Juris, 2016.

FRAGOMENI, Ana Helena. **Dicionário Enciclopédico de Informática.** São Paulo: Editora Campus, 1986.

GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle**. Marco Civil da Internet:** A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no marco civil da internet. São Paulo: Atlas, 2014.

GUIDI, Guilherme Berti de Campos. **Privacidade em perspectivas:** Modelos Regulatórios para Proteção de Dados Pessoais. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

KING, Anna Lucia Spear; NARDI, Antonio Egidio. **Nomofobia - Dependência do Computador, Internet, Redes Sociais? Dependência do Telefone Celular?** São Paulo: Atheneu, 2014.

LIMBERGER, Têmis. **O Direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo.** 22. ed. São Paulo: Malheiros Editores, 2007.

MELLO, Rafael Munhoz de. **Princípios Constitucionais de Direito Administrativo sancionador.** As sanções administrativas à luz da Constituição Federal de 1988. São Paulo: Malheiros, 2007.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

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

OSÓRIO, Fabio Medina. **Direito administrativo sancionador.** 5. ed. São Paulo: Revista dos Tribunais, 2015.

PARLAMENTO EUROPEU. ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)***. Disponível em: https://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1530135586767&uri=CELEX:32016R0679. Acesso em: 29 out. 2018.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

RESENDE, Antonio José Calhau. **O principio da razoabilidade dos atos do Poder Publico.** Revista do Legislativo: Abril, 2009.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANTOS, Andréia. Privacidade em perspectivas: **O Impacto do Big Data e dos Algoritmos nas Campanhas Eleitorais**. Rio de Janeiro: Lumen Juris, 2018.

SARTRE, Jean-Paul. **Sartre no Brasil:** a Conferência de Araraquara. Rio de Janeiro: Paz e Terra, 1986.

SAUAIA, Hugo Moreira Lima. **A proteção de dados pessoais no Brasil**. Rio de Janeiro: Lumen Juris, 2018.

SCHREIBER, Anderson. **Direitos da Personalidade.** 3. ed. São Paulo: Atlas, 2014.

SILVA, De Plácido e. **Vocabulário Jurídico.** 18.ed. Rio de Janeiro: Forense, 2001.

SOPRANA, Paula. **O que é a GDPR, a lei de proteção de dados europeia, e por que ela importa.** 2018. Disponível em: https://gizmodo.uol.com.br/lei-proteca-dados-gdpr/. Acesso em: 22 out. 2019.

TARTUCE, Flávio. **Direito civil:** lei de introdução e parte geral – v. 1. 15. ed., Rio de Janeiro: Forense, 2019.

VENOSA, Silvio de Salvo. **Direito Civil:** responsabilidade civil. 6. ed. São Paulo: Atlas, 2006.

VENTURA, Ivan. **LGPD: Eu sou um operador ou um controlador de dados?** 2019. Disponível em: https://www.consumidormoderno.com.br/2019/02/18/lgpd-operador-controlador-dados/. Acesso em: 22 out. 2019.

VIENA, Tatiana Malta. **O direito à privacidade na sociedade de informação**. Porto Alegre: Sérgio Antônio Fabris Editor, 2007.

WARNER, Richard. **Undermined norms:** the corrosive effect of information processing, technology on informational privacy. Saint Louis University Law Journal, Saint Louis, v. 55, 2011.