FUNDAÇÃO PRESIDENTE ANTÔNIO CARLOS DE UBÁ
FACULDADE DE DIREITO
2019

O CONTROVERSO DECRETO Nº 10.046 DE 2019 FRENTE À LEGISLAÇÃO BRASILEIRA DE PROTEÇÃO DE DADOS

Jardel Ciotti da Silva Lima – jardelciotti@hotmail.com

Alexandre Ribeiro da Silva – alexandreribeiroadv@gmail.com

RESUMO

O presente trabalho tem por objeto as relações entre o Marco Civil da Internet e seu decreto regulamentador, a Lei Geral de Proteção de Dados e o conflituoso Decreto nº 10.046 de 2019. A legislação brasileira assegura o direito à privacidade e à proteção de dados pessoais, estabelecendo fundamentos, princípios e regras concernentes à proteção de dados, além de instituir normas com a finalidade de garantir seu cumprimento. O Decreto nº 10.046 traz disposições contrárias à legislação, comprometendo a privacidade e demais direitos dos titulares de dados pessoais. Deste modo, será constatada a necessidade da alteração dos dispositivos contrários à proteção da privacidade e à proteção de dados presentes no Decreto nº 10.046.

Palavras-chave: Proteção de dados pessoais. Privacidade. Decreto nº 10.046 de 2019. Marco Civil da Internet. Lei Geral de Proteção de Dados.

ABSTRACT

The present work aims the relationships between the Internet Milestone and its regulatory decree, the General Data Protection Law and the conflicting Decree No. 10.046 of 2019. The Brazilian law ensures the right to privacy and the protection of personal data, establishing foundations, principles and rules concerning data protection, besides instituting standards with the purpose of ensuring its fulfillment. The Decree No. 10.046 brings provisions contrary to national legislation, compromising the privacy and other personal data holder's rights. Thus, it will be noted the need to change the devices contrary to privacy protection and data protection present in Decree No. 10.046.

Keywords: Personal data protection. Privacy. Decree No. 10.046 of 2019. Internet Milestone. General Data Protection Law.

INTRODUÇÃO

Com a chegada da sociedade da informação, surgiu para o Direito o desafio de regular os novos institutos resultantes desta evolução. Até pouco tempo atrás, os temas relacionados à

internet e à proteção de dados eram regulados no Brasil apenas por diplomas legais como o Código Civil, Código de Defesa do Consumidor, Código Penal, além, é claro, da Constituição da República de 1988. Assim, as diversas demandas que surgiam eram dirimidas somente por legislações não específicas.

Neste contexto, com as pessoas cada vez mais dependentes da internet e das diversas possibilidades que ela oferece, foi necessária a criação de diplomas legais específicos para regular a matéria, como é o caso da Lei nº 12.965/2014 (Marco Civil da Internet) e o Decreto nº 8.771/2016 que a regulamenta, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) e o Decreto nº 10.046 de 2019.

O presente trabalho tem como objetivo evidenciar o conflito entre determinadas disposições do Decreto nº 10.046 e a legislação pátria de proteção de dados.

Pretende abordar o problema gerado pelos dispositivos presentes no Decreto nº 10.046/2019 que são contrários às normas, fundamentos e princípios presentes na legislação de proteção de dados no ordenamento jurídico nacional.

Justifica-se pela insegurança jurídica gerada por tal decreto, ao comprometer a privacidade e a proteção de dados ao compartilhar dados gerais e sensíveis de forma ampla entre a administração pública federal.

A pesquisa foi desenvolvida por meio do método dialético, valendo-se de consulta jurídica na legislação, bem como em doutrina, periódicos e artigos científicos.

O trabalho está dividido em três capítulos, dispostos da seguinte maneira: (i) Da privacidade à proteção de dados, que aborda a evolução do conceito clássico de privacidade até sua conceituação nos dias atuais; (ii) A legislação de proteção de dados no Brasil, que analisa a disciplina da matéria no país; e (iii) O Decreto nº 10.046/2019 e sua contradição com a privacidade, que analisa o decreto e aponta afrontas à privacidade e à proteção de dados na legislação brasileira.

1. DA PRIVACIDADE À PROTEÇÃO DE DADOS

A proteção à privacidade já passou por diversos momentos históricos que refletiram em sua conceituação, alterando sua definição clássica ao longo do tempo. Na lição de Stéfano Rodotà (2008, p. 92), o conceito atribuído a Warren e Brandeis, que definia a privacidade como o “direito de ser deixado só”, perdeu há muito tempo seu valor genérico, devendo apenas ser utilizada em situações específicas.

Na sociedade atual, a tendência não é mais do sujeito desejar o sigilo apenas dos momentos de intimidade, ou de restrição ao acesso sobre suas informações pessoais. Para coexistir na sociedade de informação, nativamente conectada, se exige a projeção de informações do indivíduo para a realização de atividades cotidianas, ou seja, o sujeito dispõe de dados para a coletividade. Neste sentido, Alexandre Ribeiro da Silva (2017, p. 11) ensina que

> Atividades cotidianas que anteriormente se realizavam no convívio social agora envolvem o uso de ferramentas e aplicações pela internet. Tornou-se comum o uso de smartphones e computadores na realização de compras e interações em sites ou aplicativos como ifood, Facebook, Mercado Livre, Whatsapp, Tinder entre tantos outros.
> Desta forma, uma simples compra de um lanche, uma conversa com amigos e quase todos os afazeres diários apresentam-se ligados ou com a possibilidade de estarem ligados ao uso incessante de tecnologias de rede e comunicação.
> A construção da personalidade humana perante o mundo não mais se limita em um campo individual, mas sim a partir de uma intersubjetividade entre indivíduos, que em tempos presentes, perpassa os meios digitais de comunicação.
> (...)
> Para a realização destas interações pela internet necessariamente os usuários prescindem de "disponibilizar" informações pessoais que os identifiquem e os diferenciem para a própria realização de tais serviços. Isso ocorre pelo compartilhamento de seus "dados pessoais".

Portanto, é necessário que se prevaleça a possibilidade do mesmo ter conhecimento, controle e a possibilidade de endereçar ou interromper o fluxo de suas informações pessoais até o limite do necessário, fazendo com que a privacidade passe a ser entendida em sentido mais amplo, como além do direito de ser deixado só, mas também o direito de manter o controle e dispor sobre as próprias informações, ou direito à autodeterminação informativa. Ademais, o termo "privacidade" tem diferentes conceitos na legislação brasileira, sem dispor de uma definição objetiva.

A Constituição Federal de 1988 em seu art. 5º, inciso X se limita apenas em declarar que são "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

No mesmo sentido, o art. 21 do Código Civil de 2002 determina 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".

Já o Marco Civil da Internet ao tratar o acesso à internet como essencial ao exercício da cidadania, assegura em seu art. 7º, inciso I, a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação".

Para José Afonso da Silva (2015, p. 208), a terminologia do dispositivo constitucional de fato não é precisa, devendo ser considerado como direito à privacidade aquele que abrange todas as manifestações da esfera íntima, privada e da personalidade:

> O dispositivo põe, desde logo, uma questão, a de que a *intimidade* foi considerada um direito diverso dos direitos à vida privada, à honra e à imagem das pessoas, quando a doutrina os reputava, com outros, manifestação daquela. De fato, a terminologia não é precisa. Por isso, preferimos usar a expressão *direito à privacidade*, num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional em exame consagrou.

O efeito dessa realidade se dá na medida em que "na sociedade da informação a pessoa é primeiramente representada por informações, ou seja, conhecida por dados, números, rotinas de compras e gastos, na forma de textos, imagens, sons e dados registrados" (GHISI; PEZZELLA, 2013, p. 233). De tal modo, a privacidade humana atual é expressa em informações pessoais que são transformadas em dados, que são processados por meios eletrônicos, monitorados global e diuturnamente por governos e organismos internacionais e, ainda, vendidos como recurso base.

Portanto, atualmente a proteção à privacidade está diretamente ligada à proteção de dados, consoante o entendimento de Guilherme Peña de Moraes (2019, p. 198):

> O cenário da sociedade da informação, na qual a tecnologia é usada para a coleta, produção, processamento, transmissão e armazenamento de informações, resultou nas definições de "privacidade informacional" ou poder de controle e proteção, na conjuntura da Internet, ao tratamento automatizado de dados pessoais e de "privacidade decisional" ou poder de autodeterminação no tocante a exposição, no contexto dos reality shows, à divulgação de fatos da vida privada.

Corroborando com esse entendimento, Alexandre Ribeiro da Silva (2017, p. 78) afirma que a doutrina vem cada vez mais atrelando o direito à privacidade com o controle pelo cidadão de seus dados pessoais:

> Assim, o direito à privacidade não pode ser mais abordado apenas com uma visão individualista e subjetiva, como um "direito de ser deixado só", que recebe do Estado uma tutela negativa que impede o seu vilipêndio. Nesse entendimento, a doutrina vem cada vez mais atrelando a privacidade ao controle pelo cidadão de suas informações e dados pessoais nos meios automatizados de informação, como internet e bancos de dados.

Destarte, é notório que as mudanças ocorridas na sociedade alteraram o sentido da proteção à privacidade, principalmente com a chegada da sociedade da informação, o direito à privacidade já não guarda mais o sentido genérico de "o direito de ser deixado só", mas sim

passa a ter relação direta com a proteção de dados, em especial o controle dos dados pessoais e a autodeterminação informativa pelo cidadão.

1.1 A proteção de dados dos usuários

Para Patrícia Peck Pinheiro (2018, p. 25-26), dado pessoal é qualquer informação que se relacione a uma pessoa identificada ou identificável, não sendo apenas dados como nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, mas também dados de localização, placas de veículos, perfis de compras, número de Internet Protocol (IP), histórico de compras, dados acadêmicos, dentre outros relacionados à pessoa natural viva.

Existem também os chamados "dados sensíveis", conceituados pelo art. 5º, inciso II da LGPD como aqueles relacionados à personalidade do indivíduo, suas escolhas pessoais, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genético ou biométrico vinculado à pessoa natural.

Stefano Rodotà (2008, p. 96) ensina que

> A classificação desses dados na categoria de dados "sensíveis", particularmente protegidos contra os riscos da circulação, deriva de sua potencial inclinação para serem utilizados com finalidades discriminatórias. Exatamente para garantir plenitude à esfera pública, determinam-se rigorosas condições de circulação destas informações, que recebem um fortíssimo estatuto "privado", que se manifesta sobretudo pela proibição de sua coleta por parte de determinados sujeitos (por exemplo, empregadores) e pela exclusão de legitimidade de certas formas de coleta e circulação.

Como exemplo do risco de manipulação, vale destacar que em 2016 veio à tona um gigantesco escândalo relacionado a vazamento de dados, envolvendo o Facebook e a empresa britânica *Cambridge Analytica*, que inclusive trabalhou para a companha à presidência de Donald Trump. Na ocasião, contabilizou-se o vazamento de dados de 87 milhões de usuários da rede social Facebook, com a estimativa de que desse total de usuário afetados, 443 mil sejam brasileiros (LIMBERGER, 2019, p. 253).

Com efeito, a normatização que cuida da proteção de dados não deve passar uma noção de restrição à internet ou controle excessivo sobre como os indivíduos utilizam seus dados. Para Silva (2017, p. 29),

> a legislação que busca uma efetiva proteção a dados pessoais e a proteção desta "nova dimensão" da privacidade não pode e não deve se pautar pela restrição a

> serviços e tecnologias. Deve garantir o menor limite possível de manuseamento dos dados pessoais do indivíduo por terceiro sem o conhecimento e anuência do mesmo e buscar assegurar o livre desenvolvimento da personalidade e a participação de maneira autônoma nas vidas política e social por meios digitais.
> .

Portanto, a defesa dos dados e da privacidade não pode ser possível por meio de uma ação que combata à utilização de tecnologias pelo cidadão comum, mas a regulação do uso dos mesmos por agentes especializados. Sobre o ponto, Rodotà (2008, p. 24) leciona que:

> Trata-se de uma tendência determinada por fenômenos interdependentes. Às novas formas de coleta e tratamento de informações, possibilitadas, sobretudo pelo recurso a computadores, adiciona-se a crescente necessidade de dados por instituições públicas e privadas: como não é imaginável uma ação que vá ao encontro a esta tendência, comum a todas as organizações sociais modernas, é necessário considerar de forma realista tal situação, analisando as transformações que causa na distribuição e no uso do poder pelas estruturas públicas e privadas.

Afinal, de acordo com Silva (2017, p. 30), para que se efetive a tutela destes direitos, é importante problematizar a utilização de tais informações e legitimar aquele que terá o controle, visto ser improvável supor que o Estado ou empresa decline a esse sofisticado aparato informativo. É preciso ter em consideração as transformações causadas nas estruturas públicas e privadas pelo fluxo de dados.

Para Têmis Limberger (2019, p. 253-254) já é sabido há muito tempo que os dados dos usuários de internet são utilizados para criar perfis de consumo, e que, inclusive, existem suspeitas de que sejam utilizados para manipulação política, ocorrendo então a oferta comercial de dados para formação de perfil de consumidor, além da coleta de informações para serem aproveitadas em campanhas eleitorais.

A utilização da internet pelos mais variados dispositivos (notebook, desktop, tablet, smartphone, etc) é uma constante troca de dados entre o usuário de determinado serviço e a empresa que disponibiliza o serviço. Isso gera a figura do “homem de cristal”, conforme Magalhães e Longhi (2019, p. 254)

> A certeza de que hoje existe o denominado “homem de cristal”, na internet, no sentido de que há uma ampla visibilidade, a respeito das informações e dados que a pessoa disponibiliza e interesses que possui, a partir da consulta e visita aos sítios eletrônicos, que faz na internet, que ficam armazenados e contribuem para formação de um perfil, que na maioria das vezes, é repassado a outras empresas, sem o consentimento do usuário.

Isto posto, com o advento das *big datas* e o avanço tecnológico no manejo de dados, a circulação de informações pessoais passou a ser também utilizada para o desenvolvimento das

prestações públicas e serviços privados. Portanto, a própria proteção da privacidade passa pela proteção aos dados pessoais, o que resultou nas legislações que passaram a ser discutidas nos termos acima elencados.

2. A LEGISLAÇÃO DE PROTEÇÃO DE DADOS NO BRASIL

O surgimento da internet tem origens militares, tendo surgido a partir de um projeto americano realizado 1955, em meio a Guerra Fria, com o objetivo de conectar os computadores dos Estados Unidos. Em 1958 surge a ARPA (*Advanced Research Projects Agency*), ligada ao Departamento de Defesa. Anos depois, em 1969, tendo a finalidade de conectar grandes computadores de forma descentralizada e manter a comunicação no caso de uma guerra nuclear, a Agência obteve êxito ao realizar a primeira transmissão de mensagem em rede bem sucedida. Assim, na década de 70 surgiu a ARPANet, no mesmo momento em que surge o termo "Internet", usado pela primeira vez pelo fundador do *Internet Society*[1](HOBAIKA; BORGES, 2014, p. 651).

Já em 1983, ocorreu a divisão da ARPANet em MILNet, sendo que esta ficou ligada ao Departamento de Defesa, enquanto a ARPANet passou a ter caráter acadêmico. Passados dez anos, a responsabilidade da ARPANet foi transferida para a Fundação Nacional de Ciências, que teve a autorização para conexões de redes comerciais, fato que impulsionou a expansão global da internet (ibidem, 2014, p. 653).

Somente em 1992, por meio da Rede Nacional de Pesquisa (RNP), foi que a internet chegou ao Brasil, conectando universidades, centros de pesquisa e algumas organizações não governamentais do país. Após alguns anos, em 1995, foi iniciada a utilização comercial da internet no Brasil (TARJA, 2019, p. 141).

Desde então, a internet vem ganhando espaço na vida das pessoas de todo o mundo, impactando de forma direta no exercício da liberdade de expressão, além do direito de receber e transmitir informações, "com repercussões sociais, econômicas, técnicas, legais e de segurança" (HOBAIKA; BORGES, 2014, p. 653).

A legislação pátria tem avançado no sentido de regulamentar as matérias derivadas da expansão da internet, como a privacidade e a proteção de dados. Os melhores exemplos são a Lei nº 12.965/2012 (Marco Civil da Internet) e o Decreto nº 8.771/2016, que a regulamenta, também a Lei nº 13.706/2018 (Lei Geral de Proteção de Dados), além do controverso Decreto

[1] Organização não governamental sem fins lucrativos, dedicada ao desenvolvimento mundial da internet.

nº 10.046 de 2019, que dispõe sobre o compartilhamento de dados na administração pública federal.

2.1 O Marco Civil da Internet e o Decreto nº 8.771/2016

Após passar por um longo período de elaboração e debates, inclusive com a participação popular por meio da internet, e impulsionado pela solicitação de urgência em sua tramitação em razão do escândalo de espionagem revelado por Edward Snowden, o Marco Civil da Intenet (Lei 12.965/2012), foi finalmente sancionado pela então presidente da república Dilma Rousseff em 23 de abril de 2014.

Apesar de sofrer resistência de diversos setores, o projeto de lei que viria a ser o Marco Civil da Internet, teve início em 2009, quando o Ministério da Justiça em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas iniciou uma série de consultas públicas que contribuíram para moldar o primeiro texto da matéria, que foi levado à Câmara dos Deputados em 2011. Em seguida foram realizadas sete audiências públicas para discussão e aprimoramento do texto, tendo seu conteúdo sido colocado em um portal criado com a finalidade de possibilitar a participação dos internautas na elaboração do Marco Civil da Internet.

O MCI, conforme seu artigo 1º, "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria", e tem como pilares a proteção da privacidade e dos dados pessoais, bem como a neutralidade da rede e a liberdade de expressão (BIONI, 2019, p. 128).

Entre os direitos e garantias do usuário, destacam-se os que asseguram a inviolabilidade da privacidade, das comunicações privadas na internet, salvo por ordem judicial, o consentimento informado, não fornecimento de seus dados a terceiros, e o dever de prestar informações claras e completas sobre a coleta, uso, armazenamento e tratamento e proteção de seus dados pessoais, que poderão ser utilizados somente em hipóteses restritas.

Outra característica relevante do Marco Civil da Internet é a multiparticipação de diversos entes e sujeitos, transparência, colaboração e democracia, de modo que o inciso I, do seu art. 24 determina que a União, Estados, Distrito Federal e Municípios devem atuar seguindo como diretrizes o "estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica".

De acordo com Maria Marconiete Fernandes Pereira (2014, p. 864), o diploma concretiza as relações múltiplas e plurais tecnológicas concebidas por uma nova era de cultura digital, legitimando a multiparticipação entre os entes políticos e cidadãos, abrangendo espaços físicos e lógicos, assim proporcionando segurança na troca de informações.

Dois anos após a promulgação do MCI, foi promulgado também pela presidente Dilma Rousseff o Decreto nº 8.771 de 2016, que veio regulamentar o Marco e dar outras providências. Do mesmo modo que a lei que regulamenta, o decreto foi igualmente submetido a debates em uma plataforma do Ministério da Justiça na internet (SILVA, 2017, p. 67).

Em seu preâmbulo, o Decreto nº 8.771 determina que o mesmo:

> Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

O Decreto está divido em três capítulos, sendo que o primeiro trata de disposições gerais, apontando em seu art. 1º ao que ele se aplica, bem como indica procedimentos para guarda e proteção de dados, aponta medidas de transparência na requisição de dados da administração pública e estabelece parâmetros de fiscalização e apuração de infrações contidas no MCI.

O segundo capítulo trata da neutralidade da rede, princípio presente no inciso IV, do art. 3º do MCI, e cuja previsão no art. 9º do referido diploma padecia de regulamentação até o advento do Decreto 8.771/2016.

O terceiro capítulo cuida da proteção aos registros, aos dados pessoais e às comunicações privadas. Este capítulo encontra-se dividido em duas seções, quais sejam: Seção I – Da requisição de dados pessoais, e Seção II - Padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas.

Coube ao Decreto 8.771 de 2016 instituir dispositivos cuja finalidade é a proteção aos registros, dados pessoais e às conversas privadas. Desse modo, assegura que mesmo as solicitações de tais informações por autoridades administrativas deverão indicar o fundamento legal e a competência expressa para o acesso, além da motivação para o requerimento ao acesso dos dados pessoais. Por seu turno, os pedidos devem indicar precisamente as pessoas de quem os dados são solicitados e as informações desejadas, sendo proibidos pedidos coletivos genéricos ou inespecíficos.

Por fim, o quarto capítulo dispõe sobre a fiscalização e a transparência. Neste capítulo, fica determinado que a Anatel atuará na fiscalização e apuração das infrações nos termos da Lei nº 9.472, de 16 de julho de 1997; que a Secretaria Nacional do Consumidor atuará na fiscalização e apuração de infrações nos temos da Lei nº 8.078/90, que dispõe sobre a proteção do consumidor e dá outras providências; e que o Sistema Brasileiro de Defesa da Concorrência ficará a cargo da apuração das infrações à ordem econômica, nos termos da Lei nº 12.529/2011.

Assim sendo, o Decreto evolui no sentido de regulamentar e sanar algumas omissões que restaram no Marco, também definindo normas para efetivar a aplicabilidade do Marco Civil da Internet.

2.2 A Lei Geral de Proteção De Dados

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), também conhecida pela sigla LGPD, é originária do Projeto de Lei Complementar nº 53/2018 e foi promulgada pelo então presidente da república Michel Temer em 14 de agosto de 2018. O primeiro artigo da lei traz um panorama de suas disposições e seu objetivo[2].

O prazo determinado no art. 65 da LGPD para início de sua vigência foi do dia 28 de dezembro de 2018 para os artigos que tratam da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Já para os demais artigos, o prazo foi fixado em 24 meses após a data de sua publicação, ou seja, 14 de agosto de 2020.

Essencialmente a Lei Geral de Proteção de Dados traz "princípios e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas" (PINHEIRO, 2018, p. 15), sendo certo se tratar de uma legislação que busca preencher a aspiração do mercado por segurança jurídica nas atividades relacionadas ao tratamento de dados pessoais (HENRIQUE, 2019, p. 372).

Duas são as categorias de dados contempladas pela LGPD, sendo ambos conceituados nos incisos I e II do art. 5º da referida lei, a saber:

> Art. 5º Para os fins desta Lei, considera-se:

[2] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Tanto é verdade que os dados pessoais sensíveis foram especialmente protegidos pela Lei Geral de Proteção de Dados, que limitou sua utilização para somente quando houver consentimento e forma específica e detalhada do usuário, para finalidades específicas, ou, via exceção, para restritas possibilidades.

Ao passo que os dados sensíveis são cuja utilização indiscriminada pode gerar cenários de discriminação, Mendes (2014, p. 74) leciona que os dados pessoais sensíveis foram incluídos na LGPD acompanhados de regulamentação mais rígida do que a dos dados pessoais em geral, buscando aumentar a proteção das pessoas e da sociedade.

Um dos mecanismos de proteção aos dados pessoais gerais e sensíveis é a autodeterminação informativa, fundamento presente no inciso II, do art. 2º da LGPD, efetivando a regra de que o usuário tem o controle de suas informações.

Acerca dos princípios que regem a proteção de dados pessoais, presentes no art. 6º da LGPD, destacam-se o da finalidade (respeitando propósitos legítimos, específicos, explícitos e informados ao titular); adequação (conformidade do tratamento com as finalidades informadas ao titular); necessidade (utilização do mínimo tratamento possível para atingir suas finalidades); livre acesso (assegura aos titulares a consulta facilitada e gratuita sobre a forma e duração do tratamento); transparência (garantia de informações claras, precisas e de fácil acesso aos usuários quanto ao tratamento).

Desse modo, extrai-se que os princípios da Lei Geral de Proteção de Dados se encarregam de garantir a utilização e tratamento de dados pessoais de maneira restrita, a fim de atender as finalidades possíveis nos termos da lei, de forma explícita e assegurando que o titular dos dados seja informado de maneira gratuita e facilitada da finalidade, forma e duração do tratamento de seus dados.

Os princípios que tutelam a finalidade, transparência e informação ao titular também foram positivados com maior amplitude nos artigos seguintes da referida lei, como a possibilidade do titular obter informações do controlador[3] acerca de seus dados pessoais, assim como pode se opor ao tratamento efetuado em desconformidade com a LGPD, mesmo nas hipóteses de dispensa do consentimento.

[3] Conforme o inciso VI, do art. 5º da LGPD, controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

A Lei Geral de Proteção de Dados igualmente trata de elencar dispositivos relativos ao tratamento de dados pessoais pelo Poder Público. Outrossim, tais normas dão ao Poder Público o encargo de utilizar de dados pessoais somente para atender a finalidade e interesse públicos, oferecendo informações claras sobre todo o procedimento, respeitando os princípios da proteção de dados pessoais presente no art. 6º.

Portanto, a recente Lei Geral de Proteção de dados, que entrará em vigor em sua maior parte somente em 2020, veio sanar uma necessidade de regulamentar, trazendo uma redação principiológica e técnica (PINHEIRO, 2018, p. 17), toda a atividade com os dados pessoais e a relação dos atores envolvidos nesse processo, além de estabelecer fundamentos e princípios concernentes à matéria, que devem ser observados por pessoas naturais, empresas e pela administração pública.

3. O DECRETO Nº 10.046/2019 E SUA CONTRADIÇÃO COM A PRIVACIDADE E PROTEÇÃO DE DADOS

Sancionado pelo Presidente Jair Bolsonaro, o decreto nº 10.046/2019, revogou o decreto nº 8.789/2016, que dispunha sobre o compartilhamento de dados na esfera federal, tendo como uma das finalidades simplificar o acesso aos serviços públicos[4].

Assim como seu antecessor, o Decreto nº 10.046/2019 dispõe sobre compartilhamento de dados em âmbito federal, além de conceituar diversos termos para sua aplicação. Ainda, inova ao instituir o Cadastro Base do Cidadão (CBC) e o Comitê Central de Governança de Dados (CCGD), conforme disposição de seu preâmbulo, respeitando os limites e restrições legais, assim como o disposto na Lei Geral de Proteção de Dados.

O decreto possui 35 artigos, assim dispostos em seis capítulos: I – Disposição Gerais; II – Dos Níveis de Compartilhamento de Dados; III – Das Regras de Compartilhamento de Dados; IV – Do Cadastro Base do Cidadão; V – Do Comitê Central de Governança de Dados; e, por fim, o Capítulo VII – Disposições Finais e Transitórias. Note-se que o Decreto não possui capítulo com numeração VI.

Diferentemente do que ocorreu com o Marco Civil da Internet e com a Lei Geral de Proteção de Dados, o decreto foi publicado sem que fossem realizados debates ou audiências públicas acerca da matéria de que trata, entrando em vigor na data de sua publicação, em nove de outubro de 2019.

[4] Assim versava a redação do art. 2º e inciso I do revogado Decreto nº 8.789: "O acesso a dados de que trata o art. 1º tem como finalidades: I - a simplificação da oferta de serviços públicos";

Ainda recente, o decreto nº 10.046/19 não possui posicionamentos doutrinários e jurisprudenciais a seu respeito, razão pela qual se passa a analisar a literalidade de seu texto, dando especial atenção aos pontos conflituosos com a LGPD.

O decreto cuida de estabelecer regras e diretrizes para o compartilhamento de dados entre órgãos e entidades da administração pública federal, consoante previsão de seu art. 1º, tendo por finalidade facilitar a oferta de serviços públicos, aprimorar políticas públicas, além de aumentar a eficiência das operações internas da administração pública federal.

Para alcançar seu propósito, o decreto prevê o compartilhamento de dados categorizado em três níveis, que serão definidos pelo gestor de dados[5], a depender da confidencialidade. Neste cenário, o primeiro nível é de compartilhamento amplo, no qual se enquadram os dados sem restrições de acesso e de divulgação pública e livre. Por sua vez, o segundo nível é o de compartilhamento restrito, para dados protegidos por sigilo nos termos da lei, mas com permissão de uso para os órgãos e entidades federais. Já o terceiro nível é o de compartilhamento específico, também para dados protegidos por sigilo, porém, com autorização de acesso a órgãos e entidades específicos, ficando a cargo do gestor de dados determinar os limites das autorizações.

Todavia, não há previsão em lei acerca dos limites de cada nível de compartilhamento, sendo assim, o decreto estabelece que os níveis de compartilhamento serão determinados "nos termos da lei", mas não se tem legislação que defina critérios objetivos desta classificação, ficando tal incumbência a cargo do gestor de dados.

Neste ponto, é válido realizar um comparativo com a LGPD, lei que o decreto menciona sua observância para seus fins, no entanto, não é o que se extrai da redação do mesmo. Ocorre que a indefinição sobre os critérios de classificação dos níveis de compartilhamento desrespeita desde fundamentos da LGPD, como o respeito à privacidade, ofendendo igualmente princípios, como o da finalidade, da adequação, necessidade, livre acesso e, sobretudo, o princípio da transparência, pelo qual o inciso VI, do art. 5º da LGPD garante aos titulares dos dados o direito a "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento".

Os referidos princípios são assegurados por todo texto da Lei Geral de Proteção de Dados. É o que ocorre em seu Capítulo IV, que se encarrega da normatização do tratamento de dados pelo Poder Público. Nesse sentido, o inciso I, do art. 23 define que o Poder Público tem de fornecer "informações claras e atualizadas sobre a previsão legal, a finalidade, os

[5] O inciso XIII, do art. 2º, do Decreto nº 10.046/19 define gestor de dados como "órgão ou entidade responsável pela governança de determinado conjunto de dados".

procedimentos e as práticas utilizadas para a execução dessas atividades". Por conseguinte, tem-se que a incerteza sobre categorização dos dados em níveis está em desacordo com a legislação de dados do Brasil.

O diploma também cria o Cadastro Base do Cidadão (CBC), com objetivo de aprimorar o serviço público por meio do tratamento de dados de forma integrada com os bancos de dados da administração pública federal, inclusive cruzando informações a partir do número de inscrição do CPF. O CBC será composto pela base integradora, portanto, a base de dados que interliga os atributos biográficos ou biométricos[6] das bases temáticas, ficando excetuados os dados genéticos.

Insta salientar que a LGPD tem como fundamentos, entre outros, o respeito à privacidade, a autodeterminação informativa e à inviolabilidade da intimidade[7]. Assim sendo, com base em todo estudo feito até aqui acerca da proteção de dados pessoais conforme a legislação pátria, um dispositivo que compartilha amplamente dados pessoais, incluindo os chamados atributos biométricos, é contrário a tais fundamentos.

Especialmente sobre os atributos biométricos, que contêm dados compatíveis com aqueles definidos como sensíveis pela legislação, logo, devem ser utilizados com lisura e base legítima. Ainda assim, a utilização de forma ampla e não consentida de dados pessoais sensíveis encontra respaldo na alínea *b*, do inciso II, do art. 11 da Lei Geral de Proteção de Dados. Contudo, deverão ser observados princípios e regras da LGPD, respeitando a finalidade e as restrições impostas por ela, bem como informando de forma clara e fácil o titular dos dados pessoais.

Ademais, o decreto institui o Comitê Central de Governança de Dados (CCGD), composto por sete membros de diferentes áreas da administração pública federal e que tem competência para determinar as regras, orientações e parâmetros do CBC. Deste modo, será o

---

[6] O art. 2º do Decreto 10.046/19 assim considera:
"I - atributos biográficos - 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;
II - atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar";

[7] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

próprio CCGD o responsável por cuidar e fiscalizar os dados pessoais utilizados no CBC e respeitar os limites da Lei Geral de Proteção de Dados.

No entanto, caberá à Autoridade Nacional de Proteção de Dados (ANPD), órgão criado pela LGPD, zelar pela proteção de dados, assim como fiscalizar e aplicar sanções em casos de descumprimento da legislação de tratamento de dados. Por seu turno, a ANPD tem seu Conselho Diretor, órgão máximo de direção, composto por cinco diretores escolhidos pelo Presidente da República e nomeados após aprovação do Senado Federal, que apenas perderão seus cargos em caso de renúncia, condenação judicial com trânsito em julgado ou por demissão resultante de processo administrativo disciplinar.

Logo, toda responsabilidade pela correta aplicação da lei e sua fiscalização no que concerne ao tratamento de dados pessoais será realizada pela administração pública federal ou por membros escolhidos pelo Presidente da República.

Essa característica destoa daquelas diretrizes constituídas pelo Marco Civil da Internet, de que a União, Estados, Distrito Federal e Municípios devam estabelecer meios de "governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica", uma vez que centraliza ao Estado todo o controle dos dados presentes no CBC, sem controle externo da sociedade civil. Além do que, o MCI prevê que as aplicações de internet dos entes do poder público têm de buscar o "fortalecimento da participação social nas políticas públicas".

Do mesmo modo, o Decreto nº 8.771/2016 (Regulamentador do MCI) estatui que para ter acesso a dados cadastrais, deverá haver requisição da autoridade administrativa, indicando a fundamentação legal e a razão da solicitação, o que não é observado pelo texto do Decreto nº 10.046/19, que estabelece normas para o compartilhamento amplo de grande gama de dados pessoais dos cidadãos.

Portanto, o decreto nº 10.046/19 traz em sua redação disposições para a criação, funcionamento e fiscalização de bancos de dados compartilhados entre os órgãos da administração pública federal, contendo dados pessoais de cidadãos, inclusive biológicos e comportamentais, para trazer maior efetividade e eficiência aos serviços públicos. Para tal, cria o Cadastro Base do Cidadão, a quem compete a garantir a operação do compartilhamento, e o Comitê Central de Governança de Dados, que terá a tarefa de deliberar sobre regras, orientações e diretrizes acerca do compartilhamento de dados.

CONCLUSÃO

O presente trabalho abordou os direitos fundamentais à privacidade e sua projeção na proteção de dados, demonstrando que a privacidade não detém mais tão somente o conceito clássico de “direito a ser deixado só”, mas sim é vista como parte do direito de controle e informação do indivíduo sobre seus dados pessoais.

Foi explorada a legislação e doutrina correlata ao tema, quais sejam, o Marco Civil da Internet e o Decreto nº 8.771 que o regulamenta, a Lei Geral de Proteção de Dados e, por fim, o controverso Decreto nº 10.046 de 2019.

A partir dos dados apresentados, foi demonstrado o cenário atual da proteção de dados no Brasil, que se dá principalmente pelo MCI e seu decreto regulamentador, e em breve pela LGPD, quando da sua entrada em vigor em 2020. Porém, o recém publicado Decreto nº 10.046 traz em sua redação a busca por eficiência e melhora na prestação do serviços público, contudo, utiliza de normas contrárias à legislação vigente, previstas inclusive na Constituição da República, e princípios que tutelam o direito à privacidade e à proteção de dados.

Ficou demonstrado que o referido decreto cria institutos que compartilham de forma ampla e muitas vezes indiscriminada dos dados de pessoas naturais entre bancos de dados de diversas áreas da administração pública, desrespeitando a privacidade dos titulares desses dados.

A finalidade específica da utilização dos dados, garantida pela legislação pátria, não é considerada, à medida que é colocada à disposição de inúmeras entidades públicas, mesmo que não guardem relação com a natureza dos dados. Também deve-se ressaltar que foram criados três níveis de compartilhamento de dados (amplo, restrito e específico), de acordo com os termos lei. Entretanto, não há legislação que defina de forma objetiva esses níveis, ficando a cargo do gestor de dados a classificação.

Outro ponto que o Decreto nº 10.046 desrespeita é a governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, das empresas, da sociedade civil e da comunidade acadêmica. Ocorre que o decreto centraliza unicamente ao Estado o controle dos bancos de dados do Cadastro Base do Cidadão e não cumpre as referidas previsões.

Conclui-se, portanto, diante do estudo exposto, que diversos dispositivos do Decreto nº 10.046 de 2019 ofendem princípios e normas elencados em nossa Carta Magna, bem como no Marco Civil da Internet, no Decreto nº 8.771 de 2016 e na Lei Geral de Proteção de Dados, razão pela qual o mencionado Decreto merece ser analisado de forma criteriosa, alterando os dispositivos contrários à proteção da privacidade e à proteção de dados.

BIBLIOGRAFIA

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

BRASIL. **Código Civil, Lei nº 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 03 dez. 2019.

BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 03 de dez. 2019.

BRASIL. **Decreto nº 8.771**, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 12 out. 2019.

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: 09 nov. 2019.

BRASIL. **Marco Civil da Internet, Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 12 out. 2019.

BRASIL. **Lei Geral de Proteção de Dados, Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 out. 2019.

HENRIQUE, Lygia Maria Moreno Molina. **LGPD:** Cuidados na Implementação. Revista Forense - Vol. 429. Rio de Janeiro: 2019.

HOBAIKA; Marcelo Bechara de Souza; BORGES, Luana Chystina Carneiro. *In*: LEITE, George Salomão; LEMOS, Ronaldo (coord). **Marco Civil da Internet**. São Paulo: Editora Atlas S.A., 2014.

LIMBERGER, Têmis. *In*: MARTINS, Guilherme Magalhães; LONGHI, Jõao Victor Rozatti (coord). **Direito Digital** – Direito Privado e Internet. Indaiatuba: Editora Foco, 2019.

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

MORAES, Guilherme Peña de. **Curso de Direito Constitucional**. 11. Ed. São Paulo: Editora Atlas, 2019.

PEREIRA, Maria Marconiete Fernandes. *In*: LEITE, George Salomão; LEMOS, Ronaldo (coord). **Marco Civil da Internet**. São Paulo: Editora Atlas S.A., 2014.

PEZZELLA, Maria Cristina Cereser; GHISI, Silvano. **Privacidade na sociedade da informação:** controle e direito ao esquecimento em espaços públicos. Revista da AJURIS, v. 40, n. 132, dez./2013. Disponível em: <http://ajuris.kinghost.net/OJS2/index.php /REVAJURIS/article/view/257/192>. Acesso em: 09 nov. 2019.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais** - Comentários à Lei N. 13.709/2018 (LGPD). São Paulo: Editora Saraiva, 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
SILVA, Alexandre Ribeiro da. **A Proteção de Dados no Brasil:** a tutela do direito à privacidade na sociedade da informação. Juiz de Fora: UFJF, 2017. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/5374>. Acesso em: 12 out. 2019.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 38. Ed. São Paulo: Malheiros Editores, 2015.

TARJA, Sanmya Feitosa. **Informática na Educação** - O Uso de Tecnologias Digitais na Aplicação das Metodologias Ativas. 10. Ed. São Paulo: 2019.