Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito/ Curso de Bacharelado em Relações Internacionais

CAROLINA FARIA CAETANO

DIREITO E PRIVACIDADE: Uma análise comparada do Decreto nº 10.046 de 2019 diante da Lei Geral de Proteção de Dados Pessoais.

BRASÍLIA/DF
2021

CAROLINA FARIA CAETANO

DIREITO E PRIVACIDADE: Uma análise comparada do Decreto nº 10.046 de 2019 diante da Lei Geral de Proteção de Dados Pessoais.

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Victor Minervino Quintiere

BRASÍLIA
2020

CAROLINA FARIA CAETANO

DIREITO E PRIVACIDADE: Uma análise comparada do Decreto nº 10.046 de 2019 diante da Lei Geral de Proteção de Dados Pessoais.

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito/Bacharel em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Victor Minervino Quintiere

BRASÍLIA, DIA 12 ABRIL DE 2021

BANCA AVALIADORA

_____

Professor(a) Orientador(a)

_____

Professor(a) Avaliador(a)

Dedico este trabalho aos meus pais, Frederico Jr. e Maria Eliana, e ao meu irmão, Fred, pela força insubstituível de suas presenças em minha vida e por terem sempre acreditado em mim. Sem eles nada seria possível.

Dedico também, ao meu querido tio Eduardo Jorge, meu pai de coração e orientador extracurricular que me auxiliou quanto à escolha da temática analisada.

Dedico-o, por fim, ao Pedro C. C., por todo seu apoio e companheirismo durante a minha graduação. Sua presença sempre afetou positivamente a minha vida.

AGRADECIMENTOS

O desenvolvimento deste trabalho de conclusão de curso contou com a ajuda de diversas pessoas, dentre as quais agradeço:

Inicialmente, agradeço a Deus. A Ele, tudo. Agradeço pela minha vida, e por me ajudar a ultrapassar todos os obstáculos encontrados ao longo do curso.

Agradeço aos meus pais, Frederico Jr. e Maria Eliana, por tornarem esse sonho possível e por estarem sempre presentes prestando incondicional apoio a mim. Vocês são a minha maior inspiração. Amo muito vocês.

Agradeço ao meu irmão, Frederico, pelo apoio e suporte que me deu durante todo o curso e durante toda a vida, por sempre estar ao meu lado.

Agradeço ao meu namorado, Pedro, por estar ao meu lado em todos os momentos, demonstrando apoio em todas as minhas escolhas. Obrigada pelo carinho, pelo suporte e pela compreensão por quando estive ausente pelo tempo dedicado aos estudos. Obrigada por ter sido meu melhor amigo e meu maior companheiro dentro da faculdade. Seu apoio foi essencial.

Agradeço ao meu querido tio Eduardo Jorge, cuja preocupação e demonstração de carinho comigo, e com os demais sobrinhos, sempre foram sem medidas. Agradeço por todo o auxílio na escolha do tema a ser trabalhado na minha conclusão de curso, por todos os conselhos e ensinamentos sobre o assunto e, também, sobre a vida.

Agradeço aos demais familiares, importantes no meu crescimento como mulher e na construção de princípios e valores que me tornaram quem sou hoje.

Agradeço aos amigos que cativei ao longo da minha graduação. Em especial, gostaria de agradecer a Amanda Cristina, Ana Tereza, Maria Lydia e Maria Vitória, por toda a ajuda e companheirismo nesses anos compartilhados, e por terem sido essenciais na superação das dificuldades. Obrigada por serem minhas amigas.

Agradeço a Beatriz Luz Mendes. Amiga fiel. Obrigada por me acompanhar desde o ensino médio até o final da minha graduação, tornando a rotina sempre mais leve e mais divertida.

Agradeço ao meu orientador, professor Victor Minervino Quintiere. Seu auxílio e sua atenção ao longo desse trabalho foram fundamentais. Obrigada por toda a paciência e por toda a dedicação, sempre demonstrando otimismo.

Agradeço a todos os funcionários do UniCEUB, pela urbanidade com que sempre me trataram.

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

A proteção de dados constitui não apenas em um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea.

Stefano Rodotá

RESUMO

O presente trabalho pretendeu abordar questões controversas envolvendo o Decreto nº 10.046 de 2019 e a Lei Geral de Proteção de Dados (Lei 13.709/2018), percorrendo para tal análise da importância da proteção de dados pessoais no ordenamento jurídico, de forma a observar a constitucionalidade do Decreto ao se permitir que a administração pública tenha permissão para acessar e compartilhar entre seus órgãos e entidades os dados pessoais de brasileiros. O Decreto permite que diversos tipos de informações constem dessa base, sendo objeto de estudo a sua regularização com as normas gerais de proteção de dados pessoais.

Palavras-chave: Proteção de dados. Privacidade. Compartilhamento. Cadastro Base do Cidadão.

SUMÁRIO

INTRODUÇÃO

A presente monografia propõe-se a reflexão acerca do direito á proteção de dados pessoais no Brasil diante do tratamento e compartilhamento de dados pelo Poder Público diante da criação de um cadastro base pela Administração Pública.

Desse modo, a aprovação do Decreto nº 10.046, de 9 de outubro de 2019[1]**,** pelo atual Presidente da República, Jair Messias Bolsonaro, acarretou a permissão de que dados pessoais de brasileiros constem desta base de dados e de que se tenha seu compartilhamento entre os órgãos e entidades públicas.

A escolha temática se deu através do interesse à respeito da atualidade do novo Decreto, e de suas eventuais consequências, já que ele se instituirá como uma regulamentação de estrutura nova e desconhecida pela integralidade do país, e também, apesar de recente, por ser alvo de diversas críticas diante sua contradição perante a Lei Geral de Proteção de Dados e à Constituição Federal, especialmente por unificar dados sensíveis, biométricos, em um verdadeiro *Big Data* (grande conjunto de dados em uma base, para seu tratamento e armazenamento).

A fim de compreender as alterações propostas pelo Decreto, bem como sua compatibilidade com as normas nacionais de proteção de dados pessoais, esse estudo ampara-se na análise do ordenamento jurídico brasileiro, além dos ensinamentos do renomado autor brasileiro Danilo Doneda e nos pensamentos de Stefano Rodotá, conhecido jurista italiano. Dessa forma, a compreensão dos autores atua como alicerce de toda a análise acerca do relacionamento do Decreto com a regulamentação brasileira.

Em virtude de todo o exposto, a monografia em tela é composta por quatro capítulos: (I) Da Importância da Proteção de Dados Pessoais (II) Uma Breve Contextualização Histórica da Base Normativa Sobre Proteção de Dados Pessoais (III) Direito E Privacidade: A LGPD e o Cadastro Único Nacional na Gestão Governamental (IV) O Cadastro Base do Cidadão sob a Perspectiva Constitucional.

---

[1] BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 12 abr. 2021.

O primeiro capítulo destaca conceitos importantes na compreensão da pesquisa, buscando explicar a importância da tutela dos dados pessoais como um direito inerente á pessoa humana. Além disso, explica e específica os princípios norteadores dessa tutela no ordenamento jurídico.

Já o segundo capítulo trata de apresentar o breve histórico da proteção de dados no ordenamento brasileiro, bem como em legislações internacionais, por mostrarem experiência no assunto regulamentado e por ter conteúdo simbólico ao inspirar nossos regulamentos acerca do tema, como a Diretiva de Proteção de Dados Europeia, que apesar de ter sido regulada em 1995, aborda questões cruciais, sendo considerada um marco histórico na proteção de dados da União Europeia e em todo o mundo, servindo de modelo a ser seguido.[2]

Por seu turno, o terceiro capítulo traz uma análise do Decreto nº 10.046 de 2019, demonstrando suas divergências com os fundamentos e princípios que compõem a Lei Geral de Proteção de Dados, especificando suas incompatibilidades.

Finalmente, o quarto capítulo busca uma análise constitucional acerca da compatibilidade dos princípios e direitos fundamentai diante da permissão de compartilhamento de dados pessoais dos cidadãos brasileiros, a serem unificados e utilizados pela administração do governo.

A pergunta norteadora da pesquisa consiste em destacar os pontos divergentes entre o Decreto nº 10.046 de 2019 e a LGPD de 2018, que assumem relevância na proteção de dados pessoais e em sua tutela constitucional.

Quanto ao método de procedimento, a pesquisa seguirá a linha de raciocínio dedutivo, isso diante da análise das premissas previstas nas legislações expostas ao estudo e, ainda da problematização, de forma que se busque a conclusão para eventuais desencontros nos regulamentos brasileiras a respeito do tratamento e da proteção de dados pessoais.

No tocante à base metodológica, como esclarecido nos tópicos anteriores, a pesquisa envolverá análises constitucionais e legislativas do ordenamentos nacional, além de aspectos doutrinários acerca da efetiva aplicação dos regulamentos diante dos princípios norteadores da proteção de dados pessoais, sendo que a classificação adotada para o estudo será a investigação dogmática jurídica, sendo de base teórica, com fim de determinar o

[2] LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ: novas práticas em informação e conhecimento**, Curitiba, v. 2, n. 1, p. 60-76, jan./jun. 2013. Disponível em: <http://www.atoz.ufpr.br>. Acesso em: 12 abr. 2021

esclarecimento do conteúdo normativo da ordem jurídica representante da temática, por meio da interpretação gramatical, lógica, sistemática e histórica. Assim o projeto adotará a metodologia monográfica, utilizando da revisão bibliográfica teórica, documental, histórica, dentre outras.

A fonte de pesquisa utilizada para estudo e análise foi primordialmente de natureza bibliográfica, utilizando de artigos científicos constantes de revistas, sites da internet, livros doutrinários, e notícias constantes da mídia e jornal brasileiros, além daquelas advindas do mundo internacional. Considerando que o trabalho pretende o estudo legislativo, a fonte se manterá caracterizando-se como bibliográfica e teórica.

1. DA IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais se caracteriza como uma atividade de risco ao possibilitar sua exposição e sua utilização de maneira indevida e abusiva e, por isso, se faz necessária a instituição de mecanismos que possibilitem ao titular deter conhecimento e controle sobre seus dados, posto que são a tradução da expressão direta de sua própria personalidade. Nessa acepção, o pensamento de Danilo Doneda é de que a proteção de dados pessoais se faz instrumento essencial para a proteção da pessoa humana[3]. Sobre isso:

> A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costumamos denominar de Sociedade da Informação. Os dados pessoais chegam a fazer às vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável.[4]

Sendo assim, é imperioso destacar que com os adventos da tecnologia implementados no campo da administração pública e privada, além do amplo acesso por particular, o debate acerca da privacidade vem ganhando cada vez mais força no cenário dos dados e do tratamento da informação pessoal. Em relação à terminologia "informação pessoal", Doneda identifica que é uma referência às ações (como suas manifestações sobre opiniões pessoais, dados com relação ao seu consumo etc.) ou características de uma pessoa, como no caso do nome civil ou do domicílio, por exemplo. Já o dado diz respeito a uma informação em estado potencial, antes de ser transmitida, se diferenciando da própria informação[5]. (Nesse sentido:

> Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como observamos em um autor que o entende como uma informação em estado potencial, antes de ser transmitida, o dado estaria associado a uma espécie de "pré informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega também um sentido instrumental, no sentido da redução de um estado de incerteza. A doutrina não raro trata estes dois termos – dado e informação – indistintamente, ou então, procede a uma diferenciação algo empírica que merece ao menos ser ressaltada. [6]

---

[3] DONEDA, D. A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law** [EJJL], v. 12, n. 2, 2011.
[4] Ibidem.
[5] Ibidem.
[6] DONEDA, Danilo, **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019, pag.136.

Para o autor, o "dado", portanto, seria a informação em seu estado natural, sem qualquer tratamento, se resumindo apenas ao disposto em seu conteúdo, sendo que a informação traz uma significação a este conteúdo, uma instrumentalização, uma utilidade. No entanto, para fins dessa pesquisa, essa sobreposição se tornaria confusa no desenvolvimento textual, fazendo com que o leitor se perca entre a frágil diferença dos significados. Portanto, serão utilizadas as terminologias "dados pessoais" e "informações pessoais" como sinônimos, conforme disposto no artigo 5º, inciso I, da Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018).[7]

Assim, temos que dados pessoais são as informações relativas à identificação de uma pessoa natural, bem como aquelas informações capazes de traçar sua vida social, profissional e íntima, além de sua personalidade. Seguindo essa mesma linha de raciocínio, Doneda ressalta que determinada informação possa ter um vínculo objetivo com uma pessoa, revelando algo sobre ela:

> Este vínculo implica que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade á lei, como no caso do nome civil ou do domicílio, ou então, ás informações provenientes de seus atos, como os dados referentes ao seu consumo, informações provenientes de suas manifestações, como as opiniões que manifesta, e tantas outras. É importante estabelecer este vínculo, pois ele afasta outras categorias de informações que, embora também façam referência a uma pessoa, não seriam consideradas propriamente informações pessoais, no sentido pretendido: as opiniões alheias sobre esta pessoa, por exemplo, a princípio, não possuem este vínculo objetivo; também a produção intelectual de uma pessoa, em si considerada, não é per se informação pessoal (embora o fato de sua autoria o seja).[8]

Por conseguinte, o conjunto de todas essas informações reunidas e estruturadas segundo uma determinada lógica, a serem utilizadas com o máximo proveito, seria o que é conhecido por "banco de dados". O banco de dados atualmente é disposto de forma informatizada, isso se dá por meio da tecnologia aplicada ao tratamento de informações pessoais, as quais são armazenadas em grande volume, processadas rapidamente e combinadas conforme a finalidade almejada.[9] O que leva ao objeto de estudo desse trabalho: o tratamento (coleta, agregação, compartilhamento, utilização) das informações dispostas em bancos de dados cuja gestão se dá pelo Poder Público.

---

[7] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 abr. 2021.

[8] DONEDA, Danilo**, Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019, pag.139

[9] Ibidem, p. 141

É imprescindível que o tratamento desses dados tenha uma regulamentação que garanta sua proteção, de forma a limitar a atuação estatal como detentora de tantas informações. Por isso, a própria Carta Magna traz como direitos fundamentais a garantia da inviolabilidade da intimidade e a autodeterminação informativa do indivíduo, a serem explicados de forma específica no desenvolvimento do trabalho. Com o mesmo objetivo, foi aprovada a Lei Geral de Proteção de Dados Pessoais, tratando de forma específica e detalhada sobre a matéria.

O desenvolvimento das normas acerca da proteção de dados se deu em busca de uma tutela que se mostrasse eficaz e vinculada aos princípios constitucionais, fortalecendo a posição do titular dos dados. Tais princípios podem ser encontrados em várias normativas sobre proteção de dados pessoais, sendo conhecidas como "*Fair Information Principles*", caracterizando-se como um núcleo comum, um conjunto de princípios a serem aplicados na proteção de informações pessoais[10].

Para melhor esclarecimento, vale mencionar que os princípios em questão se sintetizam na publicidade – ou transparência- dos bancos de dados a partir do conhecimento público de sua existência; na exatidão, devendo os dados armazenados serem fiéis à realidade; no princípio da finalidade, o qual determina que a utilização dos dados pessoais deve obedecer a um fim, previamente comunicado ao titular; ao livre acesso do indivíduo as suas informações armazenadas no banco de dados, podendo obter cópias dessas informações e controle delas e, ainda, na segurança física e lógica contra riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado. Deve-se, então, utilizar dos mencionados princípios para proteger os dados pessoais, servindo de referência nos demais regulamentos sobre a questão dentro do ordenamento brasileiro.[11]

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabeleceu princípios próprios a serem seguidos quando o tratamento de dados pessoais se der em território nacional, elencados em seu artigo 6º, sendo o princípio da finalidade, o qual busca a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de que se tenha tratamento posterior que ocorra de maneira incompatível com essas finalidades; o princípio da adequação, no sentido de o tratamento ser compatível com as finalidades informadas ao titular; ainda, o princípio da necessidade, impondo uma limitação ao

[10] DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law** [EJJL], v. 12, n. 2, 2011.
[11] Ibidem.

tratamento de dados, o qual deve ser realizado da forma mínima necessária em atendimento ás finalidades, de forma proporcional e não excessiva.

No mesmo sentido, foram estabelecidos os princípios do livre acesso aos titulares, da qualidade dos dados a qual deve zelar pela clareza e exatidão das informações, da mesma forma, o princípio da transparência, da segurança dos dados, da prevenção quanto á ocorrência de dados por meio de implementação de medidas técnicas e administrativas aptas a proteger as informações que constem no banco de dados e, ainda, os princípios da não discriminação dos dados e da responsabilização e prestação de contas, de forma que os dados não sejam utilizados com fins ilícitos ou abusivos e que o agente gestor demonstre utilizar de medidas eficazes e seguras em seu tratamento.

Para Bonavides, "a vinculação essencial dos direitos fundamentais à liberdade e à dignidade humana, enquanto valores históricos e filosóficos, nos conduzirá sem óbices ao significado de universalidade inerente a esses direitos como ideal da pessoa humana".[12]Assim, cabe lembrar que os direitos fundamentais cumprem a função de "criar e manter os pressupostos elementares de uma vida na liberdade e na dignidade humana".[13] Dessa forma, a dignidade humana é princípio inerente à pessoa, a todo ser humano, e está no alicerce dos demais princípios que compõem os direitos fundamentais da Constituição brasileira, elencados principalmente em seu artigo 5º, como em seu inciso X, o qual fundamenta a proteção da esfera privada de uma pessoa, esfera essa que engloba tanto a intimidade da pessoa humana quanto sua vida privada.

Isso nos faz observar o conceito desse direito à privacidade (*the right to privacy)* que não se resume ao simples "direito de ser deixado só" (*the right to be let alone*), se estendendo à tutela de dados sensíveis e seu controle pelo titular[14] e, especialmente, de "respeito à liberdade das escolhas pessoais de caráter existencial".[15] Os dados sensíveis são uma categorização específica de dados, sendo aqueles em que se conhecidas e submetidas a

[12]BONAVIDES, Paulo. **Curso de Direito Constitucional**. 29 ed. São Paulo: Malheiros Editores, 2014. p. 516
[13] HESSE apud BONAVIDES, Paulo. **Curso de Direito Constitucional**. 29 ed. São Paulo: Malheiros Editores, 2014. p.514.
[14] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). **Revista de Direitos e Garantia Fundamentais**, Vitória, v. 19, n. 3, 2018.
[15] LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003. p. 9.

tratamento, podem resultar em uma lesão ao titular a depender da configuração social a que se insere.[16]

Para Stefano Rodotá, é fundamental que haja uma tutela rigorosa dos dados sensíveis, pois esses transformaram-se em conteúdo essencial para a concretização do princípio da igualdade e da não discriminação. Mais ainda, a tutela de dados pessoais sensíveis permite a efetivação, a depender de sua natureza, do direito à saúde (dados genéticos ou sanitários), do direito à liberdade de expressão e de comunicação (dados sobre opiniões pessoais), do direito à liberdade religiosa e de associação (dados sobre convicção religiosa). Assim, para o autor italiano, "(…) a associação entre privacidade e liberdade torna-se cada vez mais forte",[17] reconhecendo, desta maneira, a natureza de direitos fundamentais aos dados pessoais sensíveis.[18]

Fica evidente então o caráter principiológico e fundamental da tutela dos dados pessoais, que encontram respaldo constitucional e, ainda, dentro do essencial princípio da dignidade humana. Isso por tratar-se de informações individuais e de caráter subjetivamente íntimo, que condizem com a vida (individual e coletiva) e a personalidade de cada ser humano, devendo-se prezar pela garantia e proteção ao seu direito legal de dispor do controle sobre essas informações.

[16] DONEDA, Danilo**, Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. pag. 143.
[17] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.153
[18] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). **Revista de Direitos e Garantia Fundamentais**, Vitória, v. 19, n. 3. 2018.

2. UMA BREVE CONTEXTUALIZAÇÃO HISTÓRICA DA BASE NORMATIVA SOBRE PROTEÇÃO DE DADOS PESSOAIS

A tradição jurídica europeia se vê como modelo indutor do molde das principais legislações no mundo ocidental, sendo referência em valores para aplicação e continuidade do Direito, como acontece com o emprego do Estado de Direito, dos direitos humanos, a diferenciação entre os espaços do direito e da religião, as técnicas de codificação, aplicados em todo o mundo por uma variedade de métodos. Não seria distinto, assim, com a disciplina da proteção de dados pessoais e da privacidade, que encontra grande respaldo nos ordenamentos alienígenas europeu e norte-americano escolhidos para a análise sobre o tema.

2.1.Modelo Europeu De Proteção De Dados Pessoais

A evolução do ordenamento jurídico europeu atinente à temática da privacidade e proteção de dados pessoais mostra que a tutela da informação de caráter pessoal do indivíduo é de grande relevância no que concerne aos direitos fundamentais do homem e do cidadão, principalmente quanto a garantia da dignidade e direitos intrínsecos à pessoa humana. Dessa forma, indica a Declaração Universal dos Direitos do Homem de 1948 (DUDH)[19], em seu Preâmbulo e art. 1º, que a dignidade é considerada uma característica intrínseca à pessoa humana, associada à liberdade e igualdade, direitos inalienáveis e de proteção essencial. Seguindo a linha de raciocínio, o artigo 8º da Carta dos Direitos Fundamentais da União Europeia assegurou a proteção dos dados de caráter pessoal de todas as pessoas como indivíduos.

Por conseguinte, é apropriado precisar que, com enfoque nos direitos e garantias fundamentais e com tendência predominante para a individualização e autonomia do instituto, há três décadas os europeus se empenharam em iniciativas legislativas para a tutela de dados pessoais. Isso resultou das lacunas existentes para regulamentação jurídica diante do desenvolvimento tecnológico, das inovações e da super velocidade digital, advindos, principalmente, após a Revolução Industrial, que se utilizou de novas formas de controle para atingir seus consumidores, ainda que essas formas de controle viessem a ferir os princípios quanto à privacidade desses.[20]

---

[19] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: http://www.un.org/en/universal-declaration-human-rights/. Acesso em: 12 abr. 2021.
[20] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados. 2 ed., São Paulo: Thomson Reuters Brasil, 2019, p.50.

Na década de 1970 foram apresentadas as legislações europeias precursoras do tema em análise, configurando como a primeira tentativa a Lei de Proteção de Dados Pessoais do Lande de Hesse, em 1970 na então Alemanha Ocidental[21], caracterizada por ser uma lei sucinta, concentrada em disciplinar a atividade de centros de processamento de dados de instituições e sujeitos submetidos à autoridade de Land, além de instituir o primeiro comissário para proteção de dados pessoais. Mediante o início da abordagem do assunto, em 1973 a Assembleia Consultiva do Conselho Europeu solicitou ao Comitê de Ministros que os países europeus adotassem princípios mínimos para nortear a nova temática envolvendo tecnologia e coleta de dados pessoais, de forma que se respeitasse o artigo 8º da Carta, então mencionada, da Convenção Europeia.[22]

Em 1977 foi promulgada uma lei federal alemã sobre a questão, porém a primeira lei nacional se deu na Suécia, um pouco antes, em 1973 com o objetivo de legislar acerca do controle de banco de dados, a qual deu seguimento para demais leis em outros países europeus, como a França, Dinamarca, Áustria, Noruega, Luxemburgo e Islândia, procurando uma solução que se enquadrasse em um contexto nacional, e não de forma isolada.[23]Assim, em 1973 foi publicada uma resolução sueca, o Estatuto para banco de dados – *Data Legen* 289, ou *datalog*[24]- como meio de incentivo para que os países europeus adotassem princípios que ordenassem as novas técnicas de coleta de informações, buscando a tutela da privacidade quanto à vida privada e familiar, ao domicílio e à suas respectivas correspondências dentro da informática.[25]

Posteriormente, seria possível uma uniformização legislativa supranacional acerca da temática, visto ser inconcebível a eficácia de uma proteção realizada apenas de forma interna, quando é evidente o fato de que o acesso e a transmissão dos dados de um indivíduo podem ser realizados por fora das delimitações territoriais delimitadas por um estado, necessitando de um enquadramento no contexto internacional dentro dos direitos humanos fundamentais, notado o risco de assimetrias territoriais.

---

[21] Danilo Doneda esclarece: "A primeira tentativa de elaborar um sistema de proteção de dados em um país europeu, conforme já mencionado, foi a Lei De Pessoais do Lande Hesse, em 1970 – Hessisches Datenschutzgesetz, na Alemanha Ocidental de então." (DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 191).
[22]Ibidem, p. 190
[23] Ibdem, p. 191
[24] Ibidem, p. 174
[25] Ibidem, p. 192

As iniciativas legislativas que surgiram em busca da tutela quanto ao tratamento de dados pessoais são separadas, na classificação proposta por Viktor Mayer-Schonberger, em gerações. Dessarte, a primeira geração de leis de proteção de dados pessoais é marcada pela convicção de que direitos e liberdades fundamentais estariam ameaçados pela coleta ilimitada de dados pessoais, que até então era realizada basicamente pelo Estado, servindo como uma espécie de medidor do equilíbrio de poderes dentro do estado mediante a utilização dos dados para planejamento e controle.[26] Essas leis buscavam conceder autorizações para a criação de bancos de dados e do seu controle a posteriori por órgãos públicos[27], não tratando da privacidade ainda, e chega aproximadamente até a lei federal da República Federativa da Alemanha, de 1977, mencionada anteriormente.[28]

A segunda geração dessas leis nasce a partir da segunda metade da década de 1970, tendo como marco inicial a lei francesa de proteção de dados de 1978 – *Informatique Libertés* – seguida da lei austríaca do mesmo ano, nomeada *Datenschutzgesetz*. A característica básica dessa geração é a estrutura normativa respaldada na privacidade e na proteção dos dados pessoais, considerada uma liberdade negativa de dever do próprio cidadão, sendo para ele um instrumento para defender e tutelar diretamente seus interesses diante da insatisfação do uso impróprio de suas informações.[29]

Com o forte avanço da globalização e das inovações tecnológicas e digitais, essa geração encontrou um empecilho: o fornecimento de dados do cidadão se tornou um requisito para participar ativamente da vida em sociedade e para se utilizar dos serviços tanto públicos quanto privados, e o impedimento da circulação desses dados acaba por excluir, de certa forma, a socialização de cada pessoa.[30]

Na década de 1980 surge uma terceira geração de leis, contendo em seu bojo a preocupação em garantir a efetividade na liberdade negativa (e sua extensão) atribuída ao cidadão, enquadrando-a no contexto em que é solicitado os seus dados e fornecendo os meios

---

[26] MAYER-SCHONBERGER, Viktor. 1997. apud DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019.p. 175

[27] SAMPAIO, José Adércio Leite. 1997. apud DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 176

[28] DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 176

[29] Ibidem, p. 177

[30] Ibidem, p. 178

adequados de proteção para as situações em que puder decidir e for intimidado por condições e custos de cunho econômico e social, como a exclusão social ou o não fornecimento de serviços explicados acima.[31]

No ano de 1981 o Conselho europeu resolveu tratar a matéria na Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, conhecida ainda pelos nomes de Convenção de Strasbourg, ou Convenção 108. A intenção era o planejamento de um prisma universalista para adoção de medidas protetivas para o tratamento de dados pessoais, além do entendimento de que tal proteção seria agora tratado como um tema de direitos humanos e fundamentais, atingindo os membros da União Europeia e os signatários da Convenção, onde inclusive países latino-americanos - como México, Argentina e Uruguai - ratificaram-na.[32]

Após a Convenção, vários países aderiram às recomendações, mas a principal menção dessa classificação geracional é a decisão do Tribunal Constitucional Alemão de 1983, que vincula ao conceito de autodeterminação informativa o caráter constitucional da proteção de dados pessoais e da privacidade. Além disso, são também parte dessa geração as leis de proteção de dados da Áustria, Noruega e Finlândia.[33]

A quarta e última geração de classificação é a das leis contemporâneas, que compõem o cenário de vários países e se caracteriza por tentar amenizar as desvantagens da tutela baseada na escolha individual e por procurar fortalecer a posição da pessoa que tem seus dados coletados em relação a quem os coleta, diminuindo o desequilíbrio entre as duas partes. Além disso, com a última geração iniciou-se uma diminuição no poder de autodeterminação informativa do indivíduo, uma vez que há dados que necessitam de intenso sigilo e proteção em seu tratamento, como os dados sensíveis, que necessitam de um tratamento especial, tratamento esse que é vedado em diversas legislações independentemente de haver ou não o consentimento.[34]

Além disso, pode-se observar uma gama maior de legislações com normas específicas sobre o tema na tentativa de acompanhar o desenvolvimento tecnológico e o fenômeno da globalização, envolvendo suas particularidades. Em 1994 foi feito o acordo

[31] DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 178-179
[32] Ibidem, p. 193/194
[33] Ibidem, p. 178
[34] Ibidem, p. 179

internacional TRIPS, que estabelece regras acerca da propriedade intelectual, dados pessoais e sua relação com o comércio, além de ter sido o responsável por criar a Organização Mundial do Comércio (OMC) e de servir para dar força a adoção de um modelo comum na Europa quanto a uma legislação acerca da tutela de dados pessoais e privacidade.[35] No ano seguinte, advém a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, abordando o tratamento de dados pessoais e sua livre circulação diante da proteção dos indivíduos, obrigando os legisladores dos estados-membros a aprovar normas em conformidade com as regras estabelecidas pela Diretiva. A Diretiva teve adesão rápida, sendo que em 1997, apenas dois anos depois, 18 países já seguiam suas diretrizes e a haviam incorporado em seus ordenamentos.[36]

Posteriormente, pôde-se contemplar o modelo contemporâneo europeu relativo à proteção de dados pessoais e à privacidade, a formação de um direito comunitário ordenado pelo Regulamento Geral de Proteção de Dados (GDPR), que entrou em vigor recentemente em 2018, tendo seu esqueleto uniformizado por meio da integração de diretivas amplas e detalhadas advindas da legislação interna de cada estado-membro da União Europeia,[37] os quais agora se encarregam em legislar internamente de forma a especificar aspectos de natureza operacional e de compor os espaços deixados em aberto pelo GDPR.[38]

2.2.Contextualização Da Privacidade No Modelo Norte-Americano

A abordagem estadunidense sobre privacidade é centenária, e deve ser analisada considerando a importância do papel que tem o país nas principais áreas envolvendo tecnologia e transferências internacionais desses dados e considerando os grandes avanços de seu sistema protetivo, o qual se desenvolveu de forma fracionada mediante um processo paulatinamente evolutivo[39]em uma complexa e sistemática estrutura federativa, com disposições legislativas e jurisprudências fragmentadas[40], que foram surgindo gradativamente, assentando-se em torno do chamado *right to privacy*, terminologia utilizada para diferentes funções, como observa

[35]DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019, p. 195
[36] Ibidem, p. 196
[37] Ibidem, p. 187
[38] Ibidem, p. 189
[39] WARREN, Samuel; BRANDEIS, Louis. 1890, apud DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019, p. 222
[40] DONEDA, op. cit., p 188

William Prosser,[41]e difundida para diversos países que adotam a *common law*, sistema correspondente ao dos Estados Unidos da América, e até mesmo para os que adotam o *civil law*.

A respectiva terminologia tem origem no impactante artigo jurídico *The Right to Privacy*, escrito por Warren e Brandeis em 1890, reconhecido como a primeira publicação do país a defender o direito à privacidade, além de ser o artigo jurídico mais citado na história dos Estados Unidos da América, sendo Fred Shapiro.[42] Sua publicação - feita na Harvard Law Review - introduziu o valor da privacidade do cidadão como questão fundamental para a liberdade e a democracia e determinante para o desenvolvimento social e jurídico do país[43]que hoje tem sua aplicação em variadas situações, como aponta Danilo Doneda :

> O *right to privacy* foi ou é evocado para regular, entre outros, a tranquilidade no próprio lar, o controle sobre informações pessoais, o controle sobre o próprio corpo, a liberdade de pensamento, o controle sobre a vigilância, a proteção da reputação, a proteção contra averiguações e interrogatórios abusivos, o planejamento familiar, a educação dos próprios filhos, o aborto, a eutanásia, entre outros.[44]

O artigo não obteve notório espaço para discussão até 1902, quando a Corte de Apelos de Nova Iorque negou expressamente a existência de um *right to privacy* no caso Robertson, conhecido por ter fotos suas utilizadas por terceiros para fins publicitários sem seu consentimento, causando grande angústia e sofrimento mental na adolescente do século XIX. Porém, após isso, começou um intenso debate acerca do direito à inviolabilidade da privacidade, resultando em uma posição favorável no caso *Pavesich* (o qual teve causa semelhante ao caso Robertson ao ter sua imagem utilizada por terceiros sem a devida permissão) pela Corte do estado da Geórgia, em 1905, acolhendo a ótica de Warren e Brandeis e fazendo com que as cortes norte-americanas passassem a defender a perspectiva da existência de um *right to privacy*, marcando a evolução jurisprudencial do tema da tutela dos valores que abrangem os pensamentos, sentimentos, emoções, dados pessoais, e até a imagem e o nome do indivíduo[45] não se limitando apenas a tutela da privacidade.[46]

---

[41] PROSSER, William. 1960, apud DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 222
[42] SHAPIRO, Fred. 1996, apud DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 223
[43] DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p 217
[44] Ibidem, p. 217

[46] FESTAS, David de Oliveira. **Do conteúdo patrimonial do direito à imagem**. Coimbra. 2009. p. 32

Atualmente, a privacidade se configura como um direito constitucional, ainda que não esteja prevista na Constituição, reconhecida por trabalho de modernização da Suprema Corte[47] como um direito implícito, fundamentando-o nas 1ª, 4ª e 14ª emendas de forma a proporcionar maior liberdade na elucidação da declaração de direitos, compondo a *common law*, através de dispositivos de *privacy torts (torts law)* voltados à responsabilidade civil, tendo ainda seu reconhecimento por legislação federal tratada pelo Congresso, e por legislação estadual, pelos estados norte-americanos.[48]

Por conseguinte, é significativo que se dê especial importância à 4ª Emenda uma vez que esta dispõe: O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas.[49]

Assim, o entendimento da época a relacionava a casos de invasão de propriedade alheia, ou seja, sem consentimento, o que foi questionado após o caso Olmstead v. United States não ser enquadrado na 4ª Emenda pelo fato de uma denúncia feita com base em uma investigação - feita pelo Governo Federal por meio de interceptação de "grampos" nos telefones de comerciantes ilegais em 1928 sem autorização judicial - realizada sem que os agentes adentrassem em domínios alheios sem autorização, levando a Suprema Corte a não enquadrar o caso no regulamento como pedido pela defesa.[50]

Empeçaram, então, discussões entre os membros da Corte, demonstrando descontentamento com a interpretação rasa da Emenda, sustentando que esta deveria ser flexibilizada de acordo com cada caso concreto, levando em consideração o impacto dos progressos técnicos das investigações e suas reais intenções, de forma a proteger a vida privada e os valores intrínsecos ao homem de invasões indesejadas, protegendo pessoas e não lugares.[51]

É natural que se aconteçam reformas nas legislações e que se altere suas interpretações, de forma a adequar aos valores da sociedade em seu espaço e tempo, no contexto vivido. Assim, a interpretação constitucional muda em contextos diversos do original de quando

---

[47] DONEDA, Danilo**. Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 225
[48] Ibidem, p. 217
[49] ESTADOS UNIDOS DA AMÉRICA. **Constituição dos Estados Unidos da América**. 1787. Disponível em: http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/constituicao-dos-estados-unidos-da-america-1787.html. Acesso em: 12 abr. 2020
[50] DONEDA, op. cit., p.226
[51] Ibidem, p. 227-228

foi escrita[52] como ensina *Lawrence Tribe* ao afirmar que "a fidelidade aos valores originais requer uma flexibilidade na interpretação textual" para que seja possível a ampliação do direito já existente[53] e a harmonização de velhos princípios com ideias modernas.[54]

De forma a propor maior equilíbrio entre privacidade e liberdade de expressão - modalidades igualmente protegidas -, a primeira encontrou respaldo constitucional por intermédio da 1ª Emenda, estabelecendo um balanceamento entre ambas ao limitar a liberdade de expressão quando esta viesse a ferir e julgar a vida íntima e particular.[55] De forma complementar à adequação constitucional, a 14ª Emenda foi desenvolvida de forma a tratar a privacidade diante da garantia da autonomia privada ou da liberdade, como no âmbito familiar, educacional, na concepção, etc. [56]

Após uma breve e sucinta passagem histórica relativa ao *right to privacy*, nota-se que apesar da grande colaboração jurisprudencial para aplicação e delimitação da tutela da privacidade, o ordenamento jurídico norte-americano não conta com uma consolidação de leis acerca do tema, tampouco uma preocupação específica com a privacidade para os dados pessoais e seu tratamento. Nesse sentido, Doneda observa que em casos que envolvam a expectativa de privacidade e a divulgação de dados pessoais, a posição que vem sendo tomada pela Corte Americana permite concluir que ela ainda não estabeleceu um direito á privacidade para os dados pessoais.[57]

2.3.Estrutura Normativa Brasileira Para Proteção De Dados Pessoais

Pode-se observar que a importante análise e discussão sobre a proteção de dados pessoais no ordenamento jurídico brasileiro se mostra muito recente, com tentativas legislativas ainda em evolução. O Brasil faz sua atual tutela jurídica acerca da privacidade e da proteção de informações e dados basicamente por meio de dispositivos constitucionais, infraconstitucionais e legislações esparsas, compondo um conjunto normativo apenas há pouco tempo, estando ainda em constante evolução o debate para aquiescência da matéria.

---

[52] DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 228
[53] TRIBE, Lawrence. apud DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 228
[54] EAMBAUGHT, Eugene. 1894, apud DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019, p. 229
[55] DONEDA, op. cit., p.232-233
[56] Ibidem, p. 234
[57] Ibidem, p. 236.

A proteção de dados vem como uma espécie de direito intrínseco a sua dignidade enquanto pessoa humana, proteção essa que deriva do direito fundamental à privacidade, expressamente tutelado na Constituição Federal de 1988, em seu art. 5º, inciso 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;" e ainda garante o direito à inviolabilidade para comunicações telefônicas, telegráficas ou de dados (art. 5º, XII). O dispositivo ainda se encarrega de estabelecer que é de direito de todos a possibilidade de acessar seus dados para conhecimento ou retificação (art. 5º, LXXII) por meio do chamado habeas data, e regula a proibição de invasão de domicílio (art. 5º, XI) e violação de correspondência (art. 5º, XII).

Busca-se preservar a autodeterminação e o livre desenvolvimento da personalidade do indivíduo atribuindo garantias de controle e liberdade para que ele possa delimitar o alcance que deseja que suas informações pessoais tenha sem que viole o que os doutrinadores chamam de direito da personalidade, que pode ser visualizada também no art. 21. do Código Civil[58] ao proteger a intimidade e a vida privada ao estabelecer que "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

A matéria dos dados pessoais propriamente ditos não encontra regulamentação constitucional com a especificidade que merece para uma melhor efetividade da tutela jurídica, a qual se mostra imprescindível diante da constante evolução tecnológica aliada ao acesso globalizado de informações, que hoje é uma realidade notoriamente possível. Assim sendo, no ano de 2019, foi realizada a Proposta de Emenda à Constituição nº 17 (PEC 17/2019) para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União quanto a legislação sobre proteção e tratamento de dados pessoais, de forma a proporcionar à matéria tratada uma isonomia para com os direitos fundamentais contidos no teor da Constituição.

O ordenamento brasileiro também vem atuando na proteção de dados pessoais e de seu tratamento principalmente por meio do remédio constitucional do habeas data e pelo Código de Defesa do Consumidor em seus artigos 43 e 44, onde são estabelecidos direitos e garantias para proteção de dados e informações pessoais presentes nas relações de consumo com o intuito de evitar sua utilização abusiva. Esses artigos são aliados a uma interpretação que

[58] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 12 abr. 2021.

se estende aos princípios referentes à proteção de dados pessoais e à proteção ao consumidor. Nesse sentido, Doneda busca exemplificar:

> Assim, por exemplo, entende-se a existência do princípio da finalidade, por intermédio da aplicação da cláusula da boa-fé objetiva e da própria garantia constitucional da privacidade, pelo qual os dados fornecidos pelo consumidor deverão ser utilizados somente para os fins que motivaram a sua coleta - o que pode servir como fundamentação para o reconhecimento de um princípio de vedação da coleta de dados sensíveis e da comercialização de bancos de dados de consumidores.[59]

O habeas data é uma ação constitucional, prevista no artigo 5º, inciso LXXII, da Constituição Federal de 1988. Sua utilização se dá quando se pretende assegurar o conhecimento de informações relativas ao titular, ou para retificação dos seus dados. Desse modo, trata-se de uma forma de assegurar um direito presente em nosso ordenamento jurídico. Para Gilmar Ferreira Mendes, o habeas data vem a se confundir com o direito, também constitucional, de autodeterminação informativa, conforme esclarece:

> Embora formulado de maneira pouco clara, é certo que o habeas data destina-se a proteger aspecto autônomo do direito de personalidade, o chamado direito de autodeterminação sobre informações – Recht auf informationelle Sebstbestimmung – , que assegura a cada indivíduo o poder de decidir quando e em que medida informações de índole pessoal podem ser fornecidas ou utilizadas por terceiros.[60]

A legislação infraconstitucional brasileira conta com leis esparsas que buscam proteger os dados pessoais, como a Lei da Informática (Lei nº 7.232 de 1984)[61], a qual dispõe sobre a Política Nacional de Informática. Em seu artigo 2º, inciso VIII, está expresso o princípio da proteção do sigilo dos dados armazenados de forma a atender o interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas. Além disso, em seu artigo 3º, parágrafo 2º, restou previsto que a exploração e a estruturação de bancos de dados devem ser reguladas por lei específica, o que foi produzido recentemente com a aprovação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13. 709 de 14 de agosto de 2018), também conhecida como LGPD.

A LGPD de 2018 entrou em vigor em setembro de 2020, estabelecendo um marco em matéria de proteção de dados pessoais no Brasil. A lei estipula parâmetros para que se estabeleça o uso de informações pessoais de maneira legal e adequada de forma a proteger

---

[59] DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 266

[60] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7. ed. rev. E atual. São Paulo: Saraiva, 2012. p. 1150-1151.

[61] BRASIL. **Lei nº 7.232, de 29 de outubro de 1984**. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L7232.htm#:~:text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20Nacional,Art. Acesso em: 12 abr. 2021.

seu titular. Desse modo, os dados pessoais dos brasileiros devem seguir um regramento geral quando coletados, tratados, armazenados e compartilhados, buscando primordialmente por sua preservação.

3. DIREITO E PRIVACIDADE: A LGPD E O CADASTRO ÚNICO NACIONAL NA GESTÃO GOVERNAMENTAL

3.1.O Compartilhamento de Dados sob o Decreto nº 10.046 de 2019

No dia 9 de outubro de 2019, o atual presidente Jair Bolsonaro assinou o Decreto nº 10.046/2019, regulamentando o compartilhamento de dados entre órgãos e entidades da administração pública federal e revogando expressamente o Decreto nº 8.789, de 29 de junho de 2016. O novo Decreto veio mais extenso que o anterior e categoriza o compartilhamento de dados em diversos níveis, facilitando o compartilhamento e cruzamento entre os bancos de dados da administração pública federal, além de trazer o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Cabe ressaltar que o Decreto nº 10.046/2019 foi alterado pelo Decreto 10.403 de 19 junho de 2020, acrescentando o §3º ao artigo 4º, e os incisos XI, XII e XIII, ao artigo 21, entrando em vigor na data de sua publicação.

O Cadastro Base do Cidadão nada mais é que uma base centralizada de dados pessoais de todos os brasileiros, o qual, inicialmente, consistirá em dados vinculados ao CPF (Cadastro de Pessoa Física) de cada pessoa, chamados de dados biográficos, como por exemplo o nome completo, data de nascimento, estado civil, filiação, sexo, endereço, naturalidade. Posteriormente, os órgãos públicos poderão enviar novos dados a serem acrescidos nessas informações, sendo de natureza biográfica, tendo como exemplo o título de eleitor, vínculos empregatícios, número de identificação social (NIS) e de inscrição no PIS (Programa de Integração Social) e PASEP (Programa de formação do Patrimônio do Servidor Público), ou ainda de natureza biométrica, tal como a palma da mão, as impressões digitais, o formato da face, a voz, a retina ou a íris dos olhos, e até mesmo a maneira de andar do cidadão.

No governo Temer, o revogado Decreto 8.789 de 2016[62] buscou facilitar o compartilhamento de dados, dispensando a necessidade de celebração de acordos e convênios entre órgãos e entidades e simplificando os mecanismos de compartilhamento e cruzamento de dados. Assim, a regulamentação liberava o compartilhamento automático de dados cadastrais entre órgãos e entidades da administração pública federal, conforme seu art. 3º, ou, no caso do

[62] BRASIL. **Decreto nº 8.789 de 29 de junho de 2016**. Revogado. Dispõe sobre o compartilhamento de bases de dados na administração pública. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm#:~:text=DECRETO%20N%C2%BA%208.789%2C%20DE%2029%20DE%20JUNHO%20DE%202016&text=Disp%C3%B5e%20sobre%20o%20compartilhamento%20de,que%20lhe%20confere%20o%20art. Acesso em: 12 abr. 2021.

art. 5º, devendo o compartilhamento acontecer de acordo com as necessidades demonstradas pelos órgãos, no caso de dados individualizados não cadastrais, sendo necessário que solicitassem o acesso ao responsável, com a descrição dos dados demandados e da finalidade de uso. Conforme este Decreto, uma vez que as informações fossem compartilhadas, não poderiam ser repassadas sem autorização expressa pelo órgão responsável.

O novo Decreto, objeto de estudo do presente trabalho, trouxe mudanças significativas quanto a essa facilitação no procedimento de compartilhamento de dados. Nesse sentido, o art. 1º. caput, trata de ampliar o campo de abrangência de permissão de acesso à base de dados, incidindo não somente sobre os órgãos e entidades da administração pública federal direta, autárquica e fundacional como estabelecia o revogado Decreto de 2016, mas alcançando também os demais Poderes da União (Legislativo e Judiciário) em todas as suas instâncias (Estados, Municípios e Distrito Federal). Assim, embora se trate do acesso a dados no âmbito da administração pública federal, agora é possível que também aconteça o cruzamento de informações no âmbito judiciário e legislativo, e não somente no âmbito executivo. A implementação e a gestão do Cadastro Base do Cidadão serão de competência da Secretaria de Governo Digital, que é vinculada à Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

A nova regulamentação também se encarregou de incorporar novos elementos quanto às finalidades a que devem se ater os compartilhamentos e quanto a variedade de dados que podem ser compartilhados. No que diz respeito às finalidades, a novidade foi a inclusão do compartilhamento de dados visando "o aumento da qualidade e eficiência das operações internas da administração pública federal", o que torna as possibilidades ainda mais amplas, visto que as hipóteses previstas na regulamentação antiga previam o compartilhamento com fins: de simplificação da oferta de serviços públicos; da formulação, implementação, avaliação e monitoramento de políticas públicas; da análise da regularidade da concessão ou do pagamento de benefícios, ou da execução de políticas públicas; e da melhoria da qualidade e da fidedignidade dos dados constantes das bases dos órgãos e das entidades tratadas no artigo 1º do antigo Decreto. Essas quatro finalidades, antes previstas no art. 2º do Decreto nº 8.789 de 2016, foram preservadas e mantidas pelo Decreto nº 10.046 de 2019, acrescidas da quinta finalidade aqui descrita, e elencadas em seu art. 1º.

Quanto aos tipos de dados que têm permissão para compartilhamento, o novo Decreto amplia a dimensão de aplicação dos mecanismos de tratamento e compartilhamento de dados, tratando "dados cadastrais" não somente como identificadores, de pessoas físicas e jurídicas junto a órgãos públicos, como CPF, CNPJ, PIS, dados de nascimento e filiação,

endereço, etc. (art. 3º, §1º, Decreto nº 8.789/16); mas incluindo em suas implicações os "atributos biográficos", conforme art. 2º, inciso III, do Decreto nº 10.046/19.[63]

Assim, a regulamentação caracteriza os atributos biográficos como "dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios". Esses dados, portanto, compõem os dados cadastrais, além dos demais dados elencados nas alíneas que seguem o inciso III demonstrado acima. Cumpre ressaltar que não são somente esses os dados que poderão ser disponibilizados na base integradora do Cadastro Base do Cidadão, podendo a base integradora ser composta por dados cadastrais, atributos biográficos e, ainda, por atributos biométricos, todos provenientes da base de dados do CPF conforme dispõe o art. 18, §1º e §2º da lei em estudo.[64]

---

[63] Art. 2º Para fins deste Decreto, considera-se:
[...]
III - dados cadastrais - informações identificadoras perante os cadastros de órgãos públicos, tais como:
a) os atributos biográficos;
b) o número de inscrição no Cadastro de Pessoas Físicas - CPF;
c) o número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ;
d) o Número de Identificação Social - NIS;
e) o número de inscrição no Programa de Integração Social - PIS;
f) o número de inscrição no Programa de Formação do Patrimônio do Servidor Público - Pasep;
g) o número do Título de Eleitor;
h) a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação Nacional de Atividades Econômicas - CNAE; e
i) outros dados públicos relativos à pessoa jurídica ou à empresa individual;
(BRASIL. **Decreto nº 10.046 de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 12 abr. 2021)

[64] Art. 18. A base integradora será, inicialmente, disponibilizada com os dados biográficos que constam da base temática do CPF.
§ 1º Os atributos biográficos e cadastrais que inicialmente comporão a base integradora serão, no mínimo, os seguintes:
I - Número de inscrição no CPF;
II - Situação cadastral no CPF;
III - Nome completo;
IV - Nome social;
V - Data de nascimento;
VI - Sexo;
VII - Filiação;
VIII - Nacionalidade;
IX - Naturalidade;
X - Indicador de óbito;
XI - Data de óbito, quando cabível; e
XII - Data da inscrição ou da última alteração no CPF.
§ 2º A base integradora será acrescida de outros dados, provenientes de bases temáticas, por meio do número de inscrição do CPF, atributo chave para a consolidação inequívoca dos atributos biográficos, biométricos e cadastrais.
(BRASIL. **Decreto nº 10.046 de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de

Essa caracterização se mostra primordial para entender a estruturação e a dinâmica do compartilhamento de dados, os quais foram determinados em três diferentes níveis, sendo eles: aberto, restrito e específico. Essa distinção de níveis se deu com objetivo de estabelecer regras e estruturas para que os dados tenham alguma proteção quando do compartilhamento. O Cadastro Base será composto por uma grande base integradora de informações sobre os cidadãos e pelos mecanismos responsáveis pela transferência das informações para os órgãos e entidades da administração pública federal, enquanto os níveis descritos se encarregam de estabelecer regras e estruturas para o compartilhamento de dados que o Cadastro Base não alcance.

A classificação dos dados dentro dos três níveis ficou ao encargo do gestor do banco de dados ou da base de dados, conforme o art. 4º do decreto, devendo se ater a orientações e diretrizes definidas pelo Comitê Central de Governança de Dados, criado pelo decreto. Assim, a categorização do nível de compartilhamento deverá ser feita de forma detalhada pelo gestor de dados, com base na legislação, buscando tornar clara a situação de cada item de informação, devendo ser revista a cada cinco anos - contados da data do decreto - ou sempre que forem identificadas mudanças nas diretrizes que justificaram sua categorização. Além disso, se não houver categorização de um determinado dado que seja solicitado, o gestor deverá se encarregar de proceder a sua categorização ao responder a solicitação de permissão de acesso ao dado em questão.

Os três níveis de categorização de compartilhamento se distinguem de acordo com a confidencialidade dos dados, sendo o compartilhamento amplo o nível que demanda menor proteção em detrimento dos demais, tratando de dados públicos e não sujeitos a restrição de acesso, "cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação" (art. 4º, inciso I). Esses dados serão compartilhados sem que precise de uma autorização por parte do gestor, sendo acessíveis no Portal Brasileiro de Dados Abertos (art. 11, caput e §5º).

Na hipótese de o dado não estar disponível em formato aberto, o solicitante poderá requerer sua abertura ao gestor de dados, o qual poderá condicionar a abertura ao pagamento de custos adicionais ao solicitante, quando necessário e nos termos da lei (art. 11, §1º e §2º). Nessa acepção, o artigo 3º em seu inciso I, estabelece que a informação de natureza estatal deverá ser compartilhada de maneira ampla e pública, observando as restrições legais,

---

Dados. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 12 abr. 2021)

os requisitos de segurança da informação e comunicações e o disposto na Lei Geral de Proteção de Dados. Ainda, as medidas necessárias para manter a integridade e a autenticidade das informações deverão ser tomadas pelo solicitante/recebedor (art. 11, §4º).

O compartilhamento restrito, por sua vez, exige uma determinada reserva, posto que abrange dados protegidos por sigilo e que não podem ser acessíveis a todos, sem que se tenha qualquer discriminação (art. 4º, inciso II). Deste modo, será permitido o acesso a todos os órgãos e entidades elencados no art. 1º para a execução de políticas públicas, não sendo vedada a retransmissão e o compartilhamento desses dados entre esses (apenas no caso de estar a vedação prevista na autorização emitida pelo gestor), conforme dispõe o art. 12, §4º. Nesse caso, o compartilhamento ocorrerá mediante solicitação e em conformidade com as regras estabelecidas pelo Comitê (art. 12, caput).

No tocante ao compartilhamento específico, tem-se outro nível que resguarda o compartilhamento de dados visando respeitar o seu sigilo, no entanto, de forma ainda mais consistente. Dessarte, não são todos os órgãos e entidades elencados no decreto que terão direito de acesso como no compartilhamento restrito, sendo a modalidade de compartilhamento específico ainda mais rigorosa ao estabelecer que apenas órgãos e entidades específicos receberão a concessão, e ainda, somente nas hipóteses e para os fins previstos em lei.

A regulamentação condiciona essa modalidade de compartilhamento à indispensável permissão de acesso por parte do gestor de dados e ao atendimento de requisitos quando da solicitação (art. 14, incisos I e II do caput). Assim, a definição de requisitos mínimos (a serem atendidos pelo solicitante), além das regras de segurança da informação necessárias a serem adotadas quando do compartilhamento, se dará pelo próprio gestor, o qual deverá compatibilizar com os requisitos e regras adotados internamente por ele quando do tratamento da mesma informação (art. 14, §1º). Diante disso, o órgão interessado em acessar dados sujeitos a este nível de compartilhamento deverá, ao solicitar permissão ao gestor, "observar as condições e requisitos de acesso por ele definidos, nos termos do inciso III do caput do art. 4º, e deverá fundamentar o pedido e especificar os dados solicitados no maior nível de detalhamento possível" (art. 15, caput).

Recebida a solicitação, o gestor terá até 30 dias, contados da data do recebimento, para se manifestar. Após emitir seu parecer, se concedida a permissão, o recebedor de dados será responsável por implementar e seguir as regras de segurança assentadas no modelo de compartilhamento específico (art. 15, §§2º e 3º). Cabe ressaltar ainda que nesse nível, é vedada a retransmissão e o compartilhamento dos dados recebidos com outros órgãos ou entidades, excetuando-se nos casos em que a autorização concedida pelo gestor preveja

expressamente essa possibilidade, ou quando este conceda, posteriormente, permissão para isso (art. 14, §2º).

Destaca-se que todos os três níveis descritos seguirão disposições gerais para o compartilhamento de dados, além das particularidades de cada um. Então, uma dessas disposições diz respeito à dispensa de celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para que seja realizada a execução do compartilhamento de dados entre os sujeitos estabelecidos no artigo 1º (art. 5º). Outra disposição seria o prazo de 30 dias para se dar o acesso aos dados solicitados (art. 9º), além de outras expressas na Seção I do Capítulo III do decreto.

Para mais, o decreto em estudo trouxe a criação do Comitê Central de Governança de Dados, composto por representantes dos órgãos e entidades que compõem a administração pública federal, sem a previsão de que participem representantes da sociedade civil.[65]A participação no Comitê terá caráter de serviço público relevante, não remunerado, e com o dever de se reunir, em caráter ordinário, a cada dois meses e, em caráter extraordinário, sempre que for solicitado por seu Presidente ou por solicitação de um de seus membros, sendo o quórum de reunião correspondente a dois terços de seus membros, e o quórum de aprovação estabelecido por consenso. É ele que definirá parâmetros para as classificações de bancos de dados e bases de dados.

A competência se qualifica, principalmente, pelo poder de deliberação sobre as orientações e diretrizes a serem adotadas ao categorizar os três níveis de compartilhamento de dados (além da forma e meio de publicar essa categorização) como as regras e requisitos para o compartilhamento restrito, os princípios a serem observados no que diz respeito a preservação do sigilo e da segurança, a compatibilidade dos compartilhamentos com as políticas de segurança da informação, a inclusão de novos dados ao Cadastro Base do Cidadão, a avaliação

[65] Art. 22. O Comitê Central de Governança de Dados é composto por representantes dos seguintes órgãos e entidade
I - dois do Ministério da Economia, dentre os quais um da Secretaria Especial de Desburocratização, Gestão e Governo Digital, que o presidirá, e um da Secretaria Especial da Receita Federal do Brasil;
II - um da Casa Civil da Presidência da República;
III - um da Secretaria de Transparência e Prevenção da Corrupção da Controladoria-Geral da União;
IV - um da Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República;
V - um da Advocacia-Geral da União; e
VI - um do Instituto Nacional do Seguro Social.
(BRASIL. **Decreto nº 10.046 de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 12 abr. 2021)

quanto à fidelidade dos dados dispostos, dentre outras orientações instituídas no artigo 21 do decreto.

3.2.O Decreto nº 10.046/2019 Diante da Lei Geral de Proteção de Dados Pessoais

3.2.1. Da Necessidade e da Finalidade do Compartilhamento

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), foi aprovada no Governo Temer, em 2018, e entrou em vigência apenas em 18 de setembro de 2020, representando um marco histórico na regulamentação de dados no país, mudando o cenário de coleta, armazenamento e disponibilização de informações por instituições privadas e públicas, buscando garantir direitos fundamentais de liberdade e de privacidade e devendo ser seguida por toda a organização político-administrativa da República Federativa do Brasil.

A LGPD busca regulamentar o tratamento de dados pessoais visando resguardar a intimidade e privacidade da pessoa, vindo a prever o tratamento e compartilhamento de dados pessoais pela administração pública, conforme necessário para a execução de políticas públicas (art. 7), destinando o Capítulo IV somente à normatização do tratamento de dados pelo poder público. Ainda é uma das bases legais estabelecidas pela LGPD que o tratamento de dados pessoais sensíveis sem o consentimento do titular venha a acontecer nas hipóteses em que seja estritamente necessário e indispensável para a execução de políticas públicas previstas em leis ou regulamentos. No entanto, cabe ressaltar que a referida lei estabelece diretrizes e princípios de suma importância a serem observados no regime de proteção de dados, previstos nos seus artigos 2º e 6º, os quais devem ser aplicados sempre que dados forem objetos de tratamento, ainda que pelo poder público.

Os princípios estão elencados nos incisos que seguem o artigo 6º, estabelecendo que as atividades de tratamento de dados deverão observar, além da boa-fé: a finalidade da realização do tratamento, a adequação deste com as finalidades, a necessidade do tratamento, o livre acesso aos titulares dos dados, a qualidade dos dados juntamente com a adoção de medidas preventivas que mantenham a exatidão e clareza desses, a transparência aos titulares sobre todo o tratamento dos dados, a utilização de medidas de segurança eficazes na proteção dos dados tratados, a intolerância de tratamento dos dados com fins ilícitos e abusivos, além da

responsabilização e prestação de contas quanto à observância e cumprimento das normas de segurança.

O princípio da necessidade, previsto no art. 6º inciso III (da LGPD), é descrito pela lei como a "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". No mesmo sentido, o art. 23, inciso I, da mesma lei dispõe que o tratamento de dados pessoais pelo poder público deverá atender sua finalidade e devendo obrigatoriamente informar "as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos".

Assim, tem-se que a LGPD resguarda o tratamento de dados pessoais realizados pelo poder público, exigindo que seja demonstrada sua necessidade e o cumprimento de sua finalidade de forma clara e atualizada, prestando as devidas informações ao titular de forma acessível. No entanto, o Decreto 10.046/2019, editado após a aprovação da lei, demonstra algumas inconsistências quanto a esses princípios, principalmente ao prever a necessidade apenas quando do compartilhamento específico, desconsiderando sua aplicação nos demais compartilhamentos autorizados em sua regulamentação, tornando ainda mais ampla a possibilidade de disponibilização de dados sem exigir uma preocupação com a necessidade e finalidade de acesso por parte do solicitante.

O referido Decreto não desconsidera a Lei Geral de Proteção de Dados completamente, determinando em seu art. 3º que o nível de compartilhamento amplo de dados deverá respeitar as restrições e os requisitos previstos na lei, quando do seu processo de tratamento e acesso, devendo respeitar o art. 23 da LGPD, devendo respeitar a condição de ser o tratamento de dados pessoais, realizado pelas pessoas jurídicas de direito público, transparente quanto a sua necessidade e de respeitar sua finalidade, fornecendo conhecimento quanto aos procedimentos e práticas empregados.

Na mesma linha de raciocínio são as exigências do art. 26 da mesma lei, que estabelece a indispensabilidade de que o compartilhamento desses dados esteja em conformidade com os princípios listados no artigo 6º da lei, além de ter o compromisso de atender às finalidades específicas de execução de políticas públicas. Todavia, isso não é considerado na regulamentação disposta pelo Decreto, a qual se mostra controversa, isso porque esse último tem como diretriz o mais amplo compartilhamento de dados entre os órgãos e entidades públicas, desafiando a necessidade e a finalidade para sua execução.

Observa-se, portanto, que a compatibilidade do Decreto 10.046/2019 com a LGPD se mostra questionável, uma vez que o primeiro demonstra ter como diretriz o mais amplo compartilhamento de dados dos cidadãos, tanto no nível de compartilhamento amplo quanto no restrito, onde a permissão para acesso aos dados se dá de maneira superficial, sem uma finalidade específica, seguindo em desacordo com as orientações acerca de dados pessoais pré-estabelecidas. Como consequência, tem-se a incidência da formação de uma insegurança jurídica e da falta de transparência no campo em questão.

Nesse sentido, essa pesquisa se mostra de relevância ímpar no atual contexto brasileiro, observando a importância de serem analisadas as legislações que buscam regular a proteção de dados pessoais. Ressalta-se que há países que já adotam sistemas estruturais semelhantes ao Cadastro Nacional Único, como Estônia e Índia, além da China, que se utiliza dos dados sensíveis do cidadão de forma corriqueira para fins de segurança pública e aperfeiçoamento de seu processo penal.

A China é um ótimo exemplo a ser citado, porque além da utilização do compartilhamento de informações para fins de segurança, ela vem mostrando um comportamento questionável diante da base de dados de cidadãos. O Estado Chinês anunciou em 2014 um sistema que se chama "social scoring" (sistema de crédito social), por meio do qual será verificada a "fidelidade" dos 1,3 bilhão de chineses aos princípios e valores do Estado e, a partir disso, será determinado se um cidadão chinês (ou até pessoa jurídica estrangeira com sede na China) terá direito ao acesso a determinadas políticas públicas, como serviços médicos e hospitalares, quais escolas seus filhos poderão ser matriculados, dentre outros, fazendo uma classificação única e pública dos comportamentos daquela pessoa. O sistema seria implementado até 2020, sendo de vinculação obrigatória a todos[66].

3.2.2. Do Compartilhamento de Dados Pessoais Sensíveis

Segundo a Lei Geral de Proteção de Dados Pessoais, há uma classificação de dados pessoais que identifica uma intimidade maior da vida pessoal do cidadão, denominada "dado pessoal sensível". Esse tipo de informação, segundo o artigo 5º, inciso II, da LGPD, diz respeito a "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política,

[66] O PLANO chinês para monitorar e premiar o comportamento de seus cidadãos. **BBC News**. Disponível em: https://www.bbc.com/portuguese/internacional-42033007. Acesso em: 12 abr. 2021.

LEMOS, Ronaldo. Base que reúne dados de brasileiros ajuda ou atrapalha? **Folha de São Paulo**. Podcast gravado em 2019. disponível em: https://www1.folha.uol.com.br/podcasts/2019/10/podcast-discute-eficiencia-da-base-que-reune-dados-pessoais-dos-brasileiros.shtml. Acesso em: 12 abr. 2021.

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". Tratando especificamente sobre dados sensíveis, leciona Doneda que:

> A prática do direito da informação deu origem á criação de uma categoria específica de dados, os dados sensíveis. Estes seriam determinados tipos de informação que, caso sejam conhecidas e submetidas a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentaria maiores riscos potenciais do que outros tipos de informação. Entre estes dados, tidos como sensíveis, estariam as informações sobre raça, credo político ou religioso, opções sexuais, histórico médico ou dados genéticos de um indivíduo.[67]

O tratamento de dados pessoais sensíveis possui regulamentação específica, disposta no Capítulo II, Seção II, artigos 11 ao 13, da Lei Geral de Proteção de Dados Pessoais (LGPD de 2018). Dessa maneira, de acordo com o artigo 11, o compartilhamento desses dados só poderá ocorrer com o consentimento do titular, devendo ser demonstrada de forma clara e específica sua finalidade. De forma excepcional, esse consentimento pode ser dispensado nas hipóteses previstas no inciso II do art. 11, sendo que em sua alínea 'b' há presciência da dispensa do consentimento quando do tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos, realizado por parte da administração pública.

Portanto, constata-se que a lei inclui dados biométricos como informações sensíveis, cujo tratamento compartilhado só deve acontecer mediante consentimento dos envolvidos, excetuando, dentre outras circunstâncias, quando da necessidade para execução de políticas públicas. Sem embargo, verifica-se que mais uma vez a lei demonstra ser imprescindível a observância do princípio da necessidade, não sendo permitido o tratamento amplo e indiscriminado de dados sensíveis com a mera justificativa de desempenho das atividades da administração pública.

Neste seguimento, o renomado jurista italiano Stefano Rodotá, ao tratar do direito á proteção de dados na Carta dos Direitos Fundamentais da União Europeia, destaca que uma forte tutela dos dados sensíveis se tornou componente essencial da igualdade, para evitar que a coleta destas informações específicas possa se transformar em instrumento de discriminação da pessoa. Diante disso, para Rodotá, o momento atual europeu, se vê cada vez mais claro a sedimentação de uma associação entre liberdade e privacidade, de forma a entender

---

[67] DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. p. 142.

pela tutela das escolhas existenciais contra o controle público e a estigmatização social. [68]No mesmo sentido, Rodotá enfatiza que:

> No quadro da privacidade, a dignidade é especificada como um conceito que sintetiza os princípios do reconhecimento da personalidade e da não redução da pessoa á mercadoria, do respeito ao outro, da igualdade, da solidariedade, e da não interferência nas escolhas de vida, da possibilidade de agir livremente na esfera pública. Á privacidade é estranha a pretensão de impor valores. Não se impõem calores. Colocam-se premissas para a autonomia e para o respeito recíproco.[69]

Nota-se, portanto, que o Decreto 10.046/2019 visa permitir indiscriminadamente o compartilhamento de dados pelo poder público, de forma que dados pessoais de todos os tipos serão acessíveis por órgãos e entidades em todos os três níveis de compartilhamento pré-estabelecidos, nos quais se demonstra certo critério apenas quanto o grau de sigilo. Tão logo, acaba por permitir, em seu art. 18, §2º, inclusive, que sejam acrescidos dados biométricos à base integradora, tratados pela lei como dados sensíveis.

O transcorrer de toda essa dinâmica de tratamento e compartilhamento segue sem que se exija a anuência e o conhecimento do titular, cujos dados serão acessados por parte da administração pública, pelos demais Poderes da União e pelos demais entes federativos, sem que seja notificado do fato do tratamento dos dados ou da necessidade e finalidade de fazê-lo. Dessarte, o Decreto em estudo demonstra, repetidamente, ser incoerente com a lei, afrontando princípios e estabelecendo regras em desacordo com sua regulamentação.

---

[68] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 236

[69] Ibidem, p. 237

4. O CADASTRO BASE DO CIDADÃO SOB A PERSPECTIVA CONSTITUCIONAL

Consoante o que foi apresentado anteriormente, o Decreto 10.046/2019 demonstra incoerências com a Lei Geral de Proteção de Dados, o que pode ser similarmente verificado no que tange os fundamentos da "inviolabilidade da intimidade" e da "autodeterminação informativa". Esses fundamentos encontram-se tutelados na Constituição Federal de 1988, em seu artigo 5º, incisos X e XII, referindo-se à inviolabilidade da intimidade e da vida privada como "proteção da privacidade", e ainda, tratando da inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, ou seja, a inviolabilidade informativa.

Ainda, em 2019 foi apresentada a Proposta de Emenda à Constituição (PEC) nº 17, com o objetivo de incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, bem como fixar a competência privativa da União para legislar e tratar sobre a matéria. Importante ressaltar que a PEC 17/2019 foi aprovada e se encontra em espera para proceder à votação no Plenário, sendo que a justificativa para a sua apresentação seria de fornecer maior proteção aos indivíduos, tornando uma garantia constitucional, e de, ao estabelecer a competência restrita à União, criar uma legislação uniforme a ser adotada por todos os entes federativos, o que evitaria uma insegurança jurídica diante de legislações estaduais e municipais sobre o assunto, que possam vir a ser aprovadas eventualmente.

De acordo com Danilo Doneda, a aprovação da proposta poderá proporcionar certa "equalização" entre uma série de direitos fundamentais que possuem repercussão direta sobre dados pessoais, como o direito à privacidade, informação e transparência, sendo que a inserção de um direito à proteção de dados de forma explícita no rol de direitos fundamentais da Constituição da República proporciona uma isonomia entre esses direitos, os quais se mostram fundamentais para a proteção de liberdades fundamentais[70].

4.1. A Problemática do Compartilhamento de Dados diante da Inviolabilidade da Intimidade e da Autodeterminação Informativa

Conforme os ensinamentos de René Ariell Dotti, no que tange à intimidade, pode-se caracterizá-la como "a esfera secreta da vida do indivíduo na qual este tem o poder

[70] DONEDA, Danilo, **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019. pag. 264.

legal de evitar os demais"[71], sendo que o direito à sua inviolabilidade, segundo Paulo José da Costa Jr.:

> São tutelados dois interesses, que se somam: o interesse de que a intimidade não venha a sofrer agressões e o de que não venha a ser divulgada. O direito, porém, é o mesmo. (...) No âmbito do direito à intimidade, portanto, podem ser vislumbrados estes dois aspectos: a invasão e a divulgação não autorizadas da intimidade legitimamente conquistada.[72]

Dessa forma, a Carta Magna busca garantir como direito fundamental do homem a não invasão à esfera íntima da pessoa, por ser onde se guardam os segredos e particularidades de caráter moral e íntimo seu próprio, consoante à sua vida privada[73], o que leva a outra incoerência do Decreto 10.046/2019. Isso porque a criação de uma base de dados centralizada, seja o Cadastro Base do Cidadão ou outras bases temáticas, onde ficam dispostos dados pessoais de natureza cadastral, de natureza biográfica e até mesmo de natureza biométrica (dados sensíveis), com acesso amplo pelo poder público, demonstra exatamente a violação desse preceito constitucional, em virtude do acréscimo de dados notoriamente íntimos de maneira indiscriminada e de seu compartilhamento que, independentemente se amplo, restrito ou específico, não observa os princípios da necessidade e finalidade, previstos na LGPD como forma de maior proteção ao indivíduo.

Relacionado a inviolabilidade à intimidade, tem-se à inviolabilidade informativa, onde cuida-se, para a maioria da doutrina, de aspecto do direito à privacidade, também prevista no art. 5º, da Constituição Federal de 1988. A inviolabilidade da informação busca resguardar as informações de diversos gêneros ligados na esfera da vida privada e pública de um indivíduo, de forma que o compartilhamento dessas informações exija cautela a fim de evitar danos ao indivíduo. Em acordo com a Constituição, foi determinado o fundamento infraconstitucional da autodeterminação informativa, advinda da Lei nº 13.709 de 2018 (LGPD), prevista em seu art. 2º, inciso II. Canotilho consagra este direito fundamental como sendo a "faculdade de o particular determinar e controlar a utilização de seus dados pessoais" diante do perigo da exposição de sua privacidade[74].

Nessa acepção, o Supremo Tribunal Federal (STF), no julgamento que se deu em apreciação de medida cautelar no processo da Ação Direta de Inconstitucionalidade (ADI)

---

[71] DOTTI, René Ariel. **Proteção da Vida Privada e Liberdade de Informação**. São Paulo: Ed. RT, 1980.
[72] COSTA JR., Paulo José, **O Direito de Estar Só**: Tutela Penal da Intimidade, 1995, p.34.
[73] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 38ª edição. Ed. Malheiros, 2014, p. 210.
[74] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição**. 5. ed. Coimbra: Almedina, 2002. p. 507.

de nº 6387[75] reconheceu em decisão histórica a existência do direito à autodeterminação informativa no ordenamento jurídico brasileiro. A ADI foi proposta pelo Conselho Federal da Ordem dos Advogados do Brasil contra a Medida Provisória nº 954/2020, pleiteando pela "presença no ordenamento constitucional brasileiro do direito fundamental à autodeterminação informativa, a ensejar tutela jurisdicional quando sua violação não for devidamente justificada por motivo suficiente, proporcional, necessário e adequado e com proteção efetiva do sigilo perante terceiros, com governança que inclua o Judiciário, o Ministério Público, a Advocacia e entidades da sociedade civil".

A relatora da decisão, Ministra Rosa Weber, se baseou no artigo *The Right to Privacy*, escrito por Samuel D. Warren e Louis D. Brandeis, juízes da Suprema Corte Norte-Americana, assinalando que "já se reconhecia que as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima". [76]

Por conseguinte, a ministra declarou que "decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais". À vista disso, o Tribunal Pleno do STF referendou o entendimento da relatora, proclamando decisão histórica ao reconhecer expressamente que o direito à autodeterminação informativa é assegurado aos brasileiros pela Constituição Federal de 1988, e não somente no âmbito infraconstitucional da LGPD, sendo direito do indivíduo ter controle sobre seus dados pessoais, sendo exceção apenas quando legislação determinar de forma distinta e minuciosa

A autodeterminação informativa se traduz, então, na proteção constitucional do direito de que dispõe todo indivíduo em ter a faculdade de exercer controle sobre seus dados e informações pessoais, ainda que de maneiras distintas, e de tomar conhecimento sobre os aspectos de seu tratamento e compartilhamento, frente aos direitos da personalidade[77] e da

---

[75] BRASIL. Supremo Tribunal Federal. **Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE**. 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442823. Acesso em: 12 abr. 2021

[76] BRASIL. Supremo Tribunal Federal. **ADI 6387**. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 12 abr. 2021

[77] RODRIGUEZ, Davara. Apud. LIMBERGER, Temis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. pag. 103

dignidade humana sujeitos ao impacto tecnológico das mudanças por que passam a sociedade e a informática. Ademais, esse preceito fundamental também busca limitar o legislador ao proibir que os dados pessoais acessados pelo Estado sejam utilizados para fins diversos daqueles previstos na legislação.[78]

Isso demonstra que o princípio da finalidade previsto na LGPD está constitucionalmente implícito, devendo ser observado em consonância com a proteção à privacidade, perante a autodeterminação informativa, e devendo ser garantido ao titular das informações o seu direito de liberdade de decisão para dispor suas informações pessoais, sendo que, se permitido o acesso a elas, o recebedor deverá se ater aos fins específicos aos quais se destinam o tratamento e o compartilhamento de dados pessoais. Desse modo, entende-se que a finalidade funciona como um instrumento social que busca proteger o a privacidade do cidadão, conforme se posiciona Rodotá:

> Pretende-se evitar que as escolhas de vida sejam condicionadas por pressões públicas e privadas, permitindo assim a cada um agir em plena autonomia. Isto explica por que as próprias exigências de segurança pública não podem jamais reduzir a privacidade a formas incompatíveis com as características próprias de uma sociedade democrática; e por que a lógica econômica não pode legitimar a redução das informações pessoais a mercadorias.[79]

Dessarte, sendo a autodeterminação informativa um direito fundamental (art. 5º, inciso XII) intrínseco à proteção da privacidade, de forma a garantir a liberdade de decisão e o resguardo da intimidade e da personalidade, ela está em acordo com os princípios da necessidade e finalidade dispostos na Lei Geral de Proteção de Dados, sendo que a violação desses gera uma afronta à autodeterminação informativa. Infere-se, portanto, ser esse outro aspecto em que o Decreto nº 10.046/2019 se assevera como inconsistente não só quanto à LGPD, mas quanto à Constituição da República Federativa do Brasil.

---

[78] PIEROTH, Bodo. SCHLINK, Bernhard. **Direitos Fundamentais**. São Paulo: Saraiva, IDP, 2012.
[79] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 237

CONSIDERAÇÕES FINAIS

Conforme explanado no desenvolvimento dessa dissertação, o Decreto nº 10.046 de 9 de outubro de 2019 impõe a implementação do Cadastro Base do Cidadão como um banco de dados de acesso compartilhado entre todos os órgãos e entidades da administração pública federal direta, autárquica e fundacional, e os demais Poderes da União. Esse acesso a dados pessoais, sejam eles de natureza cadastral, biográfica ou biométrica, são constitucionalmente protegidos e possuem uma regulamentação própria pela Lei Geral de Proteção de Dados Pessoais.

O tratamento dessas informações deve seguir uma série de diretrizes e princípios dispostos no ordenamento jurídico brasileiro, de forma a resguardar o direito da intimidade do cidadão e de proteger sua vida privada. O fundamento disso é que o direito à proteção de dados é um direito garantidor do exercício da privacidade e da tutela dos direitos da personalidade. No entanto, o Decreto estudado demonstra se omitir quanto à existência dessas normas, além de enfrentar princípios que devem ser seguidos quando do tratamento de qualquer dado pessoal, ainda que pelo Poder Público.

Desse modo, os princípios da finalidade e da necessidade, previstos na Lei Geral de Proteção de Dados Pessoais como uma forma de limitar a gestão de informações dos cidadãos, são contrariados pelo Decreto analisado. Isso por consequência da previsão de permissão para compartilhamento de diversos dados dos brasileiros, acessíveis por todos os órgãos e entidades da federação, como forma de implementar políticas públicas, sem qualquer limitação.

A única preocupação se faz quanto ao nível de sigilo das informações, sendo que dados de maior confidencialidade são compartilhados dentro das políticas dos compartilhamentos chamados por restrito e específico, mas, no entanto, sem o conhecimento ou a permissão de seu titular para isso. Essa conjuntura acaba por infringir os princípios constitucionais quanto a dignidade humana, além da inviolabilidade da intimidade e ao direito de autodeterminação informativa, expondo as informações do titular, ainda que sensíveis, de forma a ferir sua vida intima e privada, além de retirar seu poder de decisão sobre quais informações deseja que sejam tratadas e componham uma base centralizada de dados de acesso tão amplo.

Posto isso e diante de todo o explanado nesse trabalho de conclusão de curso, considera-se que o Decreto 10.046 de 2019 é um tanto controverso quanto as normas gerais dispostas no ordenamento jurídico brasileiro, por violar direitos fundamentais previstos na Carta Magna de 1988. Sendo assim, a permissão de compartilhamento estabelecida e a criação de um Cadastro Base do Cidadão geram uma insegurança jurídica e o risco de danos á dignidade humana dos brasileiros.

REFERÊNCIAS

BONAVIDES, Paulo. **Curso de Direito Constitucional.** 29 ed. São Paulo: Malheiros Editores, 2014.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 12 abr. 2021.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 12 abr. 2021.

BRASIL. **Decreto nº 8.789 de 29 de junho de 2016**. Revogado. Dispõe sobre o compartilhamento de bases de dados na administração pública. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm#:~:text=DECRETO%20N%C2%BA%208.789%2C%20DE%2029%20DE%20JUNHO%20DE%202016&text=Disp%C3%B5e%20sobre%20o%20compartilhamento%20de,que%20lhe%20confere%20o%20art. Acesso em: 12 abr. 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 12 abr. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 abr. 2021.

BRASIL. **Lei nº 7.232, de 29 de outubro de 1984**. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L7232.htm#:~:text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20Nacional,Art. Acesso em: 12 abr. 2021.

BRASIL. Supremo Tribunal Federal. **ADI 6387**. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 12 abr. 2021

BRASIL. Supremo Tribunal Federal. **Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE**. 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442823. Acesso em: 12 abr. 2021

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição**. 5. ed. Coimbra: Almedina, 2002.

COSTA JUNIOR., P. J. da. **O direito de estar só**: tutela penal da intimidade. 4. ed. São Paulo: Revista dos Tribunais, 2007.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law** [EJJL], v. 12, n. 2, p. 91-108, 13 dez. 2011.

DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados, 2 ed., São Paulo: Thomson Reuters Brasil, 2019.
DOTTI, René Ariel. **Proteção da Vida Privada e Liberdade de Informação**. São Paulo: Ed. RT, 1980.

ESTADOS UNIDOS DA AMERICA. **Constituição dos Estados Unidos da América.** 1787. Disponível em: http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/constituicao-dos-estados-unidos-da-america-1787.html. Acesso em: 12 abr. 2021.
FESTAS, David de Oliveira. **Do conteúdo patrimonial do direito à imagem**. Coimbra, 2009.

LEMOS, Ronaldo. "Base que reúne dados de brasileiros ajuda ou atrapalha?". **Folha de São Paulo**. Entrevista em formato de Podcast. 2019. Disponível em: https://www1.folha.uol.com.br/podcasts/2019/10/podcast-discute-eficiencia-da-base-que-reune-dados-pessoais-dos-brasileiros.shtml. Acesso em: 12 abr. 2021. Acesso em: 12 abr. 2021.

LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003.

LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ: novas práticas em informação e conhecimento**, Curitiba, v. 2, n. 1, p. 60-76, jan./jun. 2013. Disponível em: <http://www.atoz.ufpr.br>. Acesso em: 12 abr. 2021.

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

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7. ed. São Paulo: Saraiva, 2012.

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

O PLANO chinês para monitorar e premiar o comportamento de seus cidadãos. **BBC News**. 2017. Disponível em: https://www.bbc.com/portuguese/internacional-42033007 . Acesso em: 12 abr. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: http://www.un.org/en/universal-declaration-human-rights/. Acesso em: 12 abr. 2021.

PIEROTH, Bodo; SCHLINK, Bernhard. **Direitos Fundamentais**. São Paulo: Saraiva, IDP, 2012.

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

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 38ª edição. Ed. São Paulo: Malheiros, 2014.