FACULDADE DOM BOSCO DE PORTO ALEGRE
CURSO DE DIREITO

LUCIANE GEMMELLARO

DIREITOS DOS TITULARES DOS DADOS:

Uma breve análise comparativa entre o Regulamento da União Europeia e a Lei brasileira de proteção de dados pessoais

Porto Alegre
2020

LUCIANE GEMMELLARO

DIREITOS DOS TITULARES DOS DADOS:

Uma breve análise comparativa entre regulamento da união europeia e a lei brasileira de proteção de dados pessoais

Trabalho de Conclusão de Curso apresentado como requisito para aprovação na Faculdade Dom Bosco Porto Alegre.
Professora orientadora: Dra. Anair Isabel Schaefer

Porto Alegre

2020

LUCIANE GEMMELLARO

DIREITOS DOS TITULARES DOS DADOS:

Análise comparativa entre regulamento da união europeia e a lei brasileira de proteção de dados pessoais

Trabalho de Conclusão de Curso apresentado como requisito para aprovação na Faculdade Dom Bosco Porto Alegre.

Banca examinadora:

_____

Prof(a) Dr (a)

_____

Prof(a) Dr (a)

_____

Prof(a) Dr (a)

AGRADECIMENTOS

Agradeço primeiramente com todo meu amor a minha Mãe Ivone e ao meu Pai Francisco, por serem meus exemplos de força e fé diante das barreiras de minha vida, e que me incentivaram e cuidaram com todo amor e carinho durante esta jornada.

Juntamente aos meus amados irmãos Alex e Daiane, assim como minhas estrelinhas guias Isabelle, Lucas, Isadora e Diana, meus sobrinhos amados, que tanto me serviram de razão nesta caminhada, mesmo que algumas vezes distantes, ainda assim unidos pelo coração da sua Títi, e tão vivos em mim durante minha jornada acadêmica.

Também agradeço a minha orientadora Sra. Professora Dra. Anair Isabel Schaefer, pela sua tranquila e zelosa orientação e pelo compartilhamento de seu nobre conhecimento e da qual carregarei em meu coração.

Aos amigos feitos durante este caminho por todo apoio e compreensão, em especial Adriel Giordani Christ e Victor Rovaris e nesta reta final a Lucas, Jairo e Nathalia.

Por fim, muito obrigada a Deus, aos meus antepassados, e aos amigos de luz, pela força dada a mim, para perseverar no percorrer de toda esta caminhada.

EPÍGRAFE

Nossa liberdade fundamental é o direito e o poder de decidir como qualquer pessoa ou qualquer coisa fora de nós nos afetará.
(Stephen Covey)

RESUMO

O presente trabalho se debruça sobre o tema proteção de dados pessoais, considerado no momento com um dos mais importantes temas legislativos da atualidade. Abordamos o conteúdo a partir do nascimento histórico do debate sobre proteção de dados a níveis mundiais e de forma cronológica, porém in loco no continente europeu e nos países membros da União Europeia. Analisamos o desenvolvimento legislativo do tema incluindo gerações, Diretivas e leis esparsas até a chegada do atual Regimento Geral de Proteção de Dados, considerada a norma mais completa e atual que regulamenta a proteção de dados pessoais. No mesmo contexto, estudamos a trajetória legislativa desse assunto no Brasil até o nascimento da conhecida Lei Geral de Proteção de Dados, que foi espelhada na lei europeia. A partir disso, foi feita uma breve pesquisa comparativa entre diferenças e semelhanças no capítulo III da LGPD, que versa sobre os direitos dos titulares dos dados pessoais. Concluiu-se que a legislação que protege os dados dos cidadãos é de extrema importância, pois assegura ao titular que seus dados não serão utilizados para fins ilícitos ou discriminatórios.

Palavras-chave: Dados pessoais. Proteção legislativa. Lei Geral de Proteção de Dados. Regimento Geral de Proteção de Dados.

ABSTRACT

The present paper aims to discuss the protection of private data, considered one of the most important legislative topics of our current days. We approached this content as of the historical emergence of the debate on data protection worldwide, but locally focused on the European continent and on countries that are members of the European Union. We analyzed the legislative development of this subject, including generations, Directives and sparse laws until the emergence of the current General Data Protection Regulation, considered the most complete and contemporary norm that regulates the protection of personal data. In the same context, we studied the legislative trajectory of this subject in Brazil until the advent of the Data Protection General Law, which was inspired by the European law. From here onwards, we did a comparative research about the similarities and differences found on the third chapter of the above-mentioned law, which addresses the rights of owners of personal data. We concluded that this legislation is extremely important, because it reassures to the owner that their data will not be used for ilicit or discriminatory purposes.

Key words: Personal data. Protective legislation. General Law of Data Protection. General Data Protection Regulation.

LISTA DE TABELAS

LISTA DE ABREVIATURAS

GDPR – *General Data Protection Regulation*

IBGE – Instituto Brasileiro de Geografia e Estatística

LGPD – Lei Geral de Proteção de Dados

SAFARI - Système Automatisé pour lês Fichiers Administratifis et lê Réportoire de Individus

UE – União Europeia

SUMÁRIO

1 INTRODUÇÃO

As relações humanas e a produção de informações estão vinculadas desde o início da civilização. Mesmo em épocas onde apenas a Igreja e o Estado controlavam as informações, elas já eram consideradas artifícios de poder contra todos os cidadãos. A mudança nesse cenário só ocorreu a partir do século XX, quando o crescimento tecnológico expandiu o fluxo informacional de forma inédita.

Com esse aparato tecnológico ao alcance de nossas mãos, fomos influenciados e nosso cotidiano se transformou frente ao registro de dados, sejam eles públicos ou privados. Em meio à possibilidade de registrarmos nossa localização, nosso histórico e nossas vidas, nos tornamos uma sociedade autogeradora de dados informatizados. É importante notar que as informações em circulação podem ser armazenadas, utilizadas e processadas de forma lícita, mas há o risco de serem auferidas de maneira autoritária e indiscriminada – fato que impulsionou nossos legisladores modernos a elaborarem respostas jurídicas diante de tamanho desafio.

Ao longo do tempo, analistas constataram que não se arquivavam apenas informações; também eram armazenados dados pessoais dos cidadãos, o que permite sua identificação e ocasiona forte perigo a sua vida privada. Um único dado pode ser o suficiente para levar ao perfil de um indivíduo: imagine o que aconteceria com o acesso às suas características pessoais, profissionais ou, ainda, suas preferências para compras, hábitos e necessidades; através do cruzamento desses dados, é possível acessar a sua localização, ou ainda traçar o seu perfil genético, e assim gerar discriminação devido ao controle sobre esses dados, também conhecidos como ‘dados sensíveis’, que incluem, etnia, religião e sexualidade. É nítido, com o decorrer da história, o crescente interesse do Estado e do mercado nessas informações, porém a sua livre circulação pode levar a crimes caso não seja limitada por uma legislação eficiente e protetora.

O presente trabalho será desenvolvido a partir desse contexto legal. O problema da pesquisa em questão é a importância da normativa de proteção de dados pessoais, e o problema é fazer uma breve análise comparativa entre a legislação brasileira e a europeia, na busca por compatibilidade entre elas quanto ao Direito dos titulares dos dados. O método escolhido é o dedutivo, e a coleta de dados será feita através da pesquisa bibliográfica. Abordaremos inicialmente a história da proteção de dados, seguida de um desenvolvimento dessas legislações, evoluindo para uma comparação entre o Regimento Europeu e a LGPD, que ainda se encontra em vacatio

legis. É relevante mencionar que a lei brasileira 13.709/2018 tem como fonte de formação o texto da RGPD, motivo pelo qual analisaremos ambas comparativamente.

Percebemos, portanto, que o debate sobre proteção de dados pessoais e privacidade de informações está intimamente ligado a nossos direitos constitucionais e à Lei, e que apenas através das normativas adequadas é possível assegurar aos cidadãos que seus dados estejam protegidos de ações potencialmente abusivas tanto por parte das corporações quanto por parte do Estado, considerando a relação cada vez mais entrelaçada entre mercado-Estado na atualidade. Por isso, é importante compreender a história da elaboração dessas Leis a fim de que entendamos seus objetivos, seus mecanismos jurídicos e sua aplicabilidade. É o que esse trabalho se propõe a fazer.

2 PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA E NO BRASIL

As polêmicas em torno da temática da proteção de dados pessoais se deram inicialmente na esfera internacional entre as décadas de 1960 e 1970, quando alguns países planejavam unificar seus bancos de dados com a intenção de torná-los automatizados. Esse fato provocou reflexões em parte da população dos Estados Unidos da América e Europa, o que levou ao surgimento da primeira geração normativa sobre proteção de dados nessas localidades.

Nos EUA, isso ocorreu porque o projeto *"National Data Center"* tinha como objetivo se tornar o maior centro de dados nacional, concentrando diversas tecnologias de informática e armazenamento de dados diversos da população estadunidense. Desta forma, seria possível extinguir os demais bancos de dados e a necessidade de ter que alimentá-los, dinamizando a administração de recursos do governo no que diz respeito à ciência de dados. A unificação dos bancos de dados, portanto, trazia diversas vantagens, a começar pela facilidade em extrair dados estatísticos de maneira simples e precisa, assim como o rastreamento, a facilidade para retificar dados de seus cidadãos, uma possível redução orçamentária e, principalmente, materializando a possibilidade de criar estratégias cada vez mais refinadas de controle de populações.

Durante a votação no Congresso Nacional, o projeto foi mal visto ao ficarem notórios os interesses do Estado em ter controle desses dados pessoais, o que poderia trazer prejuízos para toda nação norte-americana. Esse banco de dados iria centralizar e conter informações como os dados acadêmicos, de cidadania, previdência social, sobre tributáveis, patrimônio e dados militares, incluindo os registros criminais. Isso acarretou um forte alerta sobre os potenciais danos que o aparato de dados unificados poderia ter sobre os direitos dos cidadãos, o que fez com que o projeto nunca saísse do papel.[1]

Em meados de 1970, surgiu um projeto semelhante na França, conhecido como SAFARI. Ele foi organizado pelo Instituto Nacional de Estatística, e visava identificar seus cidadãos através de um código numérico. Mas, assim como nos EUA, este projeto de banco de dados foi extremamente mal recebido pela população, diante da

[1] MENDES, Laura Schertel. **TRANSPARÊNCIA E PRIVACIDADE**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 158 f. Dissertação (Mestrado) - Curso de Direito, UnB, Brasília, 2008, p.30.

possibilidade de violação da privacidade, o que pressionou o Estado Francês a abandonar seu plano[2]

A reação negativa dos cidadãos não foi o único motivo pelo qual se abandonaram tais projetos. Há também o fato de que eles estavam descentralizados em diversos países – portanto, não obtendo sucesso na centralização em um banco de dados realmente unificado. [3]

Além da tentativa de construir um bloco unificado de bancos de dados, houve o plano que visava criar números de identificação pessoal para cada cidadão, causando reações negativas tanto na população norte-americana quanto na europeia. Este projeto, assim como o anterior, visava ampliar as informações da Administração Pública e também a interatividade com demais bancos de dados, o que aumentaria a exatidão dos dados acondicionados por estes governos a respeito de seus administrados. Várias foram as investidas para aplicar este código numérico de identificação pessoal de cidadãos, mas é salutar neste contexto a afirmação de Colin Benett, ao indicar que nenhum destes países conseguiu alcançar a implantação destes projetos conforme o molde proposto. O que se viu na prática foi a geração de números diferentes para uso distinto em cada um destes governos, no caso dos EUA, o Social Security Number, na Inglaterra o National Health Service Number, e no Canadá, o Social Insurance Number.[4]

A preocupação gerada pelos bancos de dados unificados e pelos números de identificação pessoal tomou conta da década de 1970, pois causou nervosismo na população diante de uma possível violação de privacidade devido às informações reveladas pelas respostas contidas nos censos (questionários) aplicados em países como a Suécia. Essas respostas poderiam expor os cidadãos e beneficiar empresas de marketing, evidenciando uma arriscada comercialização desse conteúdo. O mesmo ocorreu na Inglaterra, causando polêmica devido à seriedade do tema. O fato também se repetiu entre 1983 e 1987 na Alemanha, pois nos censos eram incluídas questões pertinentes à etnia bem como dados do perfil técnico e profissional dos cidadãos,[5] trazendo à tona problemáticas históricas relacionadas a questões étnico-raciais e sociais que ainda circundavam o pós-guerra no cotidiano do povo alemão

---

2 Ibidem., p.30.
[3] MENDES, Laura Schertel. **Op.Cit.,** p.30.
[4] Ibidem. p. 31.
[5] Ibidem. p. 31

Os eventos acima descritos tiveram, como principal desdobramento, a regulamentação da proteção de dados pessoais nos referidos países. De acordo com Bennett[6], é possível observar mais semelhanças do que diferenças entre eles nesse processo pois, mesmo que haja distinções jurídicas, o foco na proteção de dados é a convergência que os une e, como um processo internacional informalmente coordenado, veio a ser chamado de tese de convergência.

A proteção de dados ultrapassa fronteiras – não podemos negar o constante desenvolvimento desta temática que se engendrou ao cotidiano de todas as populações, mesmo que estejamos diante de particularidades legislativas distintas. Sobre a questão da convergência, Bennett apud Laura Mendes[7] explicita:

> Convergência significa mais que similaridade. Denota um padrão que ultrapassa o tempo, um processo dinâmico, ao invés de uma condição estática. (…). Deste modo, a partir de uma posição em que os Estados não tinham nenhuma ou muito pouca legislação de proteção de dados e, por isso, havia diversos tipos de estratégia para o tema, um consenso emergiu durante a década de 1970, em volta de Princípios. Podemos concluir, portanto, que a convergência ocorreu.

Costa[8], em uma referência a Castells, apresenta

> "cinco quesitos centrais do atual sistema de meios de comunicação e, consequentemente, de produção: a informação vista como matéria-prima; as novas tecnologias trespassando por praticamente todas as atividades humanas; a dinâmica de redes presente nos sistemas e relações em que consta a nova tecnologia; a maleabilidade de organização e reorganização de processos, organizações e instituições; e, por fim, haveria uma tendência para a convergência e integração do sistema como um todo, acarretando em uma interdependência entre biologia e microeletrônica".

Após essa contextualização sobre os debates iniciais envolvendo o tema da proteção de dados, analisaremos o desenvolvimento histórico das legislações europeias que tinham como objetivo regulamentar o uso dos dados dos cidadãos.

2.2 Das diretivas europeias ao regimento europeu de proteção de dados

A proteção de dados pessoais e o mercado europeu passaram por um período de relevante adequação diante da expansão de suas relações comerciais na década

---

[6] Ibidem. p. 33.
[7] MENDES, Laura. **Op.Cit**., p. 34.
[8] COSTA, Mariana Monteiro. **A era da vigilância no ciberespaço e os impactos na nova lei geral de proteção de dados pessoais no Brasil**: reflexos no direito à privacidade. TCC - Curso de Direito, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2018, p. 40.

de 90, o que impulsionou o Parlamento[9] e o Conselho Europeu[10] na busca por uma regulamentação unificada desta matéria. Nasceu, então, a primeira Diretiva nº 95/46/CE[11], oriunda da Convenção nº. 108 do Conselho da Europa no dia 24 de janeiro de 1995, em Portugal. 28 Estados-Membros ratificaram este documento, que tinha como objetivo "proteger o direito fundamental à proteção de dados e assegurar a livre circulação de dados pessoais entre Estados-Membros".[12]

Dentro de um período transitório legal, anterior à chegada do Regimento Geral de Proteção de Dados Europeu, devemos ressaltar que de acordo com Mayer-Schönberger, a "Diretiva Europeia sobre proteção de dados pessoais de 1995 corresponde a mais uma evolução geracional, pela qual passou a disciplina da proteção de dados pessoais na Europa".[13]

Inicialmente, a diretiva abordava o tratamento de dados em ficheiros, mas também indicava os "meios totalmente ou parcialmente automatizados", abrangendo inclusive os dados oriundos de meios digitais - modernizando, portanto, o debate sobre o tema através da formação de princípios e direitos que seguem atualmente como norteadores do texto do Regulamento Europeu (UE) 2016/679, onde incorporou-se as principais partes do conteúdo da diretiva. Tais princípios e direitos, naquele período, vieram a expandir e a reforçar a proteção às pessoas singulares.[14]

Podemos considerar, quanto àquele momento, que a Diretiva era inovadora pois vislumbrava resguardar os dados pessoais de possíveis abusos ou tratamentos inadequados, podendo inclusive ser requerida a culpabilidade ao "responsável pelo tratamento".[15]

Dentro desse prisma de inovação, devemos mencionar alguns dos principais avanços trazidos por esta normativa, dentre eles, seus direitos, como desenvolveu Sawaris:

---

9 O Parlamento Europeu é composto por um máximo de 751 representantes dos cidadãos da UE (750 deputados mais o Presidente). Disponível em: https://www.europarl.europa.eu/factsheets/pt/sheet/20/o-parlamento-europeu-organizacao-e funcionamento. Acesso em: 05.05.2020.

10 Atualmente, o Conselho é constituído por 27 países membros devido à saída da Inglaterra da União Europeia. Disponível em: https://www.consilium.europa.eu/pt/european-council/members/. Acesso em: 05.05.2020.

11 UNIÃO EUROPEIA**.** Diretiva nº 95/46/CE, de 24 de outubro de 1995. **Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Portugal, 1995. Disponível em: shorturl.at/ADEKW. Acesso em: 05.05.2020.

12 SAWARIS, Adriana. **Op.Cit.,** p. 19.

13 MENDES**, Op.Cit.,** p. 39.

14 MENDES**, Op.Cit.,** p. 19.

15 Ibidem, p. 19

> [...] Outro contributo da Diretiva foi a atribuição de diversos direitos ao titular dos dados, quais sejam: direito de informação, de acesso, de retificação e de oposição. Dissertamos brevemente sobre eles, pois serão abordados com mais ênfase no decorrer deste trabalho. O direito de informação, em razão da sua relevância, merecerá um tópico autônomo, onde trataremos suas três vertentes. Contudo, resumidamente, nesse contexto, concede ao titular dos dados: (1) o direito de conhecer os dados que serão recolhidos e a sua pertinência; (2) o direito de saber quem são os destinatários a quem os dados vão ser comunicados e as finalidades da recolha e a sua pertinência; (3) e o direito de saber a identificação do responsável pelo tratamento dos dados e de seu representante, caso houver.
> O direito de acesso é o direito de obter do responsável pelo tratamento informações os próprios dados pessoais. O titular pode assim exigir o seu conhecimento, com presteza e sem encargos excessivos, se os dados estão sendo objeto de tratamento e, em caso positivo, para qual finalidade, qual a categoria de dados que são objeto de tratamento, a que destinatários serão remetidos e qual a origem dos dados. A comunicação destas informações por parte do responsável pelo tratamento deve ser de fácil acesso. Sendo o tratamento realizado de forma automática, deve-se dar conhecimento sobre a lógica subjacente a esse tratamento.
> O direito de retificar, apagar ou bloquear é o direito do titular dos dados de realizar estes atos sempre que o tratamento dos mesmos não cumpra as regras previstas na Diretiva. De igual modo, quando não estejam exatos ou quando estiverem incompletos. Caso este direito seja exercido, o responsável pelo tratamento deve notificar terceiros, a quem os dados possam ter sido enviados, com as alterações realizadas – exceto se for impossível ou em esforço desproporcional.
> Finalmente, o direito de oposição é aquele conferido ao titular de dados de se opor ao tratamento dos mesmos. A oposição pode se basear em razões preponderantes e legítimas relacionadas a particularidade do caso concreto. Da mesma forma, o titular poder se opor ao tratamento para efeitos de “mala direta” (envio em larga escala). [...] [16]

A Diretiva também traz princípios da proteção de dados que iremos contextualizar nos capítulos posteriores onde abordaremos a RGDP. A diretiva foi fundamental para a construção do atual texto do Regimento Europeu, ao indicar que a atuação do cidadão em todo o processo do tratamento de dados pessoais é essencial. Ela também estabelece que o tratamento seja expressamente notificado e aprovado pelo indivíduo. Por fim, traz a possibilidade de o cidadão proibir o uso de seus dados pessoais para efeitos de marketing direto.[17]

Percebemos, então, que a Diretiva apresenta um caráter dinâmico e evolutivo nas normas de proteção de dados da Europa, que foram desenvolvidas em meio a uma significativa transformação observada nas três últimas décadas e fortemente

[16] SAWARIS, Adriana**. Op.Cit**., p. 20.
[17] MENDES, Laura. **Op.Cit**., p. 39.

impulsionadas pelas inovações tecnológicas. A Diretiva europeia de proteção de dados veio para resguardar a liberdade por meio da autodeterminação informativa prevista na “proibição ou na restrição do tratamento de dados sensíveis.”[18]

Nesta mesma perspectiva, é possível constatar que as legislações dos Estados-Membros da Comunidade Europeia foram convergentes acerca da proteção de dados pessoais e da autodeterminação informativa, que foi promovida de maneira eficaz como proteção jurídica necessária para todo seu território. A comunhão da Diretiva da União Europeia e as legislativas nacionais, instituídas na prática, foram o mecanismo ideal de ligação entre o direito da autodeterminação informativa e o tema da proteção de dados pessoais. É de primeira importância, segundo Mendes[19]

> Se referir, neste período, à lei do Reino Unido de 12/07/1984, à lei alemã de 20/12/1990 e à primeira lei de Portugal de 20/04/1991, modificada pela de 26/10/1998, que transpôs a então surgida Diretiva 95/46 do Conselho Europeu. A primeira lei espanhola que disciplinou a matéria foi a de 31/10/1992, revogada pela Lei Orgânica de Proteção de Dados – LOPD – Lei nº. 15 de 13/12/1999 de 13/12/1999, a partir da qual se pretendeu a adequação ao comando da Diretiva Comunitária.

Perante tais leis, é possível constatar que a construção da Diretiva se deu após longos anos e trouxe novidades ao amplificar o objeto da tutela, anteriormente condicionada apenas “à proteção da honra, intimidade pessoal e familiar dos cidadãos, ante o tratamento de dados.”

Essas atualizações foram promovidas pela inserção dos bancos de dados, sendo eles informatizados ou não, em meio ao resguardo da lei da garantia do tratamento dos dados pessoais versus a autonomia da gestão pública, tudo isso diante das garantias fundamentais relacionadas ao âmbito da intimidade.[20]

Já na Itália, a Diretiva 95/46 foi incorporada com a publicação “da Lei n°.675, de 31/12/1996”. Este movimento não buscou apenas uma adequação legislativa, mas promover a centralidade do indivíduo, no sentido singular ou coletivo, indicada por este ordenamento, porém especificamente direcionada a tecnologia informática. O teor deste documento pode ser dividido em duas partes: a primeira, condiz com o “funcionamento da Administração pública em relação a proteção dos direitos dos administrados, sendo esta relativa à liberdade da iniciativa econômica”, a segunda corresponde ao setor privado, ou seja a “pessoa singular ou coletiva”, garantindo os

[18] Ibidem, p. 40.
[19] Ibidem., p. 39.
[20] SAWARIS, Adriana**. Op.Cit**., p. 17.

direitos a liberdade fundamental, a intimidade, a dignidade humana e a identidade pessoal.[21]

Seguindo um contexto histórico e normativo podemos mencionar que, em 07 de dezembro de 2000, foi constituída a Carta dos Direitos Fundamentais da União Europeia, também conhecida como Carta de Nice, que buscou agregar todos os documentos sobre "direitos fundamentais consagrados tradicionalmente nas Constituições dos países Membros. Já o artigo 7º, salienta o cumprimento ao respeito da vida privada e familiar, enquanto o artigo 8º trata da proteção de dados pessoais, de forma a promover um olhar relativo a uma forma "de lesão à intimidade"[22].

É perceptível que a Carta dos Direitos Fundamentais da União Europeia sancionou a autodeterminação informativa como um direito, seguindo a Diretiva e o já consagrado entendimento do Tribunal Constitucional Alemão e as Cartas Magnas da Espanha e Portugal.[23] Nesse período também ocorreu a modificação do Tratado da União Europeia, ocorrido 13/12/2007 no Mosteiro dos Jerônimos, quando se consagrou o Tratado de Lisboa, transformando juridicamente ativa a Carta dos Direitos Fundamentais da União Europeia, neste território, inclusive com a adesão de 27 novos Estados, mesmo que parcialmente Polônia e Reino Unido, tenham reservas quanto a detalhes da proteção de dados. O tratado e a concordância da maioria fomentam a vitória "ao novo direito fundamental que tutela a proteção de dados pessoais, previsto no artigo 16-B do Tratado".[24]

Seguindo a contínua necessidade de protecionismo e diante de um ambiente expansivo de comunicação eletrônica, surgiu, em 12 de junho de 2002 a Diretiva 2002/58/CE[25], que regulamenta a proteção da privacidade e o tratamento de dados pessoais em face dos serviços de prestações de comunicação eletrônicas de acesso público em redes públicas, como a Internet. Nos casos de relação e acesso à rede privada, aplicava-se a Diretiva 95/46 CE.[26]

A Diretiva 2002/58/CE visava garantir a privacidade dos usuários da Internet, atuando como reguladora dos conteúdos e delimitando o prazo do período de

---

[21] Ibidem., p. 17.
[22] Ibidem., p.18**.**
[23] Ibidem, p. 18.
[24] SAWARIS, Adriana**. Op.Cit**., p. 18.
[25] UNIÃO EUROPEIA. Diretiva nº 2002/58/CE, de 12 de julho de 2002. **Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas**. Portugal, 2002. Disponível em: shorturl.at/sH024. Acesso em: 05.05.2020.
[26] SAWARIS, Adriana. **Op.Cit.,** p. 22.

condicionamento dos dados recolhidos e de seu tráfego, além de cobrir a duração, o tempo e o volume dessas comunicações, bem como os dados de localização indicados pelos equipamentos eletrônicos – padronizando os limites de alcance da rede, incluindo o destino final dessas informações. Outra norma surgida nesse formato, criada para abarcar lacunas deixadas pela normativa anterior, é referente a prazos de conservação e localização de dados, como se viu na Diretiva 2006/24/CE[27].

Fica evidente que, antes da existência do Regulamento, o principal meio de normatização da proteção de dados pessoais no continente Europeu eram as diretivas e seus aditivos. Dessa forma, podemos compreender que essa proteção era feita por um "sistema", consagrado por

> diretivas, regulamentos, decisões vinculantes e orientações de diversos níveis hierárquicos, criando um quadro legal de diversas camadas que partem sempre de orientações gerais e estabelecem normas cada vez mais especificas sobre os direitos e obrigações relativos aos dados pessoais.[28]

A principal razão que levou a Diretiva 95/46/CE e as demais ao fracasso reside no fato de que elas não possuíam força normativa dentro dos países-membros da (UE). Mesmo que tenham sido ratificadas, poucos lhes deram força de lei, e dessa forma elas serviam apenas como assistentes norteadoras a seus sistemas jurídicos internos, ou seja, faziam parte de um conjunto de outras normas e diretrizes agrupadas e eram utilizadas para julgar/justificar as sentenças dadas dentro destes países pertencentes ao bloco. Portanto, ela não continha peso normativo, nem dentro da UE, ocorrendo inclusive divergências em sua aplicação mesmo nos países membros. Era utilizada apenas para decisões locais, reconhecida apenas no país julgador, demonstrando a ineficiência da Diretiva frente a um mercado em expansão.

Em meio a esses fatos e ao lapso temporal de praticamente uma década entre as Diretivas e o nascimento do GDPR, a engrenagem mercadológica mundial mais uma vez cresceu e se modificou. Diante dessas modificações sociais advindas das transformações capitalistas, o continente europeu viu uma expansão global das relações mercadológicas em seu território, que foi agravada pela rápida movimentação dos negócios, principalmente nos meios eletrônicos. Podemos citar a

---

[27] UNIÃO EUROPEIA. Diretiva nº 2006/24/CE, de 15 de março de 2006. **Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE.** Portugal, 2006. Disponível em: shorturl.at/vOW15. Acesso em: 15.06.2020.

[28] 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. p. 88.

reflexão do sociólogo Castells sobre a relação íntima entre o sistema capitalista e a tecnologia da informação. Ele menciona que a organização das sociedades humanas é calcada por “relações historicamente determinadas de produção, experiência e poder”.[29] No caso das sociedades modernas, Castells argumenta que elas podem ser consideradas sociedades em rede, isto é, sociedades onde a economia é estruturada em torno das redes de processamento e gerenciamento de informação.[30] Ainda sobre a era da informação, Zygmunt Bauman[31] menciona que a sociedade informacional comete reiteradas violações aos direitos fundamentais devido ao seu controle sobre dados pessoais, fato que leva à vigilância e monitoramento constantes da vida dos cidadãos.

A Europa percebeu que os dados pessoais de seus cidadãos haviam se tornado um produto altamente lucrativo, inclusive com gestão no mercado de valores. Assim, diante dessa engrenagem mercadológica pós-moderna, que se movimenta virtualmente e quase sem fronteiras, ocorreu a reunião da União Europeia junto de seu Conselho e representantes membros com o intuito de desenvolver o texto do Regulamento Geral de Proteção de Dados Europeu – GDPR 2016/679[32], ratificado pelos seus atuais 27 países membros, e que neste contexto veio a revogar assim a Diretiva 95/46/CE. A criação da GDPR - também conhecida pela nomenclatura em português, RGPD - marca uma importante evolução legislativa em relação às diretivas anteriores

Esse conjunto de sistemas aplicados anteriormente passou por uma grande transformação com a aprovação do texto do Regulamento Europeu 2016/679 após a *vacatio legis* de 2 anos, período necessário para a transição e adaptação à nova normativa que veio a vigorar a partir de maio de 2018. Além de ampliar o debate sobre a proteção de dados, ela também agregou tópicos importantes das Diretivas ao seu texto, e é considerada no cenário internacional atual como a normativa de maior abrangência e relevância no tema da proteção de dados pessoais, servindo inclusive como parâmetro para o desenvolvimento de Leis a outros países, a exemplo da brasileira.

---

[29] CASTELLS, Manuel. **A sociedade em rede**: Vol.1. A era da informação: Economia, sociedade e cultura (2 ed.). São Paulo: Paz e Terra, 1999. p. 33

[30] Ibidem, p. 33.

[31] BAUMAN, Zygmunt. **Vigilância Líquida.** Rio de Janeiro: Zahar, 2014. p. 20-25**.**

[32] UNIÃO EUROPEIA. Regulamento nº 679, de 27 de abril de 2016. **Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais [...] e revoga a Diretiva 95/46/CE.** Portugal, 2016. Disponível em: shorturl.at/eAY06. Acesso em: 10.06.2020.

Percebemos, portanto, que a proteção de dados na União Europeia ocorreu de forma gradativa, segundo Mangeth[33]. Inicialmente, a União Europeia previa a proteção de dados mediante a Diretiva 95/46 CE, que disciplinava a coleta, o uso, e o tratamento de dados em todo o seu território. Seguindo demandas globais sobre transferências, apagamento e proteção de dados pessoais, essa diretiva deu origem à elaboração de um documento mais criterioso, isto é, o atual Regulamento Europeu [RGPD], que protege expansivamente os indivíduos.

O surgimento da GDPR visava equilibrar as leis de proteção de dados dos países da (UE) em meio à movimentação de coletas e tratamentos dos dados de seus cidadãos a pessoas jurídicas e aos entes públicos.

Nesse sentido, é relevante compreender como a União Europeia conceitua o termo Regulamento: "são normas vinculativas diretamente aplicáveis a todos os países, incluindo-se aí seus cidadãos e pessoas jurídicas, valendo como se direito nacional fosse."[34]

Nessa fusão estrutural entre a Diretiva 95/46/CE e o Regimento Europeu GDPR, mantiveram-se no contexto tópicos ainda hoje muito relevantes para a efetivação da autodeterminação informativa, que só pode ser colocada em prática pelo Regimento através dos já existentes "princípios e direitos" oriundos da Diretiva. Dessa forma, os indivíduos podem utilizar essas ferramentas como limitadores aos responsáveis pelo armazenamento e tratamento de seus dados – fazendo, assim, com que o cidadão tenha poder de resguardar o máximo possível sua privacidade.

Portanto, os princípios da proteção de dados da RGPD nasceram no contexto histórico das normas de primeira e segunda geração, a partir da década de 60, até aproximarem-se dos direitos fundamentais e da proteção da pessoa, estando vinculados diretamente à proteção de dados e ao efetivo reconhecimento prático da autodeterminação informativa.

Portanto, devemos compreender essas diretrizes protetoras dispostas na atual RGPD considerando os seus princípios de publicidade, exatidão, finalidade, livre acesso e segurança.[35] No Princípio da publicidade (ou transparência) a existência e o

---

[33] MANGETH, Ana Lara. Análise comparativa entre os princípios informadores do regulamento geral de proteção de dados da união europeia e as normas do direito brasileiro**.** In: seminário de iniciação científica e tecnológica da PUC-Rio. **Relatório.** Rio de Janeiro: PUC-Rio, 2018. p. 1-16.

[34] GUIDI, Guilherme Berti de Campos. **Op.Cit**., p. 88

[35] SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies,** 65p. TCC, Curso de Direito, Universidade Federal de Uberlândia, 2018, p. 19.

funcionamento dos bancos de dados se darão por meio de autorização antecipada do estado, incluindo ainda a necessidade de notificação às autoridades quanto a sua existência, cabendo a estes relatórios periódicos para o conhecimento e o livre acesso ao público. O Princípio da exatidão refere-se à necessidade de manter a qualidade dos dados acondicionados, razão da qual, os bancos de dados devem comportar apenas dados verídicos, acarretando a estes, a prioridade de que sua recolha e tratamento sejam feitas com a devida prudência, e não só com o intuito de mantê-los atualizados. No Princípio da finalidade os dados pessoais das quais forem utilizados pelos bancos de dados, tem a obrigação de utilizá-los de maneira correspondente a sua finalidade, da qual, foi acordada junto ao cidadão cedente. Este mecanismo é de suma importância para o processo pratico, pois limita o tomador dos dados a simples possibilidade de transferir os dados pessoais do cidadão a terceiros, diante de uma possível condição de valia para estes conteúdos, movimento da qual fugiria da razoabilidade do uso destes dados, indo contra totalmente a este princípio, demonstrando assim um abuso por parte do tomador. O Princípio do livre acesso determina o livre acesso do cedente a seus dados disponibilizados e armazenados em bancos de dados, assegurando a ele o direito a cópias de seus registros, incluindo a esta liberdade a retificação destas informações, sejam elas errôneas ou desatualizadas, prevendo também possíveis acréscimos ou supressões nestas informações. Fazendo com que o uso deste princípio se vincule diretamente ao princípio da exatidão. O Princípio da segurança (lógica e física) proporciona a proteção de dados, segurança, diante de qualquer risco de transmissão, modificação, extravio ou ainda acesso a eles tanto no meio físico quanto no virtual, de quem quer que seja, das quais não fora consentido.

Esses princípios são facilmente encontrados nas diversas normativas sobre proteção de dados a partir da década de 80. Nesse contexto, eles eram intitulados como *Fair Information Principles*. Porém, só se popularizaram após a Convenção de Strasbourg.[36] Todos estes encontram-se abarcados no Capítulo II, Princípios, Artigo 5.º da GDPR, com o título de Princípios relativos ao tratamento de dados pessoais[37]:

> 1. Os dados pessoais são:
> a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (licitude, lealdade e transparência);

[36] SOUZA, Thiago Pinheiro Vieira de. **Op.Cit**., p. 19.
[37] União Europeia, 2016.

> b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade, com o artigo 89º, nº 1 (limitação das finalidades);
> c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização dos dados);
> d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta a finalidade para que são tratados, sejam apagados ou retificados sem demora (exatidão);
> e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, nº 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados (limitação da conservação);
> f) Tratados de uma forma que garanta sua segurança, incluindo a proteção contra seu tratamento não autorizado ou ilícito e contra sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (integridade e confidencialidade);
>
> 2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no nº 1, e tem de poder comprová-lo (responsabilidade).

Da mesma maneira, a RGPD agregou em seu texto os direitos já mencionados anteriormente dentro da Diretiva 95/46/CE. Isso tornou a GDPR tão expressiva que sua aplicabilidade abrange desde “a coleta de dados pessoais de pessoas naturais” localizadas na União Europeia, como “independentemente de sua nacionalidade, cidadania, domicilio ou residência”, além dos tratamentos de dados efetivados por empresas “de pessoas naturais, localizadas na União Europeia, não importando sua nacionalidade.” [38]

A seguir, faremos um apanhado histórico sobre o contexto em que nasceu a Lei de proteção de dados brasileira e como ocorreu sua tramitação no Congresso Nacional.

[38] MONTEIRO, Renato. **Qual é o impacto direto do GDPR em empresas brasileiras?** 2018. Disponível em: https://cio.com.br/qual-e-o-impacto-direto-do-gdpr-em-empresas-brasileiras/. Acesso em: 20 maio 2020.

2.3 O nascimento da LGDP

Seguindo o objetivo de fazer uma análise comparativa entre a legislação brasileira e a europeia neste momento pela análise das transformações históricas, passaremos a abordar o contexto da proteção de dados no Brasil. De acordo com Mangeth[39], o legislador brasileiro foi moroso ao tratar da lei de proteção de dados, posicionando-se de forma defasada em relação a outros países sul-americanos[40] que já possuíam legislação versando sobre a proteção de dados. Entretanto, o vazamento de dados causada pela agência *Cambridge Analytica* e a efetivação da GDPR, propiciaram o Legislativo a encaminhar, em 2018, dois projetos de lei.

Inicialmente, foram encaminhados os projetos do Senado (nº 330/2013) e da Câmara (nº 5.276/2016), que foram divergentes em suas proposições diante da amplitude e sobre o controle da proteção de dados dos titulares, bem como sobre seus princípios. Esses projetos de lei também divergem ante a atuação do Poder Público acerca da coleta e tratamento dos dados, bem como quando se considera a possibilidade da concepção de uma Autoridade de Proteção de dados pessoais.

Da mesma forma, a Constituição Federal de 1988 apresenta, nos seus direitos fundamentais, expostos no artigo 5º, a proteção da intimidade e da vida privada, almejando a proteção e dignidade da pessoa humana:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas,
> assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...].[41]

Entretanto, Mangeth[42] afirma que a proteção de dados pessoais já estava claramente prevista na Constituição de 1988 no texto do artigo 5º, inciso X, ao estabelecer a inviolabilidade da intimidade e da vida privada.[43] Ainda de acordo com as autoras supracitadas,[44] outro mecanismo de proteção que antecedeu a Lei de

---

39. MANGETH, Ana Lara. **Op.Cit.,** p. 3.
40 Vide Tabela I.
41 BRASIL. **Constituição da República Federativa de Brasil, de 5 de outubro de 1988.** Diário Oficial da União, Brasília, DF, Outubro de 1988. Disponível em: shorturl.at/fkJY2. Acesso em: 20.05.2020.
42 BRASIL, 1988.
43 BRASIL. Lei nº 12.965, de 23 de Abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Brasília, DF, 2014. Disponível em: shorturl.at/ipqEU. Acesso em: 20.05.2020.
44 MANGETH, Ana Lara. Op.Cit., p. 4.

proteção de dados no Brasil foi o Marco Civil da Internet[45], promulgado em 2014, cujo objetivo é a proteção dados em forma de princípios. Por exemplo: o artigo 3º, inciso II, apresenta princípios como a proteção da privacidade, normatizando o uso da Internet e tratando especificamente da proteção de dados pessoais em seu inciso III: "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei.

Ainda que o Marco Civil em 2014 parecesse inovador e muito aguardado, e tenha se portado como a primeira norma mundial a versar sobre "direitos e deveres dos usuários da rede, ainda não se perceberá mudanças substanciais, uma vez que esta não acrescentou praticamente nada à legislação vigente", segundo Tomasevicius Filho[46]. Ademais, segundo este autor, a interpretação foi empregada de forma equivocada, pois os dispositivos da Constituição Federal, do Código Civil, do Código Penal, dos Códigos de Processo Civil e Penal, do Código de Defesa do Consumidor, do Estatuto da Criança e do Adolescente e da lei sobre interceptação de comunicações (Lei n.9.296/96), não teriam aplicação nas relações jurídicas estabelecidas na internet.[47] O legislador brasileiro, de acordo com Tomasevicius Filho[48], toma uma postura ingênua ao postular que uma lei tentasse resolver uma problemática de proporção mundial utilizando-se apenas dos efeitos extraterritoriais. A internet, entretanto, não possui fronteiras e assim vindo a colaborar com as violações dos direitos dos cidadãos, deixando facilmente para trás os efeitos da jurisdição brasileira.

Dois anos depois da aprovação da MCI, surgem dois projetos de lei que seguem para Senado Federal. O PL nº 5.276/2016 aguardava a aprovação no Senado para seguir para promulgação do Presidente da República. No entanto, o projeto não foi aprovado após vasto debates entre o Senado e a Câmara, o que caracterizou um ganho social tendo em vista os textos mais criteriosos previstos nos Projetos de Lei nº 4.060 e 5.276. E só após esse processo, em 10 de julho de 2018, foi aprovado no plenário do Senado o Projeto de Lei nº 53, o que representou um marco legal para

---

[45] BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília**. 2014. Disponível em: shorturl.at/diqs5. Acesso em: 20.05.2020.

[46] TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, [s.l.], v. 30, n. 86, p. 269-285, abr. 2016. FapUNIFESP (SciELO). Disponível em: shorturl.at/axILX. Acesso em: 20.05.2020.

[47] TOMASEVICIUS FILHO, Eduardo. **Op.Cit.,** p. 274

[48] Ibidem., p. 276., 2016.

nosso país sobre esse tema. A autora indica, ainda, que já a PL nº 53 tinha, inicialmente, fortes semelhanças com a GDPR, como vemos no artigo 6º: "o caput, inicia a ideia determinando que a boa-fé deve guiar todas as atividades de tratamento de dados pessoais".[49] Quando comparamos a PL nº53 e o GDPR, percebemos que o legislador brasileiro trouxe para a normativa um forte reflexo do texto europeu. Assim, deu-se origem à atual Lei Geral de Proteção de Dados 13.709 (LGPD), promulgada em 14 de agosto de 2018.

A LGPD nasceu com o objetivo de proteger os dados pessoais no território brasileiro. A lei visa assegurar a privacidade e os dados pessoais "dos cidadãos, determinando como as empresas, organizações e poder público deverão coletar, usar, processar e armazenar esses dados no desempenho de suas atividades"**[50]**. Ela estava inicialmente prevista para entrar em vigor 24 meses após a publicação, isto é, em 20 de agosto de 2020; no entanto, foi prorrogada para 3 de maio de 2021, com a edição da Medida Provisória 959 de 2020, que alterou a redação do artigo 65, inciso II.**[51]**

A proteção de dados brasileira foi influenciada pela RGPD**[52]**, que passou a vigorar em 25 de maio de 2018. A lei brasileira inovará radicalmente a maneira como a privacidade é concebida no cenário nacional. A LGPD concede às pessoas físicas – chamadas de titulares dos dados – maior poder sobre o manejo de seus dados pessoais. A LGPD também aderiu à autodeterminação informativa, o que significa que o titular possui controle e autonomia sobre a metodologia e o destino do processamento de suas informações pessoais.[53]Os limites da lei brasileira, em conformidade com a normativa internacional, permitirão coletar, usar, processar e armazenar os dados pessoais dos titulares de forma mais criteriosa. Assim como o Regimento Europeu, a Lei brasileira de proteção de dados se baseia em princípios. Conforme Perongini[54], são princípios que visam reger a proteção de dados pessoais,

---

[49] BRASIL. Projeto de Lei nº 53/2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014.** Brasília, 2018.

[50] PROMULGADA a Lei no 13.709/2018, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD). **Lefosse Advogados.** 2018, 13p. Disponível em: https://lefosse.com/newsletters/promulgada-lei-n-13-709-2018-lei-geral-de-protec%cc%a7a%cc%83o-de-dados-pessoais-lgpd/. Acesso em: 5.jun.2020.

[51] BRASIL. Medida Provisória nº 959. [...] **Prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD.** Brasília, 2020. Disponível em: shorturl.at/PRVX0. Acesso em: 20.05.2020.

[52] LEFOSSE Advogados. **Cit.Op**., p. 1.

[53] BRASIL. Lei nº 13709/2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, 2018. Disponível em: shorturl.at/rwGNV. Acesso em: 20.05.2020.

[54] PERONGINI, Maria Fernanda. **Pequeno guia sobre a Lei Geral de Proteção de Dados:** uma breve análise sobre a nova lei brasileira de proteção de dados pessoais. Rio de janeiro, 2018, 18 p.

garantindo os direitos das pessoas e estabelecendo normas objetivas para os procedimentos efetivados por instancias públicas/privadas do tratamento de dados pessoais. Exemplo disso é o princípio que trata do compromisso do controlador de dados, que possui responsabilidade pelas decisões quanto ao tratamento de dados pessoais. Ele tem o dever de comprovar que o processamento será executado dentro dos parâmetros legais da LGPD, e com a devida prestação de contas ao cidadão. Tal norma expressa uma visão de privacidade e respeito desde os primórdios dos serviços/produtos. Nesse sentido, devemos promover uma certa atenção aos princípios elencados no artigo 6º, incisos I, II, III, IV, V, VI, VII, VIII, IX e X da LGPD:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.[55]

Assim, é possível observar o interesse do legislador em englobar o texto da RGPD na lei brasileira. Da mesma forma, é nítido que a legislação tem, como meta, a

55 BRASIL, 2018.

proteção dos cidadãos através da conscientização sobre o uso e armazenamento de dados pessoais. Cabe ressaltar que a LGDP não se encontra finalizada, pois possui parâmetros a serem abordados. Quando trata de regulação e fiscalização, por exemplo, ou quando trata de introduzir uma Autoridade Nacional de Proteção de Dados, assim como quando visa instituir um Conselho auxiliar cujo objetivo é indicar estratégias e diretrizes que foram vetadas pelo Governo, pois apenas o poder executivo pode criar tal figura. Percebemos, portanto, que essas temáticas precisam ser incluídas na pauta de debates das instituições – e temos diversas questões em aberto, sem que a normativa tenha sequer entrado em vigor. Isso indica uma provável dificuldade por parte das empresas em enquadrar-se na LGPD[56].

Perongini[57] também destaca que a LGPD é uma ferramenta importantíssima para o crescimento econômico digital em nosso país, pois promove a proteção dos direitos dos cidadãos através de uma legislação ativa e específica que veio para complementar toda estrutura legal vigente. Ela é, sobretudo, uma boa ferramenta para o mundo empresarial, pois nossas vidas giram em torno da produção ativa de dados. Seja ao recebermos materiais de propaganda, chamados marketing digital, como as de bancos, comércios e até do governo, todos esses serviços e produtos promovem coleta e análise de dados pessoais. Ou seja, todas as compras, reservas ou informações enviadas geram mais dados pessoais processados ou armazenados, aos quais são somadas novas informações que atualizam e dão movimento a esse grupo de dados.

A autora indica, também, a existência de dados pessoais utilizados ilicitamente para beneficiar ou prejudicar eleições. A verificação destes dados e a dinâmica de decisões algorítmicas pelo setor público promovem discriminação ou, ainda, avaliações errôneas dos dados, indicando que a problemática do uso e controle de dados pessoais é um tema pertinente no século XXI, pois “como cidadãos digitais, somos cada vez mais perfilados e categorizados de acordo com os dados que produzimos.”[58]

A internet atingiu níveis de sofisticação e amplitude que ensejam o surgimento de legislações relacionadas ao uso dos dados pessoais, devido ao fato da estrutura digital ser facilmente acessível e norteada pelo processamento de informações. Além

[56] PERONGINI, Maria Fernanda. **Op.Cit.,** p. 2.
[57] PERONGINI, Maria Fernanda. **Op.Cit.,** p. 2.
[58] Ibidem., p. 2

disso, nossa necessidade tecnológica movimenta abundantemente essa demanda por dados, o que faz a LGPD ser uma normativa direcionada a conceder aos cidadãos maior controle sobre seus dados pessoais, vindo a facilitar o acesso para empresas e usuários e, assim, promover a economia digital. [59]

A nova legislação, que entrará em vigor em agosto de 2020, também traz consigo importantes repercussões em nosso sistema econômico, bem como em sistemas de negócios voltados para o tratamento de dados pessoais. É o caso de instituições financeiras, hotéis, agências de turismo, hospitais, planos de saúde, farmácias, restaurantes, varejistas, universidades, provedores de serviços de internet, prestadores de serviços de telecomunicações, empresas de tecnologia, provedores de serviços de computação em nuvem, agências de publicidade, escritórios de advocacia, órgãos públicos e dentre outras. Além disso, a nova Lei também afetará diretamente as relações entre fornecedores de produtos e serviços e seus clientes, relações de consumo, relações entre empregadores e seus empregados, dentre outras relações que impliquem coleta e tratamento de dados, tanto no ambiente online como offline.[60]

A LGPD, assim como a GDPR, possui utilização extraterritorial, atingindo até mesmo empresas estrangeiras desde que possuam filial ou subsidiária em território nacional, assim como oferte seus bens ou serviços no Brasil, ou ainda recolha dados pessoais de cidadãos localizados em âmbito nacional. Segundo Perongini,[61] um dos aspectos mais relevantes da LGPD e sua extraterritorialidade é que a sua repercussão versa por movimentar diversas esferas da economia, no âmbito das “entidades públicas ou privadas, online ou offline, da P&D ao marketing, de clientes a empregados, de serviços à indústria”.[62] Esta previsão está diretamente ligada sob a égide da letra da Lei brasileira, constando no texto: Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que**:**

> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

[59] Ibidem., p. 3.
[60] LEFOSSE Advogados. **Op.Cit**., p. 2.
[61] PERONGINI, Maria Fernanda. **Op.Cit.,** p. 3.
[62] Ibidem., p. 3.

> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei[63].

Portanto, a lei brasileira caminha diretamente com a territorialidade da RGPD da União europeia, expandindo sua efetivação a outras pátrias. Fazendo com que a LGPD considere não apenas o território nacional, mas outros locais aonde os titulares ou os dados possam se encontrar. Ou seja, para aplicar a LGPD, basta que os dados sejam coletados ou processados em território brasileiro, ou que o tratamento seja direcionado a oferecer bens ou serviços a titulares estabelecidos dentro de nosso território nacional. Como exceção, devemos mencionar o texto da LGPD, que indica alguns dispositivos que não sofrerão tratamento pela Lei Geral de Proteção de dados pessoais, das quais encontram-se dispostos no Artigo 4º da referida norma, dentre eles:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III

63 BRASIL, 2018.

> do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público[64].

O desenvolvimento histórico exposto anteriormente serve para demonstrar o verdadeiro desafio de analisarmos comparativamente estas legislações sob a ótica de suas semelhanças e diferenças no capítulo III, que aparece tanto na Lei brasileira quanto no Regimento europeu, e aborda as regras dos Direitos dos Titulares de Dados - que será o objeto de nosso cotejo partindo sempre do ordenamento brasileiro para o europeu. Esse capítulo confere todos os direitos a serem exercidos e protegidos pelas normas quanto aos titulares dos dados, dentre eles: consentimento; acesso; transparência; anonimização; revogação e outros cuja aplicabilidade será trabalhada nas próximas seções desse trabalho. Como vivemos na era da informação, é essencial que aliemos o princípio de liberdade de acesso ao princípio da dignidade humana, um dos fundamentos que dá sustentação ao ordenamento jurídico do Brasil, como exposto no artigo 1º da CRFB/88.[65] É importante que o tratamento dos dados considere tanto a identidade social quanto individual dos usuários, a fim de conhecer quais métodos de proteção são adequados de acordo com as especificidades de cada indivíduo.

Os riscos de termos nossos dados expostos em diversas plataformas virtuais incluem o seu uso político, econômico e social por parte do Estado, fato que evidencia o cunho autoritário do controle de informações sem o conhecimento do usuário. Rodotá[66] menciona a imagem do “homem de vidro”, cuja origem é associada à ascensão do nazismo na Alemanha. Nesse sentido, o homem de vidro seria a representação dos cidadãos no mundo da tecnologia: transparentes, para que assim o Estado tenha conhecimento e controle sobre suas dimensões mais íntimas. Na obra A Vida na Sociedade da Vigilância, lançada em 2001, o autor supracitado já apontava para a necessidade de implementação de um órgão regulatório capaz de completar o sistema de proteção de dados. Esse órgão teria a função controlar as plataformas de

---

[64] BRASIL, 2018.
[65] Brasil, 1988.
[66] RODOTÀ, Stefano. **A vida na sociedade de vigilância:** Privacidade hoje. *apud* COSTA, Mariana Monteiro. **Op.Cit**., p. 11.

captação de dados, impedindo abusos e ilicitudes.[67] Costa[68] aponta, por fim, "que devemos refletir sobre a existência de padrões éticos nas escolhas da Inteligência Artificial", pois os algoritmos são produzidos por seres humanos – portanto, são passíveis de erro e fundamentais para a estruturação da moral da sociedade moderna. Em referência a Bauman, a autora diz que há uma tendência de "eufemização da culpa" devido à distância entre os sujeitos e o processo decisório.

A coleta e o armazenamento de informações têm sido utilizados para fundamentar decisões relevantes e de foro íntimo sobre os próprios usuários sem que eles tomem conhecimento desse fato. O tema é, portanto, complexo, e a legislação não se deve limitar à proibição que decisões sejam tomadas fazendo uso apenas dos perfis automáticos – é preciso avaliar o comportamento humano. Se faz necessário um conceito positivo de direito à informação, no sentido de que o titular deve ter a possibilidade de apreender e julgar o tratamento de suas informações.[69]

Rodotà *apud* Mariana Costaf[70] argumenta que os cidadãos poderiam sofrer uma perda cognitiva devido à automatização de perfis, cuja consequência é a penalização dos que não se enquadram nos perfis gerais. Isso acarretaria em um processo de exclusão de minorias, e anula a capacidade de percepção das sutilezas e das preferências não-habituais. Como a interação entre a coleta e o processamento de dados é complexa, ela dá origem a novas dinâmicas de uso para essas informações. Através de determinados dados, é possível obter novas informações tais como perfis de consumo, análises de preferência e dados estatísticos. Devido à possibilidade de interesse nesses dados por parte de terceiros, eles podem ser comercializados.[71] Segundo Rodotá *apud* Mariana Costa:

> Assim, se torna possível não só um controle mais direto do comportamento dos usuários, como também a identificação precisa e atualizada de certos hábitos, inclinações, interesses, preferências. Daí decorre a possibilidade de uma série de usos secundários dos dados, na forma de "perfis" relacionados aos indivíduos, famílias, grupos. Trata-se de uma nova "mercadoria" cujo comércio pode determinar os tradicionais riscos para a privacidade: mas pode, sobretudo, modificar as relações entre fornecedores e consumidores de bens e serviços, reduzindo a autonomia destes últimos de tal forma

[67] Ibidem., p. 86
[68] COSTA, Mariana Monteiro. **Op.Cit.,** p. 30
[69] COSTA, Mariana Monteiro. **Op.Cit.,** p. 31
[70] RODOTÁ, Stefano**. Op.Cit**. *apud* COSTA, Mariana. **Op.Cit.,** p. 59.
[71] COSTA, Mariana. **Op.Cit.**, p. 59

> que pode chegar a incidir sobre o modelo global de organização social e econômica.[72]

O desenvolvimento histórico exposto anteriormente serve para demonstrar o verdadeiro desafio de analisarmos brevemente porém comparativamente estas legislações sob a ótica de suas semelhanças e diferenças no capítulo III, que aparece tanto na Lei brasileira quanto no Regimento europeu, e aborda as regras dos Direitos dos Titulares de Dados - que será o objeto de nosso cotejo partindo sempre do ordenamento brasileiro para o europeu. Esse capítulo confere todos os direitos a serem exercidos e protegidos pelas normas quanto aos titulares dos dados, dentre eles: consentimento; acesso; transparência; anonimização; revogação e outros cuja aplicabilidade será trabalhada nas próximas seções desse trabalho.[73]

---

[72] RODOTÁ, Stefano**. Op.Cit**. *apud* COSTA, Mariana. **Op.Cit.,** p. 59.

[73] Art. 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência
IX - agentes de tratamento: o controlador e o operador;
X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

A análise comparativa que será feita a seguir utiliza os títulos apresentados pelas normas do regimento europeu como parâmetro de verificação de sua existência na norma brasileira, porém o ponto de partida será o contexto da norma nacional em relação à Lei europeia.

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;
XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Medida Provisória nº 869, de 2018)
XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.
XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.
XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

3 DIREITO À INFORMAÇÃO E ACESSO AOS DADOS PESSOAIS

3.1 Transparência e regras para exercício dos direitos dos titulares dos dados

Considerando estes dados históricos anteriormente mencionados, é possível perceber que a proteção de dados é um direito em desenvolvimento e de suma importância - importância esta que foi concebida pelos países do continente europeu em suas práticas jurídicas desde a década de 1970, como já mencionado. Ainda assim, diante deste quadro, é difícil conseguir definir com exatidão o início do debate sobre proteção de dados pessoais, pois ele se desenvolveu gradualmente e sofreu ajustes devido à necessidade de atualização tecnológica.[74]

É nesse contexto que Mayer-Schönberger[75] conjectura questões éticas quanto à liberdade e a dificuldade que o indivíduo pode enfrentar para efetivar seu direito à privacidade e à proteção de dados pessoais:

> A proteção de dados pessoais como liberdade individual pode proteger a liberdade do indivíduo. Ela pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo que se tem de pagar por isso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas? Será que nós alcançamos o estágio ótimo da proteção de dados se garantirmos os direitos à privacidade que, quando exercidos, acarretarão a exclusão do indivíduo da sociedade?

É necessário compreender como esse direito é abordado nas duas normativas, porém sob títulos diferentes: o Regimento europeu o intitulou de “Transparência e regras para este exercício dos direitos dos titulares dos dados; já na lei brasileira, o termo utilizado é a “Titularidade de seus dados pessoais”. Trata-se do mesmo significado: garantir aos titulares dos dados o direito à proteção, sobretudo no que diz respeito às regras e à necessidade de clareza de todo processo executado com seus dados.

A Lei brasileira institui no seu Art. 17 que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei”[76]. Ou seja, indica que a titularidade do cidadão sobre seus dados pessoais é garantida por essa lei, em comunhão com direitos já postulados em nossa Magna Carta. Ao observar os direitos à informação e acesso aos dados pessoais referentes à transparência e às regras para o exercício dos direitos dos titulares, encontramos as diferenças e as sutis

[74] MENDES, Laura. **Op.Cit.** p. 33
[75] MAYER-SCHÖNBERGER. 2001, p. 228. *apud* Ibidem, p. 36.
[76] BRASIL, 2018.

semelhanças entre a norma nacional e o Regimento europeu. No contexto da titularidade, é possível verificar a origem da existência de semelhanças entre o Art. 18, inciso II, da LGPD[77], e o artigo 12º da RGDP[78], onde ambos os regimentos asseguram que o titular tenha garantido o acesso aos seus dados tratados. No entanto, o referido artigo apresenta apenas uma indicação no inciso I referindo-se ao direito do titular de obter do controlador a "confirmação da existência de tratamento dos dados".[79] Na RGPD, pode-se perceber que o título "transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados" encontra-se especificado a partir do item 1 do artigo 12[80], estabelecendo que

> o responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.o e 14.o e qualquer comunicação prevista nos artigos 15.o a 22.o e 34.o a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrônicos. Se o titular dos dados solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.
> 2. O responsável pelo tratamento facilita o exercício dos direitos do titular dos dados nos termos dos artigos 15.o a 22.o. Nos casos a que se refere o artigo 11.o, n.o 2, o responsável pelo tratamento não pode recusar-se a dar seguimento ao pedido do titular no sentido de exercer os seus direitos ao abrigo dos artigos 15.o a 22.o, exceto se demonstrar que não está em condições de identificar o titular dos dados.
> 3. O responsável pelo tratamento fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos artigos 15.o a 20.o, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento informa o titular dos dados de alguma prorrogação e dos motivos da demora no prazo de um mês a contar da data de receção do pedido. Se o titular dos dados apresentar o pedido por meios eletrónicos, a informação é, sempre que possível, fornecida por meios eletrónicos, salvo pedido em contrário do titular.
> 4.Se o responsável pelo tratamento não der seguimento ao pedido apresentado pelo titular dos dados, informa-o sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial.

[77] Brasil, 2018
[78] União Europeia, 2016
[79] BRASIL, 2018
[80] UNIÃO EUROPEIA, 2016.

> 5.As informações fornecidas nos termos dos artigos 13.o e 14.o e quaisquer comunicações e medidas tomadas nos termos dos artigos 15.o a 22.o e 34.o são fornecidas a título gratuito. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento pode:
> a) Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; ou
> b) Recusar-se a dar seguimento ao pedido.
> Cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.
> 6.Sem prejuízo do artigo 11.o, quando o responsável pelo tratamento tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta o pedido a que se referem os artigos 15.o a 21.o, pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados.
> 7.As informações a fornecer pelos titulares dos dados nos termos dos artigos 13.o e 14.o podem ser dadas em combinação com ícones normalizados a fim de dar, de uma forma facilmente visível, inteligível e claramente legível, uma perspetiva geral significativa do tratamento previsto. Se forem apresentados por via eletrónica, os ícones devem ser de leitura automática.
> 8. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 92.o, a fim de determinar quais as informações a fornecer por meio dos ícones e os procedimentos aplicáveis ao fornecimento de ícones normalizados.

Podemos iniciar a verificação para compreender como é elaborado o direito à transparência das informações e comunicações na RGPD, além de observarmos como as regras devem ser aplicadas para o exercício dos direitos dos titulares dos dados, mostrando a existência do direito à titularidade muito bem assegurada pela norma europeia. É perceptível que o responsável pelo tratamento dos dados deve fornecer diversas informações ao titular dos dados mediante requisição, sem demora injustificada e dentro de um prazo estipulado pelo regimento. A Lei ainda indica que essas informações serão fornecidas gratuitamente, e algumas outras especificações mais técnicas que não iremos abordar. Da mesma forma, percebemos que, em ambas as normas, encontramos o direito à titularidade, porém a letra da norma brasileira é extremamente enxugada e lacunosa no que diz respeito a titularidade, não especificando o que tal direito abarca e, ainda, considerando como medidas protetivas outros dispositivos constitucionais já garantidores dos direitos dos cidadãos brasileiros, mas não todos os que devem ser abarcados para o exercício do direito dos titulares dos dados, cidadãos que a Lei deve proteger. É possível que a indicação dos direitos fundamentais como liberdade, intimidade e privacidade consiga abarcar todos os indivíduos atingidos pela Lei nacional? Será que podemos fazer uma análise

comparativa entre essas regras diante da mísera proteção da letra da Lei brasileira contra o Regimento europeu, muito mais dinâmico e em acordo com as necessidades sociais atuais, cujo cerne é proteger seus titulares? A legislação europeia é mais reguladora e abrangente a todos os envolvidos, pois prevê o direito de extraterritorialidade de forma mais detalhada do que a Lei brasileira, pois atinge os direitos de titulares dentro e fora do seu território. A GDPR aponta que esses direitos devem ser garantidos de forma concisa, transparente e centralizada ao tema da proteção de dados pessoais, afinal eles são entes incorpóreos, que ficam resguardados em nuvens ou bancos de dados espalhados pelo mundo.

Se observarmos os mesmos temas nos artigos da LGDP, é possível apontar diferenças entre eles e as da RGDP. Mesmo que a legislação brasileira tenha se espelhado no Regimento europeu, a letra da lei nacional não especifica tão criteriosamente o direito à transparência das informações nem as regras para o exercício dos direitos dos titulares, intitulado na norma brasileira como titularidade, que deve indicar as medidas tomadas pelo responsável com relação ao titular. Já a RGPD não apenas determina que o responsável pelo tratamento tome medidas adequadas quando requisitado, mas também define medidas e impõe o prazo de um mês a contar da data de recepção do pedido. A única novidade que podemos verificar está no artigo 18 da Legislação brasileira, em seu parágrafo 8º, quando prevê o exercício do direito de acesso aos dados perante os órgãos de defesa do consumidor, ou seja, em caso dessa lei não abranger e sanar a lide fica indicado buscar a proteção do Código de Defesa do Consumidor – CDC, subsidiariamente buscando resolver o conflito.

Na seção a seguir, desenvolveremos mais uma análise comparativa entre a Lei brasileira e o Regimento europeu, dessa vez tratando sobre como ambas as normas abordam os dados pessoais recolhidos junto do titular.

3.2 Dados pessoais recolhidos junto do titular

Laura Mendes[81] aponta que, mesmo diante do histórico citado acima, o mais elementar aspecto das normas de segunda geração está na viabilidade de atuação do cidadão, através de seu consentimento, na coleta e processamento de seus dados, permitindo a livre tomada de decisão individual sobre o destino de dados pessoais.

---

81 MENDES, Laura. **OpCit**., p. 36.

Mais uma importante modificação trazida por esta nova geração surgiu na esfera institucional, que potencializou a atuação das autoridades administrativas responsáveis pela proteção de dados e pela garantia ao direito à privacidade. Assim também sustenta Mayer-Schönberger[82]:

> Primeiramente, algumas das instituições de segunda geração não apenas investigavam as ofensas à proteção de dados pessoais, mas também se tornaram uma espécie de ombudsman da proteção de dados pessoais para os cidadãos. Quando os direitos individuais eram violados, os cidadãos deveriam poder se reportar a alguma instituição – uma instituição que de algum modo poderia ajudá-los a reforçar o direito individual à proteção de dados pessoais. Segundo algumas das instituições de segunda geração transformaram-se em órgãos adjudicatórios que concediam opiniões de como a burocracia poderia ou não interpretar as normas de proteção de dados pessoais.

No entanto, é importante refletir sobre a segunda geração das leis de proteção de dados pessoais e o conflito quanto à eficiência prática do consentimento dos cidadãos e o concreto desempenho de seu direito de liberdade e escolha, pois o cidadão pode ser privado de certos direitos caso se negue a compartilhar seus dados com o governo, mercado e particulares. Isso indica que, no Estado Social, "existem dificuldades para manter a chamada liberdade informacional de forma incólume, sem interferir nas engrenagens dessa máquina burocrática alimentada por dados de seus cidadãos. Em contrapartida, entre os privados é penoso validar a pratica do direito à privacidade informacional, pois coloca o indivíduo na mesma condição anterior de privação, porém, podendo dificultar o seu acesso no mercado de consumo, onde a moeda de troca entre fornecedores e clientes, são os seus registros de informações pessoais".[83]

O início da terceira geração foi determinado pela sentença do Tribunal Constitucional Alemão em 1983, ao declarar a inconstitucionalidade da "Lei do Censo", de 1982, que exigira que seus cidadãos viabilizassem diversas informações pessoais sem nenhuma garantia de que esses dados estariam seguros.[84] Então, a Corte reapreciou a Lei Federal Alemã sobre proteção de dados pessoais sob a ótica de Bonn e determinou que os indivíduos têm o direito "à autodeterminação informativa"[85] e à aprovação do processamento de seus dados pessoais. O termo "autodeterminação informativa" foi utilizado, de forma pioneira, pelo Tribunal Federal

---

82 MAYER-SCHÖNBERGER. 2001, p. 228. *apud* Ibidem., p. 36.
83 MENDES, Laura. Ibidem., p. 36.
84 MENDES, **Op.Cit**., p. 37.
85 SAWARIS, Adriana. **Op.Cit.**, p. 15.

Constitucional Alemão, que julgou inconstitucional a Lei do Recenseamento em 1983. A Lei Fundamental alemã não continha expressa a previsão do direito fundamental de o indivíduo não autorizar o uso não consentido da informática para processamento de seus dados – que podem expor sua filiação política e convicções filosóficas; no entanto, o Tribunal reconheceu um direito de origem constitucional que protege esses interesses.[86]

A lei do Censo autorizava uma irrestrita coleta de dados da população alemã através de um diversificado questionário de 160 perguntas, que tinha como objetivo compilar padrões estatísticos para desenvolver práticas administrativas que não foram determinadas na letra da lei. Além disso, havia ameaça de coerção para quem não respondesse ao questionário, e o cidadão poderia vir a sofrer uma alta punição pecuniária.[87]

A partir desses achados teóricos, podemos concluir que o Tribunal considerou inconstitucional a Lei do Censo alemão e aplicou como direito constitucional a autodeterminação informativa, dando sentido estrutural aos fundamentos da proteção de dados na Alemanha, como vemos no trecho abaixo, retirado da própria decisão:

> Não se pode levar em consideração somente a natureza das informações; são determinantes, porém, a sua necessidade e utilização. Estas dependem em parte da finalidade para a qual a coleta de dados é destinada, e de outra parte, da possibilidade de elaboração e de conexão próprias da tecnologia da informação. Nesta situação, um dado que, em si, não aparenta possuir nenhuma importância, pode adquirir um novo valor; portanto, nas atuais condições do processamento automático de dados, não existe mais um dado 'sem importância'.[88]

A resposta dada pelo Tribunal diz respeito ao desenvolvimento livre da personalidade humana, que deve ser mantida afastada das ingerências externas; portanto, a decisão do Tribunal foi responsável por evitar o controle social imposto aos cidadãos devido aos riscos de invasão da privacidade individual. Menke[89] argumenta que o direito à autodeterminação informativa, enquanto base constitucional da proteção de dados, faz parte do chamado direito geral da personalidade, que vem

---

[86] NAVARRO, Ana Maria Neves de Paiva. O direito fundamental à autodeterminação informativa. Rio de Janeiro: **LETACI**, 2012. p. 11. Disponível em: http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c. Acesso em: 20.05.2020.

[87] Ibidem., p. 15.

[88] FROSINI, Vittorio. Contributi ad un diritto dell'informazione. Napoli: Liguori, 1991. *apud* COSTA, Mariana Monteiro. **Op.Cit.,** p. 40.

[89] COELHO, Alexandre; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgangs (org.). **Op.Cit.,** p. 209.

sendo aperfeiçoado pelo Tribunal Constitucional Federal desde a década de 50 e é "derivado da combinação do artigo 1º, §1º (dignidade da pessoa), e art. 2º §1º (liberdade) da Lei Fundamental"[90]. Portanto, sua ação conjunta assegura a cada cidadão a possibilidade de construir sua própria personalidade.

Cabe ressaltar que, mesmo a norma alemã não reconhecendo ainda como direito fundamental de se opor ao uso não permitido de seus dados pessoais, o Pleno não se viu impedido de legitimar a "existência de um direito constitucional e a sua respectiva tutela desses interesses." Dessa forma, a lei alemã ressaltou com essa decisão o conceito da autodeterminação informativa, aplicando o direito previsto nos artigos 1º e 2º da Constituição Alemã que alude aos direitos da dignidade da pessoa humana e o direito à liberdade, e, portanto, consentiu que estes direitos fossem refutados diante do Estado.[91]

O Tribunal também reconheceu que a referida autodeterminação informativa tem origem em uma participação mais abrangente do cidadão neste processo do que constava nos indicativos das antigas normas de proteção de dados pessoais. Isso pode ser observado pela diferença entre a segunda e a terceira geração: justamente o fato de que o envolvimento dos indivíduos deveria de ser ininterrupto em todo o procedimento, da coleta ao armazenamento e à transmissão dos dados.[92] Contudo, após essa decisão, a autodeterminação informativa permitiu que o cidadão exercitasse um domínio diante da prática do recolhimento, divulgação e utilização de seus dados pessoais. Esse direito só poderia ser limitado diante do interesse público, considerando apenas o princípio da proporcionalidade. Por isso, a Corte argumenta que o direito à privacidade pode entrar em conflito com os demais direitos fundamentais, algo que não deve ocorrer.[93]

No mesmo contexto, durante a década de 80, viu-se uma modificação relevante no contexto científico a partir do surgimento de novas tecnologias de rede e telecomunicação, que potencializaram a capacidade de transmissão de dados. Isso fez com que não fosse mais possível detectar a localização destas centrais de processamento pois eles passaram a ficar acondicionados em redes, permitindo que

[90] COELHO, Alexandre; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgangs (org.). **Op.Cit.,** p. 209.
[91] SAWARIS, Adriana. **Op.Cit**., p. 15
[92] MENDES, Laura. **Op.Cit.**, p. 37.
[93] SAWARIS, Adriana. **Op.Cit**., p. 15

os dados sejam transferidos em segundos.[94] No mesmo período, também foram aprovadas as leis de proteção de dados em países como Alemanha, Áustria, Noruega e Holanda.[95]

A participação dos cidadãos no controle de suas informações pessoais não logrou êxito na prática como idealizava a segunda geração – muitos não foram capazes de arcar com o custo de terem que buscar seus direitos e com as consequências ao serem impedidos de obter seus bens, serviços e benefícios sociais. Além disso, após consentir com o uso de seus dados pessoais, o cidadão não teria direito a reparação judicial em caso de violação de sua privacidade ou mau uso das informações por ele fornecidas.[40][96]

A norma brasileira não se menciona diretamente aos dados pessoais recolhidos junto do titular, mas traz as seguintes diretrizes no texto do Art. 3º:

> Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: ... III - os dados pessoais objetos do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.[97]

Fica evidente que o local onde os dados pessoais tenham sido coletados deve ser parte do território nacional, porém a norma não é taxativa quando explicita que esses dados tenham sido recolhidos junto ao titular, restando dúvidas quanto ao recolhimento consentido junto ao titular dos dados. Ao observarmos a letra da Lei no texto que trata dos requisitos para o tratamento dos dados pessoais, disposto no artigo 7º, encontramos a previsão na norma: [...] “o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular” [...][98]. Subentende-se que, por terem sido objeto de tratamento, os dados mencionados no Art 3º são considerados automaticamente recolhidos junto do titular dos dados, segundo o texto da Lei.

Outro quesito interessante encontra-se no artigo 7º, § 5º:

> O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do

[94] SAWARIS, Adriana. **Op.Cit.**, p. 16
[95] MENDES, Laura. **Op.Cit**., p. 38.
[96] Ibidem., p. 38.
[97] BRASIL, 2018.
[98] BRASIL, 2018

> titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei, das quais não iremos abordar.[99]

Mais uma vez, é possível perceber que o legislador brasileiro indica que os dados devem de ser recolhidos junto do titular, pois necessitam de autorização para uso. Portanto, o recolhimento de dados pessoais junto do titula se encontra pulverizado no texto da norma brasileira, diferentemente da normativa europeia que o descreve diretamente, no Artigo 13º, sob o título o "Informações a facultar quando os dados pessoais são recolhidos junto do titular":

> 1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações:
> a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
> b) Os contactos do encarregado da proteção de dados, se for caso disso;
> c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
> d) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;
> e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
> f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.o, ou no artigo 49.o, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.
> 2. Para além das informações referidas no n.o 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:
> a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
> b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
> c) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea a), ou no artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
> d) O direito de apresentar reclamação a uma autoridade de controlo;
> e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar

[99] BRASIL, 2018.

> um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
> f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
> 3.Quando o responsável pelo tratamento pessoais tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do n.o 2.
> 4.Os n.os 1, 2 e 3 não se aplicam quando e na medida em que o titular dos dados já tiver conhecimento das informações. [100]

É tamanha a preocupação do Regimento Europeu com o direito de acesso que o titular poderá solicitar a identidade e os contatos do responsável pelo tratamento, assim como de seu representante. Cabe o mesmo ao encarregado da proteção de dados, assim como para as finalidades do tratamento a que se destinam, ou seja, o fundamento jurídico para a execução do tratamento. O titular também tem o direito de saber serão os destinatários do tratamento e seus interesses, estejam eles dentro do bloco europeu ou ainda em outro país. Por fim, o titular tem direito de acessar o prazo de conservação destes dados e quais os critérios utilizados para definir tal prazo, além de outros direitos explicitados na letra da Lei.

A norma europeia é tão atenta à proteção e ao resguardo dos dados pessoais dos titulares que trata do assunto em um único artigo[101], regulando os dados não recolhidos junto do titular:

> 1. Quando os dados pessoais não forem recolhidos junto do titular, o responsável pelo tratamento fornece-lhe as seguintes informações:
> a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
> b) Os contactos do encarregado da proteção de dados, se for caso disso;
> c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
> d) As categorias dos dados pessoais em questão;
> e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
> f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.o, ou no artigo 49.o, n.o 1, segundo parágrafo,

[100] BRASIL, 2018.
[101] Art. 16º, UNIÃO EUROPEIA, 2016.

a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas;
2. Para além das informações referidas no n.o 1, o responsável pelo tratamento fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente:
a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo;
b) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;
c) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratamentor no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
d) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea a), ou no artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
e) O direito de apresentar reclamação a uma autoridade de controlo;
f) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;
g) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
3. O responsável pelo tratamento comunica as informações referidas nos nº 1 e 2:
a) Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;
b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou
c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.
4. Quando o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados pessoais tenham sido obtidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes referidas no n.o 2.
5. Os n.os 1 a 4 não se aplicam quando e na medida em que:
a) O titular dos dados já tenha conhecimento das informações;
b) Se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, sob reserva das condições e garantias previstas no artigo 89.o, n.o 1, e na medida em que a obrigação referida no n.o 1 do presente artigo seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento. Nesses casos, o responsável pelo tratamento toma as medidas adequadas para defender os direitos,

> liberdades e interesses legítimos do titular dos dados, inclusive através da divulgação da informação ao público;
> c) A obtenção ou divulgação dos dados esteja expressamente prevista no direito da União ou do Estado-Membro ao qual o responsável pelo tratamento estiver sujeito, prevendo medidas adequadas para proteger os legítimos interesses do titular dos dados; ou
> d) Os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade.

O Regimento europeu indica as mesmas obrigações e direitos de acesso do titular indicados quando recolhidos junto do titular, porém com outros itens mais detalhados em seu artigo 14° para previsão ao direito do titular, sobre seus dados que não foram recolhidos juntos do titular. Após essa análise comparativa entre ambas as legislações, percebemos que o Regimento europeu apresenta uma série de indicações quanto ao tratamento, direitos e obrigações do titular que devem ser seguidas pelo responsável, enquanto a Lei brasileira não define de maneira tão detalhada a regulamentação dos dados recolhidos junto do titular. Concluímos, então, que tal direito não é suficientemente resguardado pela norma nacional.

Na seção a seguir continuaremos nosso estudo comparativo, dessa vez com enfoque em como a Lei europeia e a LGPD abordam o direito do titular de acessar seus dados quando julgar necessário.

3.3 Direito de acesso do titular dos dados

O direito de acesso dos titulares dos dados está indicado na letra da Lei brasileira (LGPD), pelo caput do artigo 18 e seu inciso II:

> 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: ...II - acesso aos dados [...];[102]

Assim, a Lei garante o direito do titular dos dados em obter do controlador o acesso aos dados tratados por ele, mas na prática a lei não especifica quais dados tratados poderão ser acessados, tampouco como isso será praticado pelo titular; ela explicita apenas como os dados devem ser requisitados ao controlador. É o que indica seu Art. 19º:

> A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
> I - em formato simplificado, imediatamente; ou

[102] BRASIL, 2018.

> II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.
> § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
> § 2º As informações e os dados poderão ser fornecidos, a critério do titular:
> I - por meio eletrônico, seguro e idôneo para esse fim; ou
> II - sob forma impressa.
> § 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
> § 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.[103]

A letra da Lei indica regras a serem seguidas para o acesso aos dados pessoais; por exemplo, a requisição do usuário deve estar em formato simples e imediato ou em formato de declaração completa e objetiva, indicando a origem dos dados ou ainda a inexistência deles, dentre outros detalhes como os critérios e finalidade do tratamento, além de regulamentar um prazo de 15 dias para o titular acessá-los ou recebê-los, a contar da data de requerimento. Além disso, os dados deverão ser armazenados de maneira simples para facilitar o direito de acesso, indicando ainda que este acesso às informações pode ocorrer por meio eletrônico ou impresso.

Ela também indica que o acesso é regulamentado nos casos em que houver um contrato acordado, de maneira a solicitar cópia eletrônica, desde que resguardados os segredos comercial e industrial, exigindo que seu formato permita a reutilização para outras operações, tudo isso sob a égide de uma regulação prevista pela autoridade nacional, que poderá dinamizar os prazos ligados aos incisos I e II.

Já segundo o Regimento europeu, encontramos inicialmente previsão de acesso aos dados em seu artigo 12º,[104] nº1, apontando que o responsável pelo tratamento tome medidas adequadas para fornecer as informações a respeito do tratamento efetivado ao titular dos dados por meio de uma linguagem simples e clara, especialmente quando dirigido a crianças.

---

[103] BRASIL, 2018.
[104] União Europeia, 2016.

No entanto, o direito de acesso é abordado de maneira aprofundada no Artigo 15º[105], que disciplina o direito do titular dos dados em obter confirmação sobre o tratamento de suas informações pessoais pelo responsável, indicando que, desde que o tratamento tenha sido efetuado em seus próprios dados, o titular tenha o direito de acessá-los, seguindo as recomendações do regimento: quando o acesso for respeito a finalidade do tratamento; quando os dados corresponderem à categoria de dados pessoais; ou, ainda, quando os dados tiverem sido enviados a destinatários que os divulgaram, incluindo os dados enviados a países terceiros ou pertencentes a organizações internacionais; quando o acesso refere-se a prazos e à conservação dos dados. Além disso, o Art. 15º do Regimento menciona a possibilidade de solicitar ao responsável pelo tratamento a retificação, o apagamento ou ainda a limitação ao tratamento de seus dados pessoais, bem como se opor ao tratamento efetuado. A Lei europeia também prevê o direito de reclamação a autoridade de controle, e, caso os dados não tenham sido recolhidos junto ao titular dos dados, ele tem direito sobre as informações disponíveis relacionadas à origem desses dados.

A Lei europeia explicita, ainda, no nº 2 do Artigo supracitado, a obrigação do titular em ser informado das garantias adequadas dispostas na ocorrência de transferências de seus dados a países terceiros ou a organizações internacionais, seguindo os requisitos dispostos no artigo 46. Já no nº 3, existe a previsão de que o responsável pelo tratamento forneça uma cópia dos dados pessoais sem custos para o titular; porém, requeridas outras cópias, poderá ser auferida taxa razoável levando-se em consideração os custos administrativos. Há, também, a possibilidade de o titular solicitar acesso por meio eletrônico, além de poder receber seus dados virtualmente. Por fim, é importante ressaltar que o nº4 do mesmo Artigo indica que o acesso aos dados não prejudica os direitos e as liberdades de terceiros. É evidente que a Lei nacional se baseou na previsão do direito de acesso disposta no Regimento europeu; dessa forma, podemos concluir que a norma brasileira é um pouco mais abrangente ao tratar do referido direito. Ainda assim, existem diferenças entre elas, como a falta de previsão de acesso aos dados enviados ao exterior, tendo sido eles autorizados ou não.

No próximo capítulo trataremos de abordar os direitos de retificação e apagamento, comparando sua aplicabilidade dentro de ambas as legislações.

---

105 União Europeia, 2016.

4 DIREITOS DO TITULAR: RETIFICAÇÃO, APAGAMENTO, TRATAMENTO E PORTABILIDADE

4.1 Direito de Retificação

A Lei Geral de proteção de dados brasileira define o tema da retificação de maneira bem objetiva e breve em seu artigo 18, inciso III, indicando que o titular dos dados poderá obter do controlador, a qualquer instante, a correção dos seus dados, seja por motivos de inexatidão, desatualização ou, ainda, por estarem incompletos.

Percebemos que o legislador não utilizou o termo retificação, mas “correção de dados”; mesmo assim, ele prevê a referida modificação dos dados do usuário em determinadas circunstâncias como as detalhadas acima.

Já no Regimento europeu, a retificação é indicada em dois momentos de seu texto: o primeiro está localizado no Artigo 15º - Direito de acesso do titular dos dados, nº1, definindo que

> o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:
> e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; [...].[106]

Nesse caso, a retificação é permitida desde que o titular a solicite ao responsável pelo tratamento de dados, autorizando inclusive o apagamento ou limitação de tratamento dos dados pessoais caso seja cabível.

Já no Artigo 16º, a GDPR define que

> O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.[107]

Percebemos, mais uma vez, que a norma brasileira se baseou na legislação europeia devido às semelhanças em suas propostas, e sobretudo na previsibilidade de proteção aos direitos e à dignidade humana do cidadão que cedeu seus dados.

---

[106] UNIÃO EUROPEIA, 2016.
[107] UNIÃO EUROPEIA, 2016.

Na seção seguinte, analisaremos como a legislação brasileira e a europeia podem ser comparadas quanto ao direito de apagamento dos dados, também chamado de “direito a ser esquecido”.

4.2 Direito ao apagamento dos dados («direito a ser esquecido»)

Em raras circunstâncias, ambas as normas apresentam de maneira semelhante a previsão para o apagamento dos dados. Rodrigues menciona que

> Outro avanço é o da inserção na legislação regras de encerramento de tratamento de dados pessoais, seguindo a tendência de endosso da tese abordada no Enunciado 531 do Conselho de Justiça Federal, oferecendo oportunidade de apagamento de dados até a desindexação de informações descontextualizadas na realidade sociodigital [...].[108]

Percebemos que a adição do direito ao apagamento na LGPD é tida como algo positivo para diversos analistas jurídicos, pois garante mais proteção e segurança aos direitos do titular. Na norma nacional, essa previsão encontra-se no Artigo 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: VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei [...][109]

A exposição desse direito ao titular dos dados é clara diante do controlador, ou seja, ele poderá a qualquer momento, mediante requisição, solicitar a “eliminação dos dados pessoais”. Importante mencionar que a norma brasileira não utiliza os termos apagamento ou esquecimento, mas sim “eliminação” de dados. O direito à eliminação de dados se refere apenas para os dados cujo titular consentiu com o tratamento, não abarcando aqueles recolhidos e tratados sem sua autorização. Resta, portanto, uma lacuna à proteção do direito do cidadão em requerer o apagamento dos dados que não obtiveram permissão para serem expostos ou manipulados/tratados, como por exemplo as atuais “Fake News”. Outro relevante ponto da lei encontra-se nas exceções indicadas na última linha do supracitado artigo 18, inciso VI, que faz referência ao artigo 16. A letra da lei brasileira, no Art. 16, indica que:

---

[108] RODRIGUES, Yuri. A privacidade no ambiente virtual: avanços e insuficiências da lei geral de proteção de dados no brasil (lei 13.709/18). **Revista dos Tribunais Online**, São Paulo. mar. 2019, p. 12.

[109] BRASIL, 2018.

> Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.[110]

Percebemos que o artigo determina que os dados pessoais serão eliminados após termino do tratamento, dentro dos limites técnicos; há, porém, uma exceção que permite a conservação de certos dados, desde que especificadas as razões de sua manutenção indicadas nos incisos I: “dentre os dados, aqueles que venham a cumprir uma obrigação legal ou regulatória por parte do controlador”; e II: “por estudo de órgão de pesquisa, desde que garantido sempre que possível a anonimização”. Nesse contexto, percebemos o poder do Estado se impondo sobre os direitos de personalidade dos cidadãos. Tal brecha poderia ser usada para justificar o acesso, por parte do censo do IBGE, às informações pessoais dos usuários de serviços de telefonia, fato considerado inconstitucional pelo STF em decisão recente devido aos riscos eminentes ao direito da vida privada.

Em seu item III, a Lei indica que os dados serão eliminados diante da transferência a terceiros, respeitando o tratamento desses dados de acordo com a lei. No entanto, não menciona se isso ocorrerá automaticamente junto à transferência, nem tampouco se o controlador cedente tem o dever de resguardar os dados por um período de segurança antes de eliminá-los de fato, para assegurar o direito do cidadão de acessar seus dados caso ocorra algum erro no processo de transferência e este tenha de ser refeito. Já no item IV é indicado que o processo de eliminação dos dados é exclusivo do controlador, vedando seu acesso a terceiros, que só pode ocorrer desde que os dados estejam anonimizados. É possível concluir que o legislador criou, novamente, uma brecha aos dados que supostamente apenas o controlador teria acesso para eliminar, restando dúvidas de que, como, e quanto destes dados devem estar anonimizados, para que um terceiro possa ter contato e assim excluí-lo, ou seja efetivar o apagamento.

---

110 BRASIL, 2018.

Já a Regimento europeu trata, em seu título, do direito ao apagamento de dados, chamado por ele também de “direito a ser esquecido”. No Artigo 17, a letra do Regimento determina que:

> 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:
> a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
> b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
> c) O titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 2;
> d) Os dados pessoais foram tratados ilicitamente;
> e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
> f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.o, n.o 1.
> 2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.o 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.
> 3. Os nº 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:
> a) Ao exercício da liberdade de expressão e de informação;
> b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
> c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.o, n.o 2, alíneas h) e i), bem como do artigo 9º, nº3;
> d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89º, nº 1, na medida em que o direito referido no nº 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou
> e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.[111]

[111] UNIÃO EUROPEIA, 2016.

O item 1 esclarece que o titular tem o direito de manifestar, diante do responsável, seu desejo pelo apagamento dos dados, e o responsável tem o dever de efetivar o apagamento imediatamente. Já na alínea a), o direito ao apagamento é autorizado para os dados pessoais que não cumprirem mais a finalidade para a qual tenha sido recolhido ou tratado; na alínea b), o apagamento também é indicado quando o titular dos dados deseja retirar seu consentimento para o objetivo do tratamento dos dados, em especial aos motivos expostos no artigo 6º, nº. 1, alínea a). Também é concedido ao titular dos dados o direito ao apagamento de dados cujo consentimento tenha sido dado para tratamento a uma ou mais finalidades específicas; portanto, essa indicativa assegura ao titular dos dados o direito ao apagamento desde que respeitadas as formas do artigo 17. Seguindo nossa análise sobre a alínea b), ela menciona o artigo 9º, n°2, alínea a), indicando que, caso não exista fundamento jurídico para manutenção dos dados, é permitido ao titular o direito ao apagamento. Essas especificidades encontram-se junto do título Licitude do tratamento. Na alínea c) é mencionado que, quando o titular se opuser ao tratamento nos termos do artigo 21º, nº 1 – que se refere ao momento particular do titular sobre o tratamento de seus dados pessoais – e não houverem razões que justifiquem o tratamento, é permitido que o titular se oponha, desde que os impulsos de oposição se enquadrem nos termos do artigo 21º, nº 2. Esse capítulo se refere aos dados que tiverem sido tratados para comercialização direta, ou seja: automaticamente o titular tem o direito de se opor a tudo que envolve o tratamento de tais dados – e, portanto, a estes se vincula o seu direito ao apagamento.

Seguindo o mesmo entendimento, a alínea d) do artigo supracitado inicialmente define que o direito ao apagamento também abrange aos dados tratados ilicitamente, sem o consentimento do titular dos dados, ficando ele autorizado, por meio de sua manifestação, a exigir o apagamento. A alínea e) explicita que o apagamento deverá ser cumprido quando houver obrigação jurídica decorrente do direito da União ou ainda de qualquer Estado-Membro ao qual o responsável pelo tratamento esteja sujeito. Vemos aqui uma nítida previsão de proteção aos dados na relação entre civis e Estado. Já na alínea f), o direito ao apagamento dos dados também está resguardado a todos aqueles que se encontrarem dentro de um contexto de produto comercial com empresas ofertantes de serviços tecnológicos indicados no artigo 8.°, n.°1, cujo objetivo é tratar de dados consentidos por crianças; um tema delicado, porém abordado pela norma europeia.

O nº 2 do art. 17 determina que os dados pessoais cujo responsável pelo tratamento tiver tornados públicos devem ser apagados, devendo ele, portanto, seguir todas as medidas razoáveis, incluindo de caráter técnico e os custos desta aplicação. É essencial, sobretudo, informar o responsável pelo tratamento dados que o titular solicitou o apagamento – inclusive de cópias e reproduções. Percebemos, portanto, a preocupação do legislador com os casos de vazamento de informações mesmo que acidentais, e a sua exigência pelo apagamento das informações caso replicadas.

Por fim, o item 3º do artigo 17, em suas alíneas a), b), c), d), e e), se refere às situações em que o apagamento não é permitido, incluindo:

> o exercício da liberdade de expressão e de informação; a cumprimento de uma obrigação legal para com a União ou Estado-Membro, funções de interesse público ou ao exercício da autoridade pública, interesse público em matéria de saúde pública, para fins de arquivos, para fins de investigação cientifica, histórica ou estatística.[112]

Os três últimos itens citados possuem especificações no artigo 89º, n°1, para que sejam resguardados de qualquer gravidade.

Portanto percebe-se que, diante de uma comparação entre a Lei brasileira e o Regimento europeu, a RGPD demonstra ser bem mais disciplinada no que tange o direito ao apagamento. A norma nacional faz uma breve menção utilizando ainda o termo eliminação dos dados, e não apagamento. Isso nos leva a um questionamento quanto à diferença entre as normativas. No texto brasileiro, vemos que o direito pode ser requerido, porém sua aplicação é focal, promovida junto a um único controlador.

Já a letra da lei europeia é mais abrangente, pois o legislador determina que o apagamento também deve ser efetuado até mesmo com os rastros ligam esses dados a outros bancos de dados. Caso os dados tenham sido compartilhados, seja de forma consentida, ilícita ou para mais de um banco de dados, o titular sempre terá o direito ao apagamento imediato – o que se refere à sua eliminação total ou parcial, a depender da requisição do titular.

A seguir, daremos continuidade à análise comparativa entre ambas as legislações, dessa vez com enfoque no direito à limitação do tratamento pelo responsável.

---

[112] UNIÃO EUROPEIA, 2016.

4.3. Direito à limitação do tratamento pelo responsável

No entanto, é importante lembrar que, em 1981, foi aprovada a primeira ferramenta normativa internacional, a Convenção nº.108, do Conselho da Europa, cujo objetivo era resguardar os civis diante do tratamento automatizado de dados pessoais como disposto no artigo 1º da Convenção. Ela tratava dos direitos e liberdades das pessoas, em especial sobre a vida privada. A ideia era legislar sobre o devido tratamento dos dados pessoais, sem abusos, mantendo sua lisura e seguindo os parâmetros de sua autorização para uso. Ressaltava-se uma categoria chamada de 'dados especiais', considerados "dados sensíveis" como disposto no artigo 6º desta mesma Convenção. Tais dados só sofreriam tratamento automatizado com prévia liberação dos Estados-Membros do Conselho da Europa, dadas as garantias de maneira especificadas, salvaguardando a integridade dos direitos de personalidade do cidadão e seus dados pessoais sob risco de sofrer sanções penais.[113]

Ainda no mesmo ano a Comissão Europeia editou outras medidas, sendo uma delas a recomendação para todos os Estados membros da União Europeia (81/679/CEE) dedicada à "proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal". Vemos aqui uma recomendação definindo o tema como sendo um mecanismo de escudo do indivíduo, considerando portanto, a proteção de dados como um direito fundamental.[114]

Adriana Sawaris[115] aponta, ainda, que a terceira geração teve início no ano 1981, com a Convenção de Strasbourg, caracterizada pela fusão do direito europeu. Ela vislumbrava preservar os direitos individuais sem frustrar o crescimento do setor de informática e também contribuiu para a presunção constitucional dessa matéria de direito.

O sociólogo brasileiro Sérgio Amadeu da Silveira[116] aponta a importância do vínculo entre nossa sociedade, tecnologia e economia:

> As sociedades informacionais são sociedades pós-industriais que tem a economia fortemente baseada em tecnologias que tratam informações como seu principal produto. Portanto, os grandes valores gerados nessa economia não se originam principalmente na indústria de bens materiais, mas na produção de bens imateriais, aqueles que podem ser transferidos por redes digitais. Também é possível constatar que as sociedades informacionais se estruturam a partir de tecnologias cibernéticas, ou seja, tecnologias de informação e de

113 SAWARIS, Adriana. **Op.Cit.,** p. 14.
114 Ibidem., p. 15
115 Ibidem., p. 15

> controle, as quais apresentam consequências sociais bem distintas das tecnologias analógicas, tipicamente industriais.

Porém, o autor alerta que, diante de uma análise do direito à autodeterminação informativa, percebe-se que ela possui viés duplo: primeiramente, ela atinge uma proteção (negativa) com o objetivo de bloquear a interferência do Estado sobre os entes privados, permitindo que os cidadãos impeçam o acesso ou até o tratamento de seus dados pessoais; já em um segundo momento, pode-se indicar uma proteção à liberdade (positiva) onde o indivíduo é imbuído do poder, e assim confere a ele determinar/autorizar o acesso, o tratamento e o uso de seus dados pessoais, inclusive diante do Estado. Esse título trata do direito previsto pela norma, totalmente voltado ao limite que deve ser dado ao tratamento dos dados bem como para a atuação do responsável por eles. É importante que compreendamos, com base na LGPD, tudo o que se entende por tratamento de dados, significado que se encontra disposto expressamente em seu artigo 5º, inciso X[117]:

> coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados.

A letra da Lei expõe todas as formas de tratamentos possíveis previstas e aplicadas aos dados pessoais. Em um segundo momento, seus limites estão especificados no Art. 6º:[118]

> As atividades de tratamento de dados pessoais deverão observar a boa-fé, demonstrando outra nomenclatura para os limites do tratamento dos dados, encontrados nos princípios norteadores:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

[117] BRASIL, 2018.
[118] BRASIL, 2018.

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.
> Neste contexto devemos compreender primeiramente o princípio da boa-fé, que o legislador nacional citou no caput da norma, e que vem a agregar no contexto da lei brasileira, referindo-se que o princípio da boa-fé está diretamente ligado ao dever da lealdade processual, onde a honestidade e a integridade entre as partes envolvidas, logo, são premissas fundamentais. E ao contrário desta, caracterizará uma afronta, não só a parte inversa da relação processual, mas, ainda, um desacato ao próprio Estado brasileiro, que por sua vez, tem como base este princípio em sua tutela jurisdicional. Este movimento decorre do princípio da boa-fé objetiva. Que nosso legislador por sua vez, resguarda como um padrão de defesa ao nosso Estado Democrático de Direito (artigo 1º, caput, da CF)consagrado na dignidade da pessoa humana (artigo 1º, III, CF), cujos objetivos são construir uma sociedade livre, justa e solidária (artigo 3º, I, CF); proporcionando o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (artigo 3º, IV, CF) que rege suas relações internacionais pelos princípios da igualdade entre os Estados (artigo 4º, V, CF); defesa da paz (artigo 4º, VI, CF); solução pacífica dos conflitos (artigo 4, VII, CF); cooperação entre os povos para o progresso da humanidade (artigo 4º, IX, CF),disciplinado também, pelo princípio da boa-fé objetiva.[119]

Seguindo a análise do artigo 6º da LGPD, é possível verificar que todos os princípios elencados, desde a boa-fé até os incisos I, II, III, IV, V, VI, VII, VIII, IX e X, nada mais são do que formas de limitação impostas pela norma, sejam elas mínimas ou máximas no direito ao tratamento dos dados. Menciona-se, também, o Art 18º[120], que possui o mesmo propósito de impor limitações:

> 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:

[119] NOVELI, Érica de Fátima dos Reis. O princípio da boa-fé objetiva e sua incidência no Código de Processo Civil. **Jus**, Teresina, p. 1-5, jun. 2017. Disponível em: shorturl.at/uIOUY. Acesso em: 10 jun. 2020.
[120] BRASIL, 2018.

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;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. CITAÇÃO DIRETA DA LEI

Desta maneira observemos que o mesmo título da lei brasileira que dispõe de direitos ao titular, também dá limites ao tratamento. Mas que mesmo assim a norma nacional, mais uma vez não focou sua atenção objetiva para este tema, ao ponto de dar a ele a devida atenção necessária. Ao contrario do texto do Regimento europeu, que indica dois artigos que se relacionam com a limitação do tratamento, vide o Artigo 18.o Direito à limitação do tratamento

> 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações:
> a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;
> b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;
> c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
> d) Se tiver oposto ao tratamento nos termos do artigo 21.o, nº 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.
> 2. Quando o tratamento tiver sido limitado nos termos do nº 1, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro.
> 3. O titular que tiver obtido a limitação do tratamento nos termos do nº 1 é informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento.
> Artigo 19º.
> Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento
> O responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 16º, o artigo 17º, nº 1, e o artigo 18º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários.

De maneira geral, para compreendermos a comparação entre as normas, devemos saber quem são os agentes que movimentam ou manipulam os dados pessoais segundo a LGPD e o Regimento europeu. Quando falamos sobre manipulação ou tratamento de dados pessoais, falamos do responsável por essa atividade

> como sendo (i) o controlador, isto é, a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, e o (ii) operador de dados, definido como a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.[121]

[121] BRASIL, 2018.

Portanto, percebemos a existência de diversos agentes neste processo de tratamento de dados. Nesse contexto, Lefosse[122] argumenta que o trabalho do controlador pode ser terceirizado. Na prática, isso ocorre quando uma empresa contrata um prestador de serviços que é capaz de promover o tratamento dos dados de seu corpo efetivo. Nesse caso, o contratante (empregador) é considerado controlador, e a prestadora de serviços é a operadora dos dados. Cabe indicar ainda que uma mesma empresa poderá efetivar as duas funções sendo controladora e operadora de dados.

Por conta do envolvimento de diversos agentes para garantir o direito à limitação do tratamento dos dados, percebemos que o Regimento europeu é muito protetivo, tendo em vista que nele encontram-se previstos diversos direitos ao titular, como, por exemplo, a possibilidade de contestar a exatidão dos dados dentro de um período passível de verificação; ser informado caso o tratamento dado aos seus dados tenha sido ilícito e, assim, obter o direito de se opor ao apagamento da informação ilícita, permitindo limitação de seu uso; ter acesso aos dados, mesmo que seu tratamento não seja mais necessário, caso eles sejam utilizados para dar base à defesa do titular em um processo judicial; ou, ainda, o direito de verificar se o tratamento dos dados é legítimo.

Por fim, a garantia mais significativa presente no direito de limitação do tratamento pode ser encontrada no artigo 19°, em que é obrigatório ao responsável pelo tratamento comunicar a cada destinatário dos dados transmitidos que eles devem retificar, apagar ou limitar o tratamento dos dados caso seja desejo do titular e, havendo necessidade, o responsável pelo tratamento fornecerá as informações sobre os referidos destinatários.

Os fatos elencados acima demonstram que a Lei brasileira mais uma vez trata do direito à limitação do tratamento de maneira pulverizada quando a comparamos com o Regimento europeu, que trata, de maneira precisa e detalhada, sobre proteger os direitos dos cidadãos e sua vida privada diante de um cosmos eletrônico e virtual cuja dimensão é desconhecida.

Após esse apanhado jurídico que busca comparar ambas as normas quanto ao direito de limitação do tratamento dos dados, daremos continuidade à análise com foco no direito do titular à portabilidade de seus dados pessoais.

---

122 LEFOSSE Advogados. **Op.Cit,** p. 3.

4.4 Direito de portabilidade dos dados

Em ambas as normativas, o conceito de portabilidade é definido como o direito do cedente em conhecer e ter liberdade para decidir tanto o destino quanto a forma de tratamento que seus dados receberão junto a outros interessados como fornecedores de serviços ou produtos. Cada uma das normas define a aplicabilidade prática do direito à portabilidade. Na letra da lei brasileira, esse direito é encontrado no artigo 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: V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.[123]

A norma nacional é clara ao indicar que a portabilidade é um direito que os cidadãos podem obter do controlador de dados a qualquer momento, mas precisa ser requerido junto ao controlador, por meio de requisição expressa, ou seja, documentada. Essa solicitação deve ser realizada dentro dos moldes da regulamentação da autoridade nacional, sem definição sobre quem é essa autoridade ou como contatá-la. Sob o mesmo prisma, quando for do desejo do titular solicitar a portabilidade de seus dados, ele tem o dever de utilizar o mesmo formato de documentado expresso. É importante sinalizar que o legislador brasileiro mencionou no texto da norma a indicativa do resguardo dos segredos comerciais e industriais quanto à portabilidade, o que corresponde a uma exceção da regra, pois esses segredos possuem regulamentação própria. Percebemos, portanto, que a normativa brasileira é sucinta ao se referir apenas a quem tem direito à portabilidade, sem indicar de qual forma ela pode ser requerida. Além disso, a Lei nacional também não define em quanto tempo o direito do cidadão deve ser atendido, nem quais são os critérios que deverão ser seguidos pelo responsável pelos dados.

Segundo o Regimento europeu, o direito à portabilidade encontra-se no Artigo 20, intitulado Direito de portabilidade dos dados:

> 1.O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:

[123] BRASIL, 2018.

> a) O tratamento se basear no consentimento dado nos termos do artigo 6.o, nº1, alínea a), ou do artigo 9.o, nº 2, alínea a), ou num contrato referido no artigo 6.o, nº 1, alínea b); e
> b) O tratamento for realizado por meios automatizados.
> 2 Ao exercer o seu direito de portabilidade dos dados nos termos do nº1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.
> 3. O exercício do direito a que se refere o nº 1 do presente artigo aplica-se sem prejuízo do artigo 17.o. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.
> 4. O direito a que se refere o nº 1 não prejudica os direitos e as liberdades de terceiros. [124]

O título desse artigo demonstra o quanto o legislador europeu enfatizou a importância da portabilidade de dados, vide itens 1 e 2, onde determina que o titular dos dados tem o direito de receber tudo o que lhe diz respeito e que tenha sido fornecido aos responsáveis pelo tratamento dos dados. Além disso, a norma europeia sinalizou o tamanho e a abrangência do direito à portabilidade, indicando que ela deve ser requerida de forma organizada e coordenada, bem como indica a liberdade do cedente em transferir seus dados a outro responsável para tratamento.

Fica expresso na norma que o atual responsável não poderá interferir no direito de escolha do cidadão em portar seus dados desde que sejam seguidos todos os parâmetros legais e haja consentimento para novo tratamento, ou ainda que esteja dentro de um contrato. A norma prevê, inclusive, que esse direito deve ser garantido de maneira automatizada, e que os dados do cedente sejam transmitidos diretamente ao novo responsável, seguindo todos os padrões técnicos possíveis.

A RGPD ainda segue limitando a portabilidade em seu item 3 ao tratar de possíveis prejuízos ao artigo 17.º, intitulado “Direito ao apagamento dos dados”. Ele apresenta uma exceção à regra, determinando que não se aplica a portabilidade dentro do exercício das funções de interesse público nem sobre os dados das autoridades públicas, que ficam resguardados pelo responsável ao tratamento. No item 4, a RGDP determina que a portabilidade não fere os direitos ou tampouco a liberdade de terceiros, quando indica que poderá sim serem levados junto a esta portabilidade rastros de contatos com terceiros.

---

124 UNIÃO EUROPEIA, 2016.

Comparativamente, ambas as normas garantem o direito à portabilidade, porém a legislação brasileira é mais sucinta e pouco explicativa nos pontos elencados acima, o que faz do regimento europeu uma legislação muito mais protetiva dos dados pessoais. Ela não apenas dá liberdade ao direito pessoal do cedente, como determina que o responsável compreenda sua função, protegendo, assim, direitos de liberdade individuais e de personalidade – desde que respeitem as condições impostas. Além disso, a RGDP limita a portabilidade para dados que não sejam de interesse público ou relacionados ao Estado. De forma geral, compreende-se que a RGPD e a LGPD possuem mais diferenças do que semelhanças, dado que a lei brasileira aparenta estar em construção.

Após essa análise comparativa entre ambas as legislações e seus principais artigos, vamos às considerações finais, onde resumiremos a pesquisa desenvolvida anteriormente e trataremos de abordar os resultados de nosso estudo.

5 CONCLUSÃO

No trabalho apresentado iniciamos com o contexto histórico da proteção de dados na Europa e no Brasil. Seguindo de uma visão ampla por meio do nascimento jurídico através das primeiras normativas europeias como as Diretivas até a chegada do Regimento europeu. O mesmo ocorreu com a análise do nascimento da Lei Geral de Proteção de Dados no Brasil.

O objetivo deste trabalho, consiste em uma breve análise comparativa entre o Regimento europeu (RGPD) e o Lei Geral de Proteção de Dados brasileira (LGPD).

Verificando que a argumentação entre a proteção de dados pessoais e a privacidade das informações no Brasil, tem como indicativos nossos direitos fundamentais, mas que em geral o texto de nossa normativa seguiria as raízes do texto do Regimento Europeu.

Esta análise ocorre através de alguns dos títulos abarcados no Regimento europeu, para então constatarmos a existência dos direitos na normativa brasileira, o primeiro capítulo trata da informação e acesso dos dados pessoais dos titulares, neste primeiro contexto se incluiu as transparências e regras, assim como, recolhimento dos dados junto do titular e o acesso do titular aos seus dados todos foram encontrados de certa forma na norma brasileira.

Em seguida verificou-se a Retificação e o Apagamento, do qual incluía o Direito a limitação do tratamento e a portabilidade, e mesmo diante de um texto oriundo da RGPD, a norma brasileira mais uma vez demonstrou ser muito branda. Foi possível constatar quase que a ausência do direito a limitação do tratamento pelo responsável na norma nacional, pois em nada os textos se parecem, ou seja, não atingem os mesmos direitos. Mesmo que de maneira muito sucinta na grande maioria de nossa Lei, o que fica claro é que nosso legislador foi omisso e que o texto precisa ser desenvolvido.

O que é triste, pois ele se baseou na mais atual normativa, até o momento, e mesmo assim não deu a devida atenção a proteção dos titulares e seus dados pessoais, do qual foi nosso foco de observação. O que comprova diante de suas falhas o quanto são necessárias normativas como o Regimento europeu, que assegurem, de maneira firme, o direito de proteção de dados dos titulares diante das ações potencialmente abusivas de corporações ou ainda do Estado. Essa questão é fundamental diante do fato de que nossas vidas se encontram cada vez mais

entrelaçadas com o mercado/Estado. Esse trabalho tem objetivo trazer questionamentos pessoais, cujas respostas não podem ser obtidas nesse momento. No entanto, buscamos suscitar reflexões ao leitor quanto aos direitos dos indivíduos em relação a seus próprios dados e aos deveres e limites do Estado e do mercado em protegerem este conteúdo e seus usuários/titulares.

Nesse contexto, é de suma importância que a sociedade compreenda a importância histórica desses direitos e o quanto eles nos afetam; hoje, mais do que nunca, o uso e tratamento de nossos dados domina e manipula nossas vidas, atingindo o tecido social que resguarda o direito à privacidade. É relevante, sobretudo, que os atores políticos e sociais revejam essa legislação, seus objetivos e seus mecanismos jurídicos de aplicabilidade, para que demonstrem estar cientes de suas obrigações de desenvolver as leis visando os direitos dos cidadãos, parte obrigatória em seus papéis.

É preciso que nos quanto pessoas, questionemos se, como cidadãos, estamos disciplinados e capazes de refletir junto à sociedade brasileira sobre as problemáticas a respeito da proteção de dados no território nacional.

Um dos resultados que obtivemos nessa pesquisa está relacionado à forma como as informações, ou seja, os dados pessoais dos cidadãos, são tratados pela norma devido ao seu alto valor lucrativo; diversas vezes, eles são colocados à serviço das relações entre Mercado e Estado.

É possível que estejamos rumo à institucionalização de um Estado de Direito autoritário e à serviço do controle mercadológico sobre nossas escolhas individuais e coletivas. Diante dessas constatações e dos autores referenciados durante o trabalho, é possível verificar que, de maneira remota, nosso cotidiano é vigiado e conduzido a uma plateia localizada nas redes sociais, junto a geolocalizadores de aplicativos diversos. Estamos vivendo de maneira individualizada e, por consequência, fragilizada, fazendo com que nossas informações sejam mais facilmente acessadas, diante de uma normativa que ainda não está vigente e não será efetiva para nossa proteção.

É notório, diante das inúmeras lacunas que evidenciamos na Lei brasileira, que nossos cidadãos se encontram cada dia mais desprotegidos diante deste sistema normativo e mercadológico, que não pensa em proteger a privacidade, e nem tão pouco na sua individualidade, vida privada ou no coletivo. Nossa Lei já nasceu obsoleta mesmo tendo tido a oportunidade de ser muito mais protetora, pois é oriunda

do Regimento europeu, considerado o mais completo regimento de proteção de dados existente.

REFERÊNCIAS

BAUMAN, Zygmunt. **Vigilância Líquida.** Rio de Janeiro: Zahar, 2014.

BITTENCOURT, João Paulo. **Arquiteturas pedagógicas inovadoras nos mestrados profissionais em administração**. 450p. Tese, Curso de Administração, Universidade de São Paulo, 2016. Disponível em: shorturl.at/fvH78. Acesso em: 20 maio 2020.

BRASIL. Medida Provisória nº 959, de 29 de abril de 2020. **Prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD.** Brasília, 2020. Disponível em: shorturl.at/gyBFJ. Acesso em: 20.05.2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, 2014. Disponível em: shorturl.at/uxzGI. Acesso em: 20.05. 2020.

BRASIL. Projeto de Lei nº 53/2018, 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.** Brasília, 2018. Disponível em: shorturl.at/DIU09. Acesso em: 20.05.2020.

CASTELLS, Manuel**. A sociedade em rede: Vol.1.** A era da informação: Economia, sociedade e cultura (2ª ed.). São Paulo: Paz e Terra, 1999. p. 33

COSTA, Mariana Monteiro. **A era da vigilância no ciberespaço e os impactos na nova lei geral de proteção de dados pessoais no Brasil**: reflexos no direito à privacidade. 93p. TCC, Curso de Direito, Universidade Federal do Rio de Janeiro, 2018.

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.

HOSTERT, Ana Cláudia. **Proteção de dados pessoais na internet**: a necessidade de lei específica no ordenamento jurídico brasileiro. 2018. 87p. TCC, Curso de Direito, Universidade Federal de Santa Catarina, 2018.

IOB, **STF - Suspenso compartilhamento de dados de usuários de telefônicas com IBGE**. 2020. Disponível em: shorturl.at/fgJUV. Acesso em: 20 maio 2020.

MANGETH, Ana Lara**.** Análise comparativa entre os princípios informadores do regulamento geral de proteção de dados da união europeia e as normas do direito brasileiro. In: **Seminário de iniciação científica e tecnológica da PUC-Rio.** Relatório. Rio de Janeiro: PUC-Rio, 2018. 1-16p.

COELHO, Alexandre; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgangs (org.). **Direito, Inovação e Tecnologia**. São Paulo: Editora Saraiva, 2015.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 158p. Dissertação, Curso de Direito, Universidade de Brasília, 2008.

MIRAGEM, Bruno. A lei geral de proteção de dados (lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais Online**, São Paulo, n. 1009, p. 173-222, nov. 2019.

MONTEIRO, Renato. **Qual é o impacto direto do GDPR em empresas brasileiras?** 2018. Disponível em: shorturl.at/bfgW5. Acesso em: 20.05.2020.

NOVELI, Érica de Fátima dos Reis. O princípio da boa-fé objetiva e sua incidência no Código de Processo Civil. **Jus**, Teresina, p. 1-5, jun. 2017. Disponível em: shorturl.at/uIOUY. Acesso em: 10 jun. 2020.

PERONGINI, Maria Fernanda. **Pequeno guia sobre a Lei Geral de Proteção de Dados**: uma breve análise sobre a nova lei brasileira de proteção de dados pessoais. Rio de janeiro, 2018, 18p.

PROMULGADA a Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD). **Lefosse Advogados**. 2018, 13p. Disponível em: shorturl.at/mG019. Acesso em: 5.jun.2020.

RODRIGUES, Yuri. A privacidade no ambiente virtual: avanços e insuficiências da lei geral de proteção de dados no brasil (lei 13.709/18). **Revista dos Tribunais Online**, São Paulo, v. 122, n. 0, p. 181-202, mar. 2019.

SAWARIS, Adriana. **A tutela do direito à reserva sobre a intimidade da vida privada no regulamento nº 2016/679 da União Europeia.** 138p. Dissertação, Curso de Direito, Universidade de Coimbra, 2017.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies.** 65p. TCC, Curso de Direito, Universidade Federal de Uberlândia, 2018.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, n. 86, p. 269-285, abr. 2016.

UNIÃO EUROPEIA. Diretiva nº 2002/58/CE, de 12 de julho de 2002. **Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas**. Portugal, 2002. Disponível em: shorturl.at/qBGPZ Acesso em: 05.05.2020.

UNIÃO EUROPEIA. Diretiva nº 2006/24/CE, de 15 de março de 2006. **Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas**

de comunicações, e que altera a Directiva 2002/58/CE. Portugal, 2006. Disponível em: shorturl.at/fpqY7. Acesso em: 05.05.2020.

UNIÃO EUROPEIA. Diretiva nº 95/46/CE, de 24 de outubro de 1995. **Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Portugal, 1995. Disponível em: shorturl.at/bxCGN. Acesso em: 05.05.2020.

UNIÃO EUROPEIA. Regulamento nº 679, de 27 de abril de 2016. **Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE**. Portugal, 2016. Disponível em: shorturl.at/euBG2. Acessado em: 05.05.2020.

ANEXO A – Tabela 1: Evolução histórica da legislação de proteção de dados europeia

Continente	Década de 1970	Década de 1980	Década de 1990	Década de 2000
Europa Ocidental	Suécia (1973) Alemanha (1978) Dinamarca (1978) Áustria (1978) França (1978) Noruega (1978) Luxemburgo (1978)	Islândia (1981) Reino Unido (1984) Finlândia (1987) Irlanda (1988) Holanda (1988)	Portugal (1991) Espanha (1992) Suíça (1992) Bélgica (1992) Mônaco (1993) Itália (1996) Grécia (1997)	
Europa Oriental			Eslovênia (1990) Hungria (1992) Rep.Tcheca (1992) Rússia (1995) Estônia (1996) Lituânia (1996) Polônia (1997) Eslováquia (1998) Letônia (2000)	
América do Norte	Estados Unidos (1974)	Canadá (1982)		Canadá (2000)
América do Sul			Chile (1999)	Argentina (2000)
Oceania		Nova Zelândia (1982) Austrália (1988)	Austrália (1997)	
Oriente Médio e Ásia		Israel (1981) Japão (1988)	Coréia do Sul (1994) Hong Kong (1995) Taiwan (1995) Tailândia (1998)	Japão (2004)

Fonte: MENDES, 2008.

ANEXO B – Tabela 2: Semelhanças entre a LGPD e a GDPR

LEI BRASILEIRA (13709 – LGPD)	LEI EUROPEIA (GDPR)	INTERPRETAÇÃO DA PESQUISADORA
Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.	*Artigo 12.º* **Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados**: 1. O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças.	Ambos possuem o direito quanto a titularidade de seus dados.
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;	*Artigo 12.º* **Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados**: O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, 3. O responsável pelo tratamento fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos artigos 15.º a 20.º, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido.	Em ambos deve existir a confirmação do tratamento mediante requisição.
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: II - acesso aos dados;	*Artigo 12.º:* **Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados**: 1. O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças.	Em ambos deve existir ao titular o acesso aos dados.
Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simplificado, imediatamente; [..]	*Artigo 12.º* **Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados** 1. O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples,	Em ambos existe a previsão de um acesso fácil.
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: III - correção de dados	*Artigo 15.º:* **Direito de acesso do titular dos dados**: 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados [...].	Ambos indicam o direito a correção/retificação dos dados.

incompletos, inexatos ou desatualizados.	*Artigo 16.º* **Direito de retificação:** O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional	
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: V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;	*Artigo 20.º* **Direito de portabilidade dos dados**: 1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:	Ambos preveem a portabilidade.
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: VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;	*Artigo 15.º* **Direito de acesso do titular dos dados**: 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: e) A existência do direito de solicitar ao responsável [...] a retificação, o apagamento ou a limitação do tratamento de dados pessoais [...].	Ambos preveem um tipo de apagamento.
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: IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.	*Artigo 14.º:* **Informações a facultar quando os dados pessoais não são recolhidos junto do titular:** 2. Para além das informações referidas no n.º 1, o responsável pelo tratamento fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente: d) Se o tratamento dos dados se basear no artigo 6º, nº 1, alínea a), ou no artigo 9º, nº2, alínea a), a existência do direito de retirar o consentimento em qualquer altura [...].	Ambos preveem a revogação dos dados tratados.
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: § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.	*Artigo 14.º* - **Informações a facultar quando os dados pessoais não são recolhidos junto do titular:** 2. Para além das informações referidas no nº1, o responsável pelo tratamento fornece ao titular as seguintes informações: [...] e) O direito de apresentar reclamações a uma autoridade de controlo [...];	Ambos tem o direito de requerer uma petição/reclamação a autoridade.

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: § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.	*Artigo 14.º* - **Informações a facultar quando os dados pessoais não são recolhidos junto do titular:** 2. [...] o responsável pelo tratamento fornece ao titular as seguintes informações [...]: c) a existência do direito de solicitar ao responsável o acesso aos dados pessoais que lhe digam respeito, e a retificação, apagamento ou limitação do tratamento [...] e do direito de se opor ao tratamento, bem como o direito à portabilidade de dados.	Previsão de se opor ao tratamento em ambas. Na LGPD, pode se opor e o Regimento EU tem o direito de se opor.
Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: § 2º As informações e os dados poderão ser fornecidos, a critério do titular: I - por meio eletrônico, seguro e idôneo para esse fim; ou II - sob forma impressa.	*Artigo 12.º:* **Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados:** 1. O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.	Em ambos as informações/dados poderão ser fornecidos por meio eletrônico, impresso
Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial	*Artigo 14.º* : **Informações a facultar quando os dados pessoais não são recolhidos junto do titular:** 2. Para além das informações referidas no n.º 1, o responsável pelo tratamento fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente: g) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.	Em ambas tratam de fornecer decisões automatizadas, úteis e claras. (Tenho dúvida quanto a interpretação que fiz)

Fonte: Elaboração própria

ANEXO C – Tabela 3: Diferenças entre a LGDPR e a GDPR

LEI BRASILEIRA (1379 – LGDP)	LEI EUROPEIA (GDPR)	INTERPRETAÇÃO DA PESQUISADORA
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: IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;	Artigo 17.º **Direito ao apagamento dos dados:** 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:	Na LGPD, aborda a eliminação de dados desnecessários de forma lacunosa. E no RGPD o apagamento de ser feito de forma mais criteriosa bem como especificado no regimento.
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: III - correção de dados incompletos, inexatos ou desatualizados;	Artigo 16.º - **Direito de retificação**: O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.	A LGPD trata de correção de dados via requisição e o RGPD trata de retificação de dados que seja por via de declaração.
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: V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;	Artigo 20.º **Direito de portabilidade dos dados** 1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: 2 Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.	Na LGPD a portabilidade é mediante requisição expressa. No RGPD não tem exigência de uma requisição mas há a previsão de uma transmissão direta.
Art. 18. O titular dos dados pessoais tem direito a obter do controlador [...], a qualquer momento e mediante requisição: § 1º O titular dos dados pessoais tem o direito de	Artigo 15.º : **Direito de acesso do titular dos dados**: 1. O titular dos dados tem o direito de obter do responsável [...] a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: f) O direito de apresentar reclamação a uma autoridade de controlo;	Na LGPD é necessário que o titular tenha que peticionar a autoridade nacional, que será um órgão do

peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.		governo. No RGPD o titular dos dados tem que apresentar reclamação direta a autoridade de controle.
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; (sem prazo determinado)	Artigo 12.º - **Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados**: 3. O responsável pelo tratamento fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos artigos 15.º a 20.º, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento informa o titular dos dados de alguma prorrogação e dos motivos da demora no prazo de um mês a contar da data de receção do pedido. Se o titular dos dados apresentar o pedido por meios eletrónicos, a informação é, sempre que possível, fornecida por meios eletrónicos, salvo pedido em contrário do titular.	Em ambas o controlador tem que entregar as informações para o titular, porém a diferença fundamental é que na LGPD, não há determinação de prazo enquanto no RGPD existe uma determinação de um prazo de trinta dias.
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: § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.	Artigo 20.º - **Direito de portabilidade dos dados**: O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:	A LGPD prevê o direito de portabilidade de dados pessoais, mas não inclui os dados anonimizados. A diferença é que o RGPD prevê a portabilidade, mas em nada especifica sobre os dados anonimizados e nem utiliza este termo técnico.
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: § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.	Artigo 12.º - **Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados**: 4. Se o responsável pelo tratamento não der seguimento ao pedido apresentado pelo titular dos dados, informa-o sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial.	A diferença é que a LGPD faz previsão para o uso dos organismos de defesa do consumidor e o RGPD, em contraponto, apenas indica o direito de intentar ação judicial.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.	Artigo 14º - [i]**Informações a facultar quando os dados pessoais não são recolhidos junto do titular:** 2. Para além das informações referidas no n.º 1, o responsável pelo tratamento fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente: g) a existência de decisões automatizadas, incluindo a referida no artigo 22º, nº 1 e 4 [...] e informações úteis à lógica subjacente, bem como a importância e as consequências de tal tratamento para o titular.	Na LGPD, o titular dos dados tem o direito de solicitar revisão, enquanto no RGPD a previsão é de que o responsável pelo tratamento forneça as informações sobre a existência destas decisões automatizadas.

Fonte: Elaboração própria

FACULDADE DOM BOSCO DE PORTO ALEGRE
BACHARELADO EM DIREITO

LUCIANE GEMMELLARO

MODULAÇÃO DE EFEITOS COM BASE EM RAZÕES ECONÔMICAS NAS DECISÕES DO SUPREMO TRIBUNAL FEDERAL

PORTO ALEGRE
2017

LUCIANE GEMMELLARO

MODULAÇÃO DE EFEITOS COM BASE EM RAZÕES ECONÔMICAS NAS DECISÕES DO SUPREMO TRIBUNAL FEDERAL

Projeto de pesquisa apresentado como requisito para aprovação na disciplina de Trabalho de conclusão I na Faculdade Dom Bosco de Porto Alegre -RS.

Professora orientadora: Dra. Anair Isabel Schaefer

PORTO ALEGRE

2017

SUMÁRIO

1 DADOS DE IDENTIFICAÇÃO DO PROJETO

Título provisório

Modulação de efeitos com base em razões econômicas nas decisões do Supremo Tribunal Federal

Autor

Luciane Gemmellaro

Natureza da pesquisa

Projeto de Trabalho de Conclusão de Curso.

Previsão de duração

Início em agosto de 2017 e término em novembro de 2017.

Orientadora

Dra. Anair Isabel Schaefer

Local

Porto Alegre – RS

2 TEMA

MODULAÇÃO DE EFEITOS COM BASE EM RAZÕES ECONÔMICAS NAS DECISÕES DO SUPREMO TRIBUNAL FEDERAL.

3 DELIMITAÇÃO DO TEMA

O presente trabalho pretende analisar a aplicação das modulações dos efeitos das sentenças proferidas pelo Supremo Tribunal Federal em matéria de direito tributário.

Em especial, analisar a argumentação constitucional em matéria de lei ou ato normativo, e se os motivos como segurança jurídica, interesse social e econômicos seriam considerados suficientes para justificar as modulações de efeitos nas decisões do Suprema Corte em matéria tributária.

4 FORMULAÇÃO DO PROBLEMA

É justificável ao Supremo Tribunal Federal valer-se das modulações de efeitos da sentença, com fundamento nas razões econômicas quando trata de matéria tributária?

5 HIPÓTESES

a) Porque o trabalho de pesquisa sobre Modulações de Efeitos é importante.

O trabalho de pesquisa sobre Modulações de Efeitos da sentença pelo STF é, não importante porque se trata-se de uma técnica que flexibiliza os efeitos *ex tunc* do controle de constitucionalidade, permitindo reflexos nas demandas de Direito Tributário. Ademais há recurso da decisão proferida (exceto embargos declatórios0

b) O tema Modulação de Efeitos é atual?

A modulação dos efeitos das sentenças foram incluídos de forma expressa na Lei 9868/99, em seu artigo 27, permitindo a aplicação no controle concentrado. Após a EC 45/2004, na qual foi incluída a necessidade de comprovação pelo recorrente da repercussão geral no recurso extraordinário, a técnica passa a ser aplicada no controle difuso, com efeitos erga omnes. A análise no presente trabalho procura verificar se as decisões de matéria tributária, permitem a modulação dos efeitos , ainda que acarretem prejuízos ao contribuinte.

c) Modulações de Efeitos possuem repercussão na sociedade?

As Modulações de Efeitos das sentenças proferidas pelo Supremo Tribunal Federal repercutem na sociedade, podendo atingir direitos fundamentais dos contribuintes.

d) Existe discussão doutrinária a respeito do tema modulação de efeitos?

Há discussão doutrinária sobre a modulação dos efeitos da sentença pelo Supremo Tribunal Federal, em matéria tributária, mediante posições contrárias (fundamentadas nos direitos fundamentais dos contribuintes) e favoráveis, considerando que cabe ao Recorrente provar a repercussão geral para apreciação no controle difuso. O debate sobre a aplicação da modulação dos efeitos em matéria tributária pelo STF, ainda que aplicado de modo restrito, pode ser assim sintetizado, segundo Heleno Torres, que trazemos à colação, por pertinente

> O STF tem sido sobremodo restritivo no exame dos pressupostos para cabimento de modulação de efeitos em matéria tributária. No passado, o único caso com emprego relevante dos efeitos prospectivos, ainda que acompanhado de severas críticas ao modo casuístico e não suficiente para prover a segurança jurídica esperada, foi o que segue:
>
> > As normas relativas à prescrição e à decadência tributárias têm natureza de normas gerais de direito tributário, cuja disciplina é reservada a lei complementar, tanto sob a Constituição pretérita (art. 18, § 1.º, da CF de 1967/1969) quanto sob a Constituição atual (art. 146, III, b, da CF de 1988). Interpretação que preserva a força normativa da Constituição, que prevê disciplina homogênea, em âmbito nacional, da prescrição, decadência, obrigação e crédito tributários. Permitir regulação distinta sobre esses temas, pelos diversos entes da federação, implicaria prejuízo à vedação de tratamento desigual entre contribuintes em situação equivalente e à segurança jurídica. II. Disciplina prevista no Código Tributário Nacional. O Código Tributário Nacional (Lei 5.172/1966), promulgado como lei ordinária e recebido como lei complementar pelas Constituições de 1967/69 e 1988, disciplina a prescrição e a decadência tributárias. III. Natureza tributária das contribuições. As contribuições, inclusive as previdenciárias, têm natureza tributária e se submetem ao regime jurídico-tributário previsto na Constituição. Interpretação do art. 149 da CF de 1988. Precedentes. IV. Recurso extraordinário não provido. Inconstitucionalidade dos arts. 45 e 46 da Lei 8.212/91, por violação do art. 146, III, b, da Constituição de 1988, e do parágrafo único do art. 5.º do Decreto-lei 1.569/77, em face do § 1.º do art. 18 da Constituição de 1967/1969. V. Modulação dos efeitos da decisão. Segurança jurídica. São legítimos os recolhimentos efetuados nos prazos previstos nos arts. 45 e 46 da Lei 8.212/1991 e não impugnados antes da data de conclusão

> deste julgamento" (STF, Pleno, RE 560626, Repercussão Geral, rel. Min. Gilmar Mendes, j. 12.06.2008).

No mesmo sentido, José Souto Maior Borges: "É a surpresa, a antissegurança (mais que a insegurança), o agravo a direitos individuais erigidos em sistema. Daí porque se impõe atribuir efeitos apenas ad futurum nas decisões judiciais modificativas de práticas judiciais e/ou administrativas reiteradas ao abrigo da própria jurisprudência" (BORGES, José Souto Maior. O princípio da segurança na Constituição Federal e na Emenda Constitucional 45/2004. Implicações fiscais. In: PIRES, Adilson Rodrigues; TÔRRES, Heleno Taveira (Org.). Princípios de direito financeiro e tributário: estudos em homenagem ao professor Ricardo Lobo Torres. Rio de Janeiro: Renovar, 2006. P. 262). Igualmente, César García Novoa, para quem. "sin embargo, este efecto de cosa juzgada, 7iência7s7to a favor del ciudadano, que no puede ver agravada su situación jurídica por la aplicación retroactiva de una norma que viene a 7iência7s7 a aquella que, aunque inconstitucional, fue corroborada por un 7iência7s7to77 jurisprudencial, se ha visto pervertido por la doctrina del propio Tribunal Constitucional" (GARCÍA NOVOA, César. *El principio de 7iência7s7 jurídica en 7iência tributaria*. Madrid: Marcial Pons, 2000, p. 195).

. "Las 7iência7s7 (o expectativas) de certeza jurídica están cumplidas si: (a) puede evitarse la 7iência7s7to77 y (b) el resultado coincide 7iênci código valorativo, es decir, es 'correcto' en el sentido sustancial de la 7iência. Evitar la 7iência7s7to77 significa aproximadamente lo mismo que 7iência7s7to77e. Más aún, la 7iência7s7to77e puede ser definida por 7iênc de la 7iência7s7to7. Todo 7iência7s7to que satisface los 7iência7s del discurso racional da como resultado decisiones previsibles" (Aarnio, Aulis. Lo racional como razonable: un tratado sobre la justificación jurídica. Madrid: Centro de Estudios Constitucionales, 1991. P. 82).

. Como afirma Virgílio Afonso da Silva: "Se segurança jurídica puder ser traduzido, entre outras coisas, como um mínimo de previsibilidade na atividade jurisdicional, a forma mais segura de 7iência-la não passa apenas pela definição de métodos que possibilitem controle intersubjetivo – nesse ponto, tanto a subsunção quanto o sopesamento possibilitam tal controle. A verdadeira previsibilidade da atividade jurisdicional se dá a partir de um acompanhamento cotidiano e crítico da própria atividade jurisdicional" (SILVA, Luís Virgílio Afonso da. A constitucionalização do direito: os direitos fundamentais nas relações entre particulares. São Paulo: RT, 2004. P. 149; cf., ainda: RAMOS, Elival da Silva. Parâmetros dogmáticos do ativismo judicial em matéria constitucional. Tese (Titularidade). 2009. 289 p. Universidade de São Paulo, São

Paulo; ENGISCH, Karl. La idea de concreción en el derecho y en la 8iência jurídica actuales. Tradução de Juan José Gil Cremades. Granada: Comares, 2004; MULLER, Friedrich. Teoria estruturante do direito. São Paulo: RT, 2008).

TORRES, Heleno Taveira, Modulação de efeitos da decisão e o ativismo judicial. CONSULTOR TRIBUTÁRIO – jul. 2012. Acessado em 18/09/2017. P 7 - 9 https://www.conjur.com.br/2012-jul-18/consultor-tributario-modulacao-efeitos-decisoes-fundamental

6 JUSTIFICATIVA

Tema de suma importância e em voga no atual mundo jurídico, as decisões proferidas dentro da técnica de modulações de efeitos, remontam diretamente ao nosso Supremo Tribunal Federal, único detentor de capacidade para promover tal pratica jurídica. O que justifica o objetivo central deste tema e redundantemente sua aplicabilidade sob a seara do Direito Tributário, tão consequente sob nossas vivências.

Tecnicamente esta flexibilização de sentença, aplicada apenas pelo Superior Tribunal Federal, tem por objetivo atender as demandas jurídicas que debatem as questões ligadas a constitucionalidade de algumas ações.

Sua ampla necessidade de analise fundamenta-se basicamente sob a égide da segurança jurídica, repercussão social e de argumentos econômicos.

A repercussão de sentenças com modulação de efeitos em matéria tributária será verificada na pesquisa, de forma a analisar os motivos e se estes são suficientes para promover a estabilidade no que se refere aos direitos dos contribuintes.

7 OBJETIVOS

Tem como objetivo analisar as consequências causadas por decisões tomadas por nossa Suprema Corte em matéria de controle concentrado de constitucionalidade ou de inconstitucionalidade. Dentro de nosso sistema de controle difuso ou misto, ao modular efeitos, de sentenças que tratam de especialmente da ordem tributária, e assim se cabe a estas basear-se em argumentos econômicos para aplicar tal técnica.

7.1 OBJETIVO GERAL

Verificar as modulações de efeitos das decisões pelo STF, envolvendo matéria tributária.

7.2 OBJETIVOS ESPECÍFICOS

a) Verificar as inconstitucionalidades ajuizadas em controle difuso junto ao STF, em matéria Tributária;

b) Examinar os princípios que regem nosso ordenamento jurídico assim como nosso Código Tributário Nacional;

c) Analisar as demandas julgadas pelo STF, quanto à modulação dos efeitos em matéria tributária.

d) Examinar o que mudou após o advento do artigo 27 da Lei 9.868/99, que promove a respectiva técnica, aplicável ao controle difuso;

8 FUNDAMENTAÇÃO TEÓRICA

A referida técnica das Modulações de Efeitos de Sentenças é de longe praticada pelas Cortes no mundo inteiro, sua aplicação teve origem no sistema de modelo norte americano que se dinamiza estruturalmente como controle difuso de constitucionalidade. Além deste modelo, também existe o sistema Austríaco definido como sistema de controle concentrado que também promoveu as modulações de efeitos como meio de sentenças no âmbito constitucional.

Prática exclusiva dos órgãos detentores do direito de julgar a constitucionalidade de matérias ou atos.

Historicamente no Brasil tais precedentes, permitiram com que a nossa Suprema Corte já aplicasse este método, porém, apenas em decisões de processos excepcionais, por não haver previsão expressa em lei se utilizavam de princípios e precedentes norteadores.

Ocorre que as modulações de efeitos consistem em um sistema de controle de constitucionalidade misto, no caso do sistema normativo brasileiro, é uma conhecida técnica aplicada na tomada de decisões, em ditames de inconstitucionalidade ou de desdobramentos complexos em casos de extrema relevância.

Já a referida norma possuía precedente de aplicabilidade por nossa Corte sem necessitar de previsão de lei.

Porém nos dias de hoje vem o questionamento entre os doutrinadores quanto ao advento do artigo 27 da Lei n. 9.868/99, autoriza/permitir, diante de processos e julgamentos das ações direta de inconstitucionalidade ou ação declaratória de constitucionalidade e ainda na ação direta de Constitucionalidade, todas impetradas perante o Supremo Tribunal Federal, quando na busca de um parecer sobre inconstitucionalidade de matéria ou ato, podendo ocorrer um desdobramento técnico que modulará a sentença que transitar em julgado.

Tal justificativa se dá pelo texto da lei 9.868/99 art. 27 determina que, a referida autoriza, ao declarar a inconstitucionalidade de lei ou ato normativo, que tendo em vista de razões de segurança jurídica ou de excepcional interesse social, poderá o Supremo Tribunal Federal, por maioria de dois terços de seus membros, restringir os efeitos daquela declaração ou decidir que ela só tenha eficácia a partir de seu trânsito em julgado ou ainda que este ocorra em outro momento, a ser fixado pela sentença.

Sob a égide deste texto verificamos a devida possibilidade de aplicar os efeitos modulativos da sentença, e ainda após o transito em julgado promover um efeito no tempo, ex tunc, ex nunc ou pró futuro.

E por tais motivos temos como objetivo explorar tais decisões do Supremo Tribunal Federal que abranjam as modulações de efeitos nas decisões, nos delimitando nas ações de declaração de inconstitucionalidade das normas tributárias.

Examinar o uso desta técnica, suas decisões e principalmente seus fundamentos e motivações que levaram nossos ministros a tais entendimentos e promove-los serão primordiais para compreender seus efeitos no âmbito tributário.

Diante de tais buscas é importante definir o que é inconstitucionalidade: Segundo” Oswaldo Luiz Palu: A inconstitucionalidade é a incorreção da norma com o parâmetro superior positivo, quer sob o aspecto da *incorreção formal* (ou seja, do

processo legislativo, órgão emissor competente), quer sob o aspecto da *incorreção material* (conteúdo substancialmente incompatível com a Constituição) (2001, p. 69).

No texto de SANCHES, Liliane, A Modulação dos Efeitos das Decisões no Controle de Constitucionalidade em Matéria Tributária. **RBC** n. 20 – jul./dez. 2012 – ISSN: 1678-9547. Acessado em 18/09/2017. http://www.esdc.com.br/seer/index.php/rbdc/article/viewFile/8/7 p. 122 (PALU, Oswaldo Luiz. Controle de Constitucionalidade. 2ª ed. São Paulo: RT, 2001.)

Já André Dias Fernandes sustenta que a inconstitucionalidade é "uma *relação de incompatibilidade* com uma Constituição eleita como parâmetro de confronto" (2009, p. 23). Referenciando :

De acordo com SANCHES, Liliane, A Modulação dos Efeitos das Decisões no Controle de Constitucionalidade em Matéria Tributária. **RBC** n. 20 – jul./dez. 2012 – ISSN: 1678-9547. Acessado em 18/09/2017. http://www.esdc.com.br/seer/index.php/rbdc/article/viewFile/8/7 p. 122 FERNANDES, André Dias. Eficácia das decisões do STF em ADIN e ADC: Efeito vinculante, coisa julgada erga omnes e eficácia erga omnes. Salvador : JusPOVIN, 2009.

A citação de "Jorge Miranda (2009, p. 24):

> Constitucionalidade e inconstitucionalidade designam *conceitos de relação*: a *relação que se estabelece entre uma coisa – a Constituição – e outra coisa – um comportamento* – que lhe está ou não conforme, que cabe ou não cabe em seu sentido, que tem nela ou não a sua base. (...) De modo pré-sugerido, resultam do confronto *de uma norma ou de um acto* com a Constituição, correspondem a atributos que tal comportamento recebe em face de cada norma constitucional."

De acordo com SANCHES, Liliane, A Modulação dos Efeitos das Decisões no Controle de Constitucionalidade em Matéria Tributária. **RBC** n. 20 – jul./dez. 2012 – ISSN: 1678-9547. Acessado em 18/09/2017. http://www.esdc.com.br/seer/index.php/rbdc/article/viewFile/8/7 p. 122 que o cita. FERNANDES, André Dias. Eficácia das decisões do STF em ADIN e ADC: Efeito vinculante, coisa julgada erga omnes e eficácia erga omnes. Salvador : JusPOVIN, 2009. Que foi quem citou Jorge Miranda, não localizei a referencia.

Direcionando para a matéria tributária, Sanches indica Em matéria tributáriao assunto se torna especialmente complexo e delicado, diante da impossibilidade de restituição de valores recolhidosem função de norma que veio a ser declarada inconstitucional,

sendo que o seu exame se reveste de particular interesse e utilidade, na medida em que permite visualizar os rumos e tendências da Corte Suprema nessa seara.

De acordo com SANCHES, Liliane, A Modulação dos Efeitos das Decisões no Controle de Constitucionalidade em Matéria Tributária. **RBC** n. 20 – jul./dez. 2012 – ISSN: 1678-9547. Acessado em 18/09/2017. http://www.esdc.com.br/seer/index.php/rbdc/article/viewFile/8/7 p. 121

Vislumbra também, Heleno Taveira Torres, quando expõe que as declarações de inconstitucionalidade de leis nos tributos não cumulativos têm uma grave afetação às relações tributárias, com notáveis consequências para os contribuintes, com relação ao regime de créditos e obrigações acessórias envolvidas. Em vista disso, a modulação de efeitos da decisão (*ex nunc*, retroativa ou *pro futuro*) é fundamental para garantir a *segurança jurídica* e a efetividade dos valores que permitam determinar o excepcional interesse social.

Em alguns casos, os pressupostos justificadores da modulação podem decorrer das complexas relações entre empresas que atuam no mercado interno e cuja consequência pode privilegiar uma em detrimento da outra. Nesse caso, deve-se examinar até que ponto uma declaração de nulidade poderia criar vantagens competitivas para uma parcela de empresas, em detrimento das demais.

Como sabido, o princípio da *neutralidade concorrencial* permite a intervenção do Estado na economia, inclusive por meio de normas tributárias, mas impede que sejam privilegiados determinados agentes econômicos, em detrimento de outros que atuem no mesmo mercado relevante, de forma a provocar distúrbios concorrenciais. Este princípio da neutralidade, guardada as devidas proporções, pode aplicar-se também às decisões judiciais, no sentido de se reconhecer a garantia de neutralidade entre os agentes econômicos em virtude de decisões judiciais. Este é, sem dúvidas, um motivo de excepcional interesse social.

Em matéria tributária, portanto, o controle de inconstitucionalidade pode ser modulado no tempo por considerações de neutralidade concorrencial, em virtude de obrigações principais ou acessórias, mormente nos casos de controles de poder de polícia, como se verifica com os registros e outros.

Fica evidente que nas declarações de inconstitucionalidade de norma tributária as modulações de efeitos devem ser tratadas com extraordinária atenção, pois a de se ter olhos atentos para não promover a repetição de indébito, que se trata de recolher

repetidamente valores em função de ato ou norma invalidada pela decisão. Tal disfunção poderia ocorrer em quais quer das sentenças, mesmo se estas forem em sentido ex nunc, ex tunc ou ainda pró futuro.

De acordo com Regina Maria Macedo Neri Ferreira a definição de a define como
Por tais razões a importância do exame do controle de constitucionalidade utilizado em nosso sistema e consequentemente diretamente ligado as tomadas de decisões de nosso Supremo Tribunal Federal, nos casos de modulação.

Imaginemos, em uma situação hipotética, e onde examinemos tal divergência entre contribuintes concorrentes no mesmo mercado de atuação, e com tais adventos para a tomada de decisão, vir a beneficiar, mais um ou quem sabe talvez promover vantajosamente um combate que colida diretamente com o princípio da proteção do mercado e da livre demanda. Que consequências iriam ocorrer após uma situação destas, seria dantesco a cadeia de queda promovida, além de incentivar possíveis monopólios.

Quando tratamos de direito tributário, em sua totalidade estaremos atingindo diretamente o princípio da proteção do mercado, mas também a todo contribuinte, e a sua liberdade de escolha. Por tais motivos as modulações poderão vir a promover através dos principais elementos a serem analisados para a tomada de decisões a proteção de princípios como a ponderação, razoabilidade, segurança jurídica assim como a boa-fé entre as partes estes que são basilares do ordenamento jurídico brasileiro.

Por tais norteadores é que a busca pelos precedentes e a analise destes onde houve a ponderação dos efeitos das modulações positivas ou negativas, serão de suma importância ao verificando os principais fundamentos, utilizados para a tomada de decisão de jurisprudências na seara tributária, com vistas a uma

1 METODOLOGIA

1.1 MÉTODO DE ABORDAGEM

Será utilizado o método dedutivo, que se traduz em um raciocínio no qual, a partir de gerais, enumerados, inferimos uma verdade singular ou parcial. O argumento vai do geral para o particular, pois irá partir de características gerais da realidade do Poder Judiciário brasileiro para a apresentação do posicionamento da doutrina e da jurisprudência como mecanismo adequado de solução de conflitos aos contratos de adesão de telefonia móvel no qual recai as clausulas de fidelidade e de multa.

1.2 TÉCNICAS DE PESQUISA

Ao se analisar diferentes métodos existentes, verificou-se que os procedimentos mais apropriados para o desenvolvimento da pesquisa são: a revisão doutrina, e a jurisprudência.

2 CRONOGRAMA

2017					
ATIVIDADES	**AGO**	**SET**	**OUT**	**NOV**	**DEZ**
Escolha do tema e do orientador					
Encontros com o orientador					
Pesquisa bibliográfica preliminar					
Leituras e elaboração de resumos					
Elaboração do projeto					
Entrega do projeto de pesquisa					
Defesa					

2018					
ATIVIDADES	**MAR**	**ABR**	**MAI**	**JUN**	**JUL**
Revisão bibliográfica complementar					
Redação do capitulo 1					
Redação do capitulo 2					
Redação das considerações iniciais e finais					
Revisão e entrega do trabalho					
Defesa do trabalho em banca					

3 PROPOSTA DE SUMÁRIO

INTRODUÇÃO
I. Modulações de efeitos nas decisões do Supremo Tribunal Federal
1. Modulação dos efeitos das sentenças pelo STF
2. Controle concentrado: artigo 27 da lei 9868
3. Controle difuso: Repercussao geral
II. Modulação fundamentada exclusivamente em impacto econômico
1. Casos modulados pelo STF em matéria tributaria
2. Fundamento econômico nas decisões em matéria tributaria
3. Decisões favoráveis ao contribuinte
Conclusão
Referências bibliográficas

13 REFERÊNCIAS

ÁVILA, Humberto. Segurança Jurídica. 3. ed. São Paulo: Malheiros Editores Ltda, 2011.

ÁVILA, Ana Paula. A Modulação de Efeitos Temporais pelo STF no Controle de Constitucionalidade. ed. Porto Alegre: Livraria do Advogado Editora Ltda, 2009.

BARROSO, Luís Roberto. Mudança da jurisprudência do Supremo Tribunal Federal em matéria tributária: segurança jurídica e modulação dos efeitos temporais das decisões judiciais. REVISTA DE DIREITO DO ESTADO, Rio de Janeiro, n. 2. p. 261-288, abri./jun.2006.

DE SANTI, Eurico Marcos Diniz. Kafka, Alienação e Deformidades da Legalidade. 1. ed. São Paulo: FISCOSoft Editora Ltda. Revista dos Tribunais, 2014.

PALU, Oswaldo Luiz. Controle de Constitucionalidade. 2ª ed. São Paulo: RT, 2001.

SANCHES, Liliane, A Modulação dos Efeitos das Decisões no Controle de Constitucionalidade em Matéria Tributária. **RBC** n. 20 – jul./dez. 2012 – ISSN: 1678-9547. Acessado em 18/09/2017. http://www.esdc.com.br/seer/index.php/rbdc/article/viewFile/8/7

TORRES, Heleno Taveira, Modulação de efeitos da decisão e o ativismo judicial. CONSULTOR TRIBUTÁRIO – jul. 2012. Acessado em 18/09/2017. https://www.conjur.com.br/2012-jul-18/consultor-tributario-modulacao-efeitos-decisoes-fundamental

NEVES, Mariana Barboza Baeta, A Modulação de Efeitos e Sua Aplicação em Matéria Tributária. LEX EDITORA S/A - ISSN 1981 -1489. Acessado em 18/09/2017. http://www.lex.com.br/doutrina_26702022_A_MODULACAO_DE_EFEITOS_E_SUA_APLICACAO_EM_MATERIA_TRIBUTARIA.aspx

DE SANTI, Eurico Marcos Diniz, A Modulação no Controle de Constitucionalidade de Novos Tributos. CONSULTOR JURÍDICO – 10/jul. 2014. Acessado em 18/09/2017. https://www.conjur.com.br/2014-jul-10/eurico-santi-modulacao-supremo-criacao-tributo

FRANCISCO, Alison Cleber, Jurisprudência do STF e Modulação de Efeitos em Matéria Tributária. IBET- INSTITUTO BRASILEIRO DE ESTUDOS TRIBUTÁRIOS – Ribeirão Preto – 2011. Acessado em 18/09/2017. http://www.ibet.com.br/wp-content/uploads/2017/07/Alison-Cleber-Francisco-Jurisprud%C3%AAncia-do-STF-e-modula%C3%A7%C3%A3o-de-efeitos-em-mat%C3%A9ria-tribut%C3%A1ria..pdf

DE ALMEIDA, Vânia Hack, A Modulação dos Efeitos da Declaração de Inconstitucionalidade. PONTIFICIA UNIVERSIDADE CATÓLICA MESTRADO EM DIREITO - PUCRS/BCE – 0.904.322-0 – Porto Alegre – 2007.

GALLINA, Paola Maria; BASSOLI, Profª. Drª. Marlene Kempfer. Análise crítica à modulação dos efeitos em decisão de inconstitucionalidade de matéria tributária. REVISTA DE DIREITO PUBLICO, Londrina, v,4, N. 2, p.59-77, Maio/Ago. 2009. Acessado em 18/09/2017. http://www.uel.br/revistas/uel/index.php/direitopub/article/viewFile/10753/9407

BUFFON, Marciano; JUNIOR, Juliano Dossena. A modulação dos efeitos nas ações declaratórias de inconstitucionalidade em matéria tributária. REVISTA DA AJURIS, Porto Alegre, v,41, n.133 (2014). Acessado em 18/09/2017. http://www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/view/231