UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

DISPONIBILIZAÇÃO DE DADOS PESSOAIS PELO PODER PÚBLICO: BREVES CONSIDERAÇÕES SOBRE O DIREITO À PROTEÇÃO DE DADOS E DEMAIS DIREITOS QUE INCIDEM NA ESFERA PÚBLICA

JOÃO MARCOS LEITE FARREL

JOÃO MARCOS LEITE FARREL

DISPONIBILIZAÇÃO DE DADOS PESSOAIS PELO PODER PÚBLICO: BREVES CONSIDERAÇÕES SOBRE O DIREITO À PROTEÇÃO DE DADOS E DEMAIS DIREITOS QUE INCIDEM NA ESFERA PÚBLICA

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Filipe José Medon Affonso**

CIP – Catalogação na Publicação

L J62d

Leite Farrel, João Marcos
DISPONIBILIZAÇÃO DE DADOS PESSOAIS PELO PODER PÚBLICO: BREVES CONSIDERAÇÕES SOBRE O DIREITO À PROTEÇÃO DE DADOS E DEMAIS DIREITOS QUE INCIDEM NA ESFERA PÚBLICA / João Marcos Leite Farrel. -- Rio de Janeiro, 2021.
55 f.

Orientador: Filipe José Medon Affonso.
(mestrado) - Universidade Federal do Rio de Janeiro, , 2021.

1. Introdução. 2. 1 - Os impactos da Lei Geral de Proteção de Dados no ordenamento jurídico brasileiro. 3. 2 - Previsões acerca do tratamento de dados pessoais pelo Poder Público. 4. 3 - Aplicação prática da proteção de dados pelo Poder Público. 5. Conclusão. I. Medon Affonso, Filipe José, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

JOÃO MARCOS LEITE FARREL

DISPONIBILIZAÇÃO DE DADOS PESSOAIS PELO PODER PÚBLICO: BREVES CONSIDERAÇÕES SOBRE O DIREITO À PROTEÇÃO DE DADOS E DEMAIS DIREITOS QUE INCIDEM NA ESFERA PÚBLICA

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Filipe José Medon Affonso**

Data da Aprovação: __/__/__.Banca

Examinador:

_____

Filipe José Medon Affonso

_____

Marcos de Souza Paula

_____

Daniel Fortes Aguilera

AGRADECIMENTOS

Em primeiro lugar, agradeço às pessoas que colaboraram significativamente na elaboração desse trabalho, dentre as quais destaco o Professor Filipe José Medon Affonso, cuja atuação como orientador foi impecável e essencial no percurso dessa monografia. Obrigado pela confiança, pela paciência e pela dedicação. Agradeço também à minha família, que me deu a paz e o apoio necessários para que eu pudesse me dedicar às minhas atividades, e a meus amigos e amigas que auxiliaram com indicações, materiais e demais meios de suporte, Camila Casali; Diego Semeraro; Gabriel Batista; Gabriel Santos; Iolanda Gonçalves; Lígia Magalhães; Lucas Martins; Olga Martins; e um especial agradecimento a Fernando Bourguy e Gilberto Martins de Almeida, que além de me ensinarem na prática, colaboraram com a minha pesquisa.

Nesse momento de conclusão de curso, aproveito para expressar minha gratidão a todos e todas que me marcaram de alguma forma nessa jornada.

Um dos elementos mais importantes para mim foi o privilégio de ter a presença de pessoas que me ensinam, me inspiram e me engrandecem. Dentre elas, a pessoa mais importante é minha mãe. Ela me deu toda a base e me forneceu tudo aquilo que preciso para que eu possa construir meu futuro. Ela me ensinou, por meio do convívio mais amoroso, os valores mais importantes que desejo reproduzir ao longo da vida. A ela dedico tudo o que alcancei e alcançarei.

Agradeço a todos e todas da família que me fortaleceram e me ajudaram nessa caminhada, espero que eu possa retribuir, de alguma forma, o apoio que me dão. Especial agradecimento à minha mãe; tia Angela; tio Dauro; meu padrinho Francisco; tio Sergio; tia Tânia; tia Valéria e tia Vera. O suporte de vocês é fundamental e vocês me inspiram muito.

Meus amigos e minhas amigas também foram essenciais no meu caminho até a formatura. Agradeço a força dada por todos os irmãos que o Colégio de São Bento me deu: Antônio Henrique Ferreira; Diego Semeraro; Francisco Vinhaes; Gabriel Carelli; João Gabriel Guerra; João Pedro Lippi; João Raphael Aranha; Lucas Martins; Tiago Amorim; Raphael Neves; João Guilherme Cóe; Pedro Kuhlmann; Rafael Monnerat; Raphael Neves e Rodrigo Pimentel. Agradeço também aos maiores presentes que a Faculdade Nacional de Direito me deu: Bruna Magalhães; Cássia A. Clésio; Geovana Santos; Iolanda Gonçalves; João Victor Ribeiro; Olga Martins; Pedro Rocco;

Raphael Garbayo; Tiagol Cruz e Vitor Lima. Para além dos ambientes acadêmicos, agradeço aos grandes amigos e amigas Aline Aurílio; Beatriz Serra; Eduardo Araújo; Lígia Magalhães; Luiza Antico; Yasmim Piorino; à minha prima Isabella Rodrigues e aos meus primos Bruno Nigri e Pedro Nigri.

Na minha trajetória até a conclusão da graduação, tive o privilégio de participar de diversas experiências sociais e acadêmicas ricas. Registro aqui minha gratidão a todas e todos que se dedicam ao ensino e à educação de qualidade, a todas as pessoas que permitem o funcionamento da UFRJ, da FND e de todas as demais faculdades. Professoras e professores, funcionárias e funcionários dessas instituições são a base da construção da nossa sociedade. Muito obrigado pelo empenho nessa árdua tarefa e pela contribuição indescritível para o nosso futuro.

Na minha vida acadêmica tive ao lado pessoas especiais, que me motivaram e motivam, e que, por meio de suas posturas admiráveis, tornaram-se exemplos do que desejo alcançar. Antes de entrar na universidade, tive o apoio não só da minha mãe como da minha tia Valéria, que me carregou (literalmente) durante o período da escola. No período da faculdade, uma das pessoas que mais participou da minha formação foi meu grande amigo e tutor Francisco Formel, a quem agradeço todo o cuidado e a atenção durante o curso e minha trajetória no ramo jurídico. Destaco também a inspiração que minhas amigas, Cássia A. Clésio e Maria Eugenia Cirillo, e minha tia Tânia transmitem em suas atuações. Elas são um exemplo de que o esforço para o sucesso dos projetos individuais não precisa nem deve afastar a disposição em ajudar quem precisa em paralelo. Essas características me inspiram na minha busca pessoal e profissional.

Agradeço também aos colegas de profissão, que me ensinaram e auxiliaram na minha atuação como estagiário. Agradeço ao Kevin Bennesby, chefe atencioso e preocupado, pela experiência transmitida no primeiro escritório em que estagiei. Agradeço à Ana Carolina Martins; Andressa Braga Maria Eugenia Cirillo; Jeniffer e Vitor Chavantes pelo companheirismo no estágio; e especialmente à Andrea Caputo; Carolina Martins; Davi Reis; Flávia Benaion; Nathália Menezes; Prissila Camacho e Rafael Lima por me receberem tão bem e por me mostrarem que a integridade e o comprometimento com o trabalho são capazes de resistir às maiores adversidades.

Obrigado à minha atual equipe, do Martins de Almeida Advogados, da qual tenho o privilégio de fazer parte. Obrigado ao Fernando Bourguy, pelas orientações, ensinamentos e diversos exemplos

de atuação como advogado e como chefe. Obrigado à Dr.ª Patrícia Martins de Almeida pelo tratamento tão cordial e ao Dr. Gilberto Martins de Almeida pela dedicação com o aprendizado. O acolhimento e o cuidado dessa família foram de extrema importância na minha jornada.

A todos que de alguma forma contribuíram até a conclusão desse curso, a minha gratidão e meu eterno compromisso.

RESUMO

A implementação da Lei Geral de Proteção de Dados, promulgada em 2018, com vigência plena em agosto de 2021, traz uma série de condições e determinações a serem observadas nas atividades de tratamento de dados de pessoas naturais. Nesse cenário, é importante reavaliar os fluxos de dados pessoais tratados pelo Poder Público, à luz dos princípios positivados pela LGPD, uma vez que a adequação desses atores é essencial para a efetiva proteção de dados dos brasileiros e das brasileiras. Considerando o compartilhamento de dados pessoais um dos tratamentos mais comuns e impactantes para os direitos dos titulares, esse trabalho busca, por meio das considerações trazidas, refletir sobre as considerações necessárias à elaboração dos limites de compartilhamento de dados pelo Poder Público. Para tanto, serão abordados os impactos da LGPD sobre o Poder Público e as características dos demais direitos fundamentais que dialogam com as atividades de tratamento de dados, a fim de se visualizar os possíveis caminnhos para a harmonização normativa desses direitos fundamentais.

Palavras-chave: proteção de dados; Lei Geral de Proteção de Dados; dados pessoais; disponibilização; publicidade; sigilo de dados

ABSTRACT

The introduction of the General Law on Data Protection, signed into law in 2018 and fully enforced in August 2021, brings a series of conditions and determinations to be observed in data processing activities involving individuals. In this scenario, it is important to reevaluate the flows of personal data processed by the Public Authorities, under the principles established by the LGPD, as the adequacy of these actors is essential for the effective data protection of Brazilians. Considering the sharing of personal data one of the most common and impacting processing procedures for the rights of data subjects, this paper seeks, through the considerations presented herein, to reflect on the considerations necessary for the elaboration of the limits on data sharing by the government. To this end, the impacts of the LGPD on the public authorities and the characteristics of the other fundamental rights that dialogue with data processing activities will be addressed to understand the possible paths for the normative harmonization of these fundamental rights.

Keywords: data protection; General Data Protection Regulation; personal data; sharing; publicity; confidentiality of data

LISTA DE SIGLAS E ABREVIATURAS

ADI – Ação Direta de Incostitucionalidade

AO – Ação Originária

ARE – Agravo em Recurso Extraordinário

CDC – Código de Defesa do Consumidor

CGPD – Comitê Gestor de Proteção de Dados

CGU – Controladoria-Geral da União

CNJ – Conselho Nacional de Justiça

CRFB – Constituição da República Federativa do Brasil

GDPR – General Data Protection Regulation – Regulamento (UE) 2016/679

LAI – Lei de Acesso à Informação – Lei nº 12.527/2011

LGPD – Lei Geral de Proteção de Dados – Lei nº 13.709/2018

MCI – Marco Civil da Internet – Lei nº 12.965/2014

OCDE – Organização para a Cooperação e Desenvolvimento

PEC – Proposta de Emenda à Constituição

STF – Supremo Tribunal Federal

TJSC – Tribunal de Justiça do Estado de Santa Catarina

SUMÁRIO

INTRODUÇÃO

O direito à proteção de dados pessoais torna-se cada vez mais caro à proteção da personalidade dos indivíduos, como um todo, e à proteção do próprio sistema democrático. Nesse cenário, por diversos fatores, que serão tratados, o Brasil adotou uma norma própria para regular a matéria. Trata-se da Lei Geral de Proteção de Dados – LGPD, que traz diversos impactos para os mais variados setores, atingindo inclusive o âmbito público.

A Lei Geral de Proteção de Dados – LGPD, promulgada em 14 de agosto de 2018, com vigência completa em agosto de 2021, tem um grande potencial para alterar o ordenamento jurídico brasileiro, no que diz respeito às atividades relativas a dados pessoais. As inovações trazidas pela LGPD devem ser implementadas pelo Poder Público em sua atividade, que recebe da lei especial tratamento, diante de sua extensão e de sua condição assimétrica em relação aos titulares de dados.

A fim de garantir a adequação do Poder Público à LGPD, faz-se necessário estabelecer os limites do compartilhamento e da disponibilização de dados, tratamentos muito comuns e decisivos para o controle efetivo do fluxo de dados pessoais. A divulgação excessiva de dados pessoais representa um dano à personalidade de seus titulares. Por outro lado, a ausência dela, quando necessária ao controle das atividades públicas, resulta no cerceamento da democracia.

Desse modo, percebe-se que para a correta implementação das normas de proteção de dados, é necessária a análise da relação desse direito com os demais que incidem sobre as atividades de tratamento de dados pessoais. Dentre eles, destacam-se a privacidade, a inviolabilidade do sigilo de dados e o direito de acesso à informação. A partir da compreensão da relação desses direitos, torna-se mais evidente quais pontos devem ser trabalhados na elaboração dos limites do compartilhamento de dados pessoais pelo Poder Público.

O presente trabalho objetiva apontar algumas considerações relativas à adequação à LGPD pelo poder público, considerando a necessidade de harmonização com os demais direitos fundamentais previstos no ordenamento jurídico brasileiro, para se ponderar em qual medida e como os dados pessoais devem ser compartilhados.

O primeiro capítulo trata da Lei Geral de Proteção de Dados, explicando brevemente o contexto em que ela foi elaborada, a importância desse tema na sociedade contemporânea e quais os procedimentos práticos que devem ser realizados diante da execução de um tratamento de dados pessoais.

No capítulo seguinte, aborda-se a importância da matéria sobre a atividade pública e como as normas da LGPD incidem sobre o Poder Público, explicitando quais as particularidades que a Lei traz sobre os agentes que realizam esses tratamentos de dados pessoais no âmbito público. São brevemente apresentadas as características de outros direitos fundamentais que dialogam com a proteção de dados e de que forma eles se relacionam.

Assim, são abordadas, separadamente, as propriedades de cada um dos direitos fundamentais pertinentes à proteção de dados. O primeiro direito a ser apresentado é a privacidade, responsável pelo surgimento da proteção de dados, porém diferente desta. Em seguida, trata-se do sigilo de dados, que apesar de não tutelar as informações em si, contribui para a proteção destas em algum nível. Por último, discorre-se sobre o acesso à informação, direito extremamente caro à manutenção e ao avanço do sistema democrático e cada vez mais prestigiado no direito brasileiro. Tal direito não é necessariamente contrário à proteção de dados, no entanto a aplicação conjunta dos dois demanda um cuidado maior, por conta dos diferentes objetivos de ambos.

Ao final do segundo capítulo, expõe-se a jurisprudência do Supremo Tribunal Federal – STF acerca da divulgação da remuneração de servidores públicos, a fim de visualizar, a partir de um caso prático, como o direito de acesso à informação e a privacidade devem incidir diante do interesse público, pensando também em como essa relação pode ser aplicada à proteção de dados.

O terceiro e último capítulo traz algumas informações sobre o estágio atual da implementação da proteção de dados no âmbito público, buscando apontar as medidas adotadas até o momento. Toma-se como exemplo o Poder Judiciário, responsável pelo tratamento e disponibilização de uma quantidade expressiva de dados pessoais, que como poderá ser observado, aparenta estar num caminho positivo em relação à garantia desse direito fundamental. Observa-se também a título exemplificativo os interessantes métodos de decisão da

Controladoria-Geral da União – CGU sobre os recursos de solicitação de informações públicas que contenham dados pessoais via Lei de Acesso à Informação.

Ao final, a conclusão retoma os pontos mais caros ao objetivo do trabalho, resumindo o que se observa na prática até o momento em relação à adequação do Poder Público e o que ainda pode ser alterado, na busca efetiva pela proteção de dados pessoais dos cidadãos e cidadãs do Brasil.

1. OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS NO ORDENAMENTO JURÍDICO BRASILEIRO

1.1 Contexto legislativo no qual a LGPD foi elaborada

A proteção de dados e principalmente a privacidade são concebidos pelo ordenamento jurídico brasileiro muito antes da elaboração da Lei Geral de Proteção de Dados[1] - LGPD.

A Constituição Federal disciplina nos incisos X e XII do artigo 5º sobre a inviolabilidade à intimidade, à vida privada, à honra e a imagem das pessoas, ao sigilo da correspondência e das comunicações telefônicas[2]. O inciso LXXII[3] prevê a concessão do habeas data, que promove maior controle dos indivíduos sobre seus dados pessoais no âmbito público. O habeas data, regulado pela Lei 9.507/1997, é um tipo de ação constitucional, que, como aponta o Professor Danilo Doneda, apesar de ser considerada pobre e pouco efetiva, carrega importância por sua função simbólica, por ser um instrumento de proteção de dados positivado na Constituição Federal do Brasil e pelo pioneirismo de sua adoção, em relação aos demais países da América Latina[4].

A Lei 8.078/1990, popularmente denominada Código de Defesa ao Consumidor - CDC - possui uma seção, em seu capítulo V - Das Práticas Comerciais, que garante um tratamento mais

---

[1]Andreia Saad menciona o White Paper: Proteção de Dados: a legislação vigente no Brasil. 2017. Disponível em https://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf, que traz uma lista de normas relativas à proteção de dados. SAAD, Andreia. *Ela, a LGPD, vista pelas empresas: uma proposta de visão prática – e otimista*" –. In: CUEVA, Ricardo Villas Bôa; DONEDA, Danilo; MENDES, Laura Schertel (Org.). *Lei Geral de Proteção de Dados (Lei nº 13.709/2018) A caminho da efetividade: contribuições para a implementação da LGPD*. p. 23

[2] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
[...]
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
[...]
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;"

[3] "LXXII - conceder-se-á "habeas-data":
a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"

[4]DONEDA, Danilo. *Da privacidade à proteção de dados*. Editora Revista dos Tribunais. 2ª Edição. p.286

protetivo sobre as informações pessoais registradas em bancos de dados e cadastros, no âmbito de suas relações de consumo[5].

A norma que regula os bancos de dados com informações de adimplemento de pessoas naturais e jurídicas para fins de histórico de crédito - Lei 12.414/2011 ou Lei do Cadastro Positivo - traz uma definição própria para banco de dados[6]. Além disso, veda o tratamento de informações excessivas ou "sensíveis"[7], cujo conceito assemelha- se muito à concepção de dados sensíveis, positivada posteriormente pela LGPD.[8]

A Lei 12.527/2011, nomeada Lei de Acesso à Informação - LAI, instrumento de regulação da transparência dos atos do poder público, define "informação pessoal" como "aquela

---

[5]SEÇÃO VI Dos Bancos de Dados e Cadastros de Consumidores:
Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6° Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015) (Vigência)
Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.
§ 1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado.
§ 2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 2

[6]"Art. 2º Para os efeitos desta Lei, considera-se:
I - banco de dados: conjunto de dados relativo a pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro; [...]"

[7] "Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
[...]
§ 3º Ficam proibidas as anotações de:
I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas."

[8] A LGPD conceitua em seu artigo 5º, II, os dados sensíveis. Para tanto, utiliza-se de um rol exemplificativo similar ao da Lei 12.414/2011.

relacionada à pessoa natural identificada ou identificável", adotando um conceito expansionista[9], ratificado na definição de dados pessoais dada pela LGPD. Além disso, a LAI aponta para a responsabilidade do poder público em proteger tais informações pessoais e traz uma seção exclusiva com especificações sobre o tratamento delas (Seção V do Capítulo III, artigo 31).

A Lei 12.965/2014, também conhecida como Marco Civil da Internet - MCI, menciona no inciso III do artigo 3º a proteção de dados como um dos princípios do uso da internet no Brasil[10], e estabelece limites e condições para o tratamento de dados pessoais ao longo de seu texto.

A partir desses exemplos, nota-se que a LGPD não regula um objeto inédito no direito brasileiro. Sua função não é apresentar matéria nova, mas centralizar a regulação desse tema, antes esparsa. Além disso, ela delimita a aplicação da proteção de dados, sistematizando tal direito no ordenamento jurídico brasileiro.

A Lei Geral de Proteção de Dados foi assinada em 14 de agosto de 2018, e entre tentativas frustradas e prósperas de alterações sobre as datas de início de sua vigência, de forma segmentada, a norma entrou em vigor por completo como estabelecido em seu artigo 65:

> Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)
>
> I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)
> I-A – dia 1º de agosto de 2021, quanto aos arts.52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)
> II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

O marco temporal de sua promulgação é consequência de um cenário internacional que adota a regulação de tratamentos de dados pessoais como requisito para o desenvolvimento de relações econômicas, principalmente no âmbito privado. O maior símbolo desse movimento é a

---

[9]Nesse sentido, ensina Rony Vaiznof: "O Brasil adotou o conceito expansionista de dado pessoal, pelo qual não somente a informação relativa à pessoa diretamente identificada estará protegida pela Lei, mas também aquela informação que possa - tem o potencial de - tornar a pessoa identificável." VAINZOF, Rony. *Capítulo I – Disposições Preliminares*. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega; (coords.). *LGPD: Lei Geral de Proteção de Dados comentada*. Ed: 2ª. rev., atual. e ampl. São Paulo. Thomson Reuters Brasil, 2019. p.89

[10]Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
[...]
III - proteção dos dados pessoais, na forma da lei

entrada em vigor, em 25 de maio de 2018, da General Data Protection Regulation – GDPR, lei responsável por regulamentar a proteção de dados na União Europeia.

As discussões no Brasil acerca de uma legislação centralizada e mais robusta sobre a matéria já existiam desde o início da década de 2010. Algumas influências internacionais, no entanto, aceleraram os procedimentos legislativos para a elaboração da LGPD, destacando-se possíveis prejuízos em decorrência da insuficiência normativa face a GDPR e a intenção do Brasil em integrar a Organização para a Cooperação e Desenvolvimento Econômico – "OCDE", marcada pela solicitação formal de adesão integral, elaborada pelo país em 2017[11].

A GDPR obstaculiza o fluxo de dados pessoais entre a União[12] Europeia e demais países que não possuam regulação de proteção de dados no mesmo nível da primeira[13]. Em paralelo, a

[11]Brasil vai cumprir todos os requisitos para acessão à OCDE, garante Fendt. Publicado em 23/02/2021 17h05 Atualizado em 25/02/2021 11h44. Disponível em https://www.gov.br/economia/pt-br/assuntos/notícias/2021/fevereiro/brasil-vai-cumprir-todos-os-requisitos-para-acessao-a-ocde-garante-fendt]

[12]"Cf. MENDES, Laura Schertel; DONEDA, Danilo. *Comentários à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil*. Revista de Direito do Consumidor. vol. 120. ano 27. p. 555-587. São Paulo: Ed. RT. nov.-dez. 2018: "A sanção da Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), no dia 14 de agosto de 2018, é resultado de um esforço de, pelo menos, oito anos de debates e duas consultas públicas, que se iniciaram desde a elaboração da primeira versão do anteprojeto de lei pelo Ministério da Justiça em 2010. A partir de um processo democrático realizado na internet e de forma muito semelhante ao debate público do Marco Civil da Internet, as consultas públicas realizadas em 2010 e 2015 resultaram em um total de quase 2.000 contribuições da sociedade civil, especialistas, órgãos do governo e empresas. Em 2016, o Projeto foi enviado à Câmara dos Deputados e passou a tramitar em paralelo com Projeto de Lei do Senado sobre a mesmo tema (PLS 330/2013). Na Câmara dos Deputados, foi criada a Comissão Especial de Proteção de Dados Pessoais e designado como relator o Deputado Orlando Silva, que, após uma série de audiências públicas, seminários e reuniões intersetoriais, conduziu a matéria para a sua aprovação por unanimidade em plenário. Em seguida, por meio da relatoria do Senador Ricardo Ferraço, o PLC 53/2018 foi aprovado por unanimidade também no Senado Federal"

[13]A GDPR determina que só pode haver transferência de dados pessoais para fora da União Europeia, sem autorização específica, caso haja decisão da Comissão Europeia anterior que ateste que o país, território ou organização internacional com a qual se dará a transferência assegura um nível de proteção adequado, como aponta o artigo 45, §1º:

"Artigo 45º
Transferências com base numa decisão de adequação
1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica."

Caso não haja tal decisão, as transferências de dados pessoais poderão ocorrer desde que sujeitas às garantias adequadas, conforme estabelecido no artigo 46:

"Artigo 46º
Transferências sujeitas a garantias adequadas
1. Não tendo sido tomada qualquer decisão nos termos do artigo 45º, nº 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

OCDE coloca a necessidade da existência de uma regulação bem desenvolvida sobre proteção de dados dentre os requisitos de ingresso de futuros países à Organização.

Após breve análise do contexto de elaboração da norma, deve-se compreender sua real importância como ferramenta de defesa de direitos fundamentais, individuais e coletivos, seus conceitos mais urgentes e inéditos e como eles devem ser incorporados no ordenamento jurídico brasileiro. Muitos deles dialogam com fluidez com normas e princípios anteriores, contudo, outros geram questionamentos sobre determinados aspectos do direito brasileiro. Nos casos correspondentes à segunda hipótese, diversos pontos devem ser revisitados, questionados e até mesmo remodelados.

1.2 Contexto social atual e a importância da proteção de dados

A famosa capa da conceituada revista "The Economist", da edição de 6 de maio de 2017, trouxe o título "The world's most valuable resource" ilustrando prédios das empresas "Amazon", "Uber", "Microsoft", "Google", "Facebook" e "Tesla" sob o oceano, fazendo alusão às plataformas de petróleo. A comparação da relevância econômica dos dados com o petróleo ilustra o processo de comoditização de dados, principalmente os relativos a pessoas naturais[14]. A evolução tecnológica aprimorou não só a capacidade computacional de armazenamento de dados e de gestão/análise dos dados, como também ampliou e facilitou os meios de coleta de dados.

---

2. Podem ser previstas as garantias adequadas referidas no nº1, sem requerer nenhuma autorização específica de uma autoridade de controlo, por meio de:
a) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
b) Regras vinculativas aplicáveis às empresas em conformidade com o artigo 47º;
c) Cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame referido no artigo 93º, nº 2;
d) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93º, nº 2;
e) Um código de conduta, aprovado nos termos do artigo 40º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou
f) Um procedimento de certificação, aprovado nos termos do artigo 42º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados.
3. Sob reserva de autorização da autoridade de controlo competente, podem também ser previstas as garantias adequadas referidas no nº1, nomeadamente por meio de:
a) Cláusulas contratuais entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou organização internacional; ou
b) Disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados."

Nota-se que, não por coincidência, em análise realizada em maio de 2021[15], dentre as sete empresas mais valiosas no mundo atualmente, seis têm suas operações focadas em serviços de coleta e gestão de dados pessoais[16], como por exemplo redes sociais, serviços de busca, e/ou de armazenamento de informações em nuvem[17].

O exponencial aprimoramento da utilização de dados, viabilizado pela evolução tecnológica demonstrou servir não só a interesses comerciais, como políticos também. A partir do mapeamento de gostos, vontades, preferencias, opiniões e pensamentos, num geral, é possível direcionar mensagens mais efetivas para a conquista de determinados interesses, muitas vezes nefastos.

Tal possibilidade foi evidenciada diante da revelação das atividades ilícitas e antidemocráticas da Cambridge Analytica, que utilizou dados pessoais coletados junto ao Facebook, sem o consentimento e sequer a ciência de seus titulares, para a construção de estratégias em campanhas eleitorais como a de Donald Trump para presidência dos EUA e do movimento a favor da saída do Reino Unido da União Europeia – British Exit ou "Brexit". Percebe-se que, por múltiplos motivos, a regulação da proteção de dados é urgente. Desse modo, Ana Frazão ensina que:

> Vistos já como o novo petróleo, os dados são hoje insumos essenciais para praticamente todas as atividades econômicas e se tornaram, eles próprios, objeto de crescente e pujante mercado. Não é sem razão que se cunhou a expressão data-driven economy, ou seja, economia movida a dados, para designar o fato de que, como aponta Nick Srnicek, o capitalismo do século XXI passou a centrar-se na extração e no uso de dados pessoais.
>
> Obviamente que o fenômeno, longe de se restringir à seara econômica, apresenta inúmeras repercussões nas esferas individuais dos cidadãos, além de levar à total reestruturação das relações sociais e políticas. Consequente mente, os dados ganharam uma importância transversal, tornando-se vetores das vidas e das liberdades individuais, assim como da sociedade e da própria democracia.
>
> É verdade que a coleta de dados pessoais não é algo propriamente novo, sendo a história da humanidade marcada por inúmeras experiências e avanços na tarefa de obter, coletar, registrar e acessar dados. Entretanto, o Big Data e o Big Analytics possibilitaram que tais atividades ocorressem de maneira muito mais eficiente, com mais veracidade, velocidade, variedade e volume. Mais do que isso, o Big Data e o Big Analytics

[15] Relatório *Global Top 100 companies by market capitalization*. Disponível em https://www.pwc.com/gx/en/audit-services/publications/assets/pwc-global-top-100-companies-2021.pdf. p.22. Acesso em 4 out. 2021.
[16] O relatório aponta para a seguinte ordem no "*Top 100 global companies*": 1º Apple Inc; 2º Saudi Aramco; 3º Microsoft Corp; 4º Amazon.Com Inc; 5º Alphabet Inc; 6º Facebook Inc; 7º Tencent.
[17] A Amazon Web Services oferece armazenamento em nuvem, como se pode verificar no site: https://aws.amazon.com/pt/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=*all&awsf.Free%20Tier%20Categories=*all. Acesso em 4 out. 2021.

> permitiram que, a partir da coleta e do registro de dados, fossem a eles atribuídas utilizações e aplicações que não seriam sequer imagináveis há pouco tempo e que, na ausência de uma regulação adequada, passaram a ser realizadas sem limites e com resultados que podem se projetar para sempre.

A analogia estabelecida entre dados e petróleo demonstra de maneira didática diversos pontos em comum entre os dois elementos. Do mesmo modo que o petróleo serviu como fonte de combustível para movimentar os motores que sustentam a economia por diversas décadas, os dados servem para alimentar as atividades que mais impactam a economia atualmente. E assim como o petróleo se tornou um ativo valioso, o valor dos dados hoje é gigantesco[18]. Apesar da pertinência da comparação, Silvio Meira aponta que:

> DADOS não são o "novo PETRÓLEO". Comparando com fontes de energia, DADOS seriam o novo URÂNIO. Têm que ser REFINADOS para separar o que se quer do que não serve, têm que atingir MASSA CRÍTICA para gerar energia [VALOR!] e o DESCARTE é um perigo, para o negócio e o ecossistema.

Nesse cenário, é importante afastar a ideia de que a LGPD impacta negativamente o fluxo de dados pessoais, essencial ao desenvolvimento da sociedade. A lei não desestimula tal prática, mas a aperfeiçoa. A cultura da proteção de dados, muito ligada ao princípio da minimização, combate os excessos, para proteger direitos fundamentais, caros não só aos titulares de dados pessoais, como à estrutura democrática do Estado.

Processo semelhante ocorreu em relação às normas de trânsito, com a ressalva de que a regulação de dados pessoais diz respeito a direitos da personalidade abstratos como a privacidade e intimidade, enquanto as normas de trânsito resguardam direitos da personalidade concretos como a vida e a integridade física.

Com o avanço da tecnologia, à medida que os veículos automobilísticos se modernizaram e se popularizaram, o tráfego destes foi fortemente incorporado pela sociedade. Diante desse processo, destacam-se dois fatores que demandam a regulação do fluxo veicular, cada vez mais

---

[18] Rodrigo Dias de Pinho Gomes analisa, à luz da proteção de dados, a incorporação da FitBit empresa inserida no mercado fitness, possuidora de um banco de dados pessoais de saúde, obtidos a partir do monitoramento das condições físicas de usuários a partir de wearables e outros dispositivos, e da empresa Nest, de fornecimento de câmeras de vigilância e de sensores inteligentes ao google, que comprou as duas empresas. Em: *A transferência de bancos de dados entre empresas em caso de fusão ou aquisição*. GOMES, Rodrigo Dias de Pinho. Disponível em: file:///C:/Users/jmfar/OneDrive/Documentos/Curso%20DPO%20ESA%20RJ%20-%2018.01.21/Aula%2001%20-%20Rodrigo%20Pinho/A-transferencia-de-bancos-de-dados-entre-empresas-em-caso-de-fusao-ou-aquisicao-JOTA-Info.pdf. Acesso em 05 out. 2021

impactante: (i) a necessidade de mitigar riscos a possíveis danos à personalidade, tanto dos indivíduos que utilizam os veículos, quanto dos pedestres que interagem com eles; e (ii) a necessidade de criar um ambiente seguro, ordenado e propício ao desenvolvimento do trânsito, benéfico tanto para a sociedade quanto para a indústria automobilística.

As leis que tratam do trânsito não atrapalharam o fluxo de veículos, mas permitiram sua expansão. Nesse mesmo caminho, segue a Lei Geral de Proteção de Dados. As normas trazem segurança jurídica para que os agentes que tratam dados pessoais possam realizar suas atividades de forma segura, protegendo não só os titulares de dados, como os próprios agentes quando em conformidade com a lei.

Diante da expansão da compreensão acerca da necessidade da proteção de dados, esta passou a ser considerada um direito fundamental no Brasil. Visando a consolidação desse direito, o Congresso Nacional aprovou a Proposta de Emenda à Constituição – PEC 17/2019[19], que acrescenta ao final do inciso XII do artigo 5º explicitamente o direito a proteção de dados dentre os demais direitos e garantis individuais[20]. A PEC também foi responsável por incluir no rol de competências privativas da União, no artigo 22, "a proteção e tratamento de dados pessoais" trazida em novo inciso[21].

Antes mesmo de estar positivado na Constituição, o STF, ao julgar as ADIs 6387, 6388, 6380 e 6390 sobre a suspensão da MP nº 954, que dispunha sobre o compartilhamento de dados de usuários de telefonia com o IBGE, reconheceu o direito à proteção de dados como um direito fundamental autônomo, à luz do art. 5º, XII, CF/88.

Por fim, cabe ressaltar que, ainda que a adequação às normas de proteção de dados imponha novos ônus aos agentes de tratamento (muitas vezes onerosos), trata-se não só de uma exigência legal que previne posteriores multas, sanções, litígios e até mesmo perda de reputação,

---

[19]No momento da finalização deste texto, a PEC já foi aprovada pelo Congresso Nacional. Seu texto aguarda a Promulgação. Disponível em https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao. Acesso em 20 out. 2021

[20] "Acrescenta ao final do inciso XII do artigo 5º: "bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". O dispositivo passa a vigorar com a seguinte redação: "XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;".

[21]Texto da PEC 17/2019 na íntegra disponível em: " https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1630441824501&disposition=inline. Acesso em 4 out. 2021

mas também de uma tendência no mercado atual. Nesse sentido, o cumprimento à lei, preventivo, concomitante e posterior ao tratamento de dados pode ser um diferencial competitivo. Muitas empresas adotam a adequação às normas de privacidade como pré-requisito para a contratação de terceiras prestadoras de serviço.

1.3 Estrutura da LGPD e nova dinâmica para o tratamento de dados

O poder legislador brasileiro, a fim de regular a matéria de proteção de dados, optou por replicar a estrutura adotada pela GDPR, elaborando uma lei principiológica[22] e multisetorial[23].

Para realizar um tratamento de dados adequado, devem-se cumprir algumas etapas. A primeira é analisar se a LGPD é aplicável à atividade. A lei é voltada exclusivamente para dados de pessoas naturais. Diante do tratamento de uma informação não pessoal, ou de algum dado de pessoa jurídica, não incidirá a norma. Há também, como exceção, situações em que o tratamento de dados pessoais não é regulado pela lei. Nesses casos, outras normas pertinentes serão observadas em relação à gestão de dados, porém as exigências da Lei 13.709/2018 não serão cabíveis. Caso a LGPD seja aplicável, a etapa seguinte é a verificação quanto à possibilidade da atividade, à luz da norma. Um tratamento só pode ocorrer se cumprir os requisitos básicos previstos na LGPD, caso contrário, não poderá ser realizado, por constituir uma violação à lei. Superadas essas duas etapas, o tratamento de dados deve atender aos princípios previstos na norma e respeitar demais regras específicas.

Como apontado, em primeiro lugar, é necessária a análise da incidência da lei em questão. Nesse sentido, é fundamental identificar se o objeto de tratamento é de fato um dado de pessoa natural, compatível com a definição trazida pela norma, pois a LGPD não regula outros tipos de dados ou informações, como os dados de pessoas jurídicas.

De forma didática, o artigo 5º da Lei 13.709/2018 explica seus conceitos basilares, possibilitando uma interpretação melhor do texto, e, consequentemente, uma compreensão mais

---

[22] GALLINDO, Sergio Paulo Gomes. *A Era Digital e a Economia Intensiva em Dados.* In: CUEVA. Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel; Lei Geral de Proteção de Dados (Lei nº 13.709/2018) A Caminho da efetividade: contribuições para a implementação da LGPD. São Paulo. Thomson Reuters Brasil, 2020. p.150

[23]Nos EUA há leis específicas para determinados setores ou assuntos relativos à proteção de dados, como por exemplo o Children's Online Pivacy Protection Act (COPPA)

precisa de sua aplicabilidade. As atividades reguladas pela LGPD são denominadas “tratamento” de dados pessoais. O inciso I do referido artigo traz a definição de “dados pessoais” e o inciso X define e exemplifica os tratamentos que envolvem tais dados:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável
> [...]
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

O caráter “Geral” da Lei 13.709/2018 diz respeito à extensão de sua aplicabilidade, extraída principalmente dos Artigos 1º, 3º e 4º. Nesse sentido, são elementos determinantes: (i) as condutas tipificadas pela lei; (ii) o meio pelo qual ocorrem; (iii) os agentes que as exercem; (iv) a extensão territorial a qual a lei se aplica; e (v) as entidades vinculadas à lei.

De maneira objetiva, pode-se dizer que a LGPD regula: (i) o tratamento de dados de pessoas naturais, salvo as exceções previstas em lei; ii) nos meios físico ou digital; (iii) exercidas por pessoas jurídicas tanto privadas quanto públicas, bem como por pessoas naturais que a pratiquem com interesses econômicos; (iv) ocorridas no território brasileiro ou fora dele, quando os dados pessoais em questão tiverem sido coletados no Brasil, ou pertencerem a indivíduos que se encontrem no país; (v) sendo todas as suas normas observadas pela União, Estados, Distrito Federal e Municípios”.

O artigo 4º assinala os casos de tratamento de dados de pessoas naturais os quais a lei não se aplica: (i) quando o agente for pessoa natural com finalidades particulares e não econômicos; ou (ii) quando se tratar de atividade exclusivamente jornalística, artística ou acadêmica; ou (iii) quando envolver segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais; ou (iv) quando um agente internacional armazenar no Brasil dados pessoais, de indivíduos de seu país, desde que este conte com grau de proteção de dados pessoais adequado ao previsto pela LGPD, e que não haja participação de qualquer sujeito brasileiro ou de terceiro país na atividade.

Diante dessas considerações, percebe-se que a abrangência da lei é demasiadamente extensa e profunda, o que por si só é suficiente para revelar a complexidade de seus efeitos. Após

a análise das hipóteses de aplicação da LGPD, ou seja, "quando" se aplica a lei, é necessário observar como ela se aplica e os impactos que decorrem de suas inovações normativas.

Uma vez aplicável a LGPD, o tratamento de dados pessoais só pode ocorrer se tal atividade atender a dois requisitos inafastáveis: (i) a existência de um propósito legítimo, específico, explícito e informado ao titular, intitulado "finalidade"[24] para o tratamento; e (ii) a compatibilidade com as hipóteses de tratamento de dados previstas objetivamente pela lei. Só podem ser iniciados e mantidos tratamentos nessas circunstâncias. Se não houver inicialmente uma finalidade ou uma base legal para o tratamento, ele não poderá sequer iniciar, e caso ele se inicie nas condições corretas, mas perca um desses requisitos ao longo do tempo, o tratamento deve ser interrompido.

Como apontado, a finalidade para o tratamento de dados deve ser específica, ou seja, necessita ser bem delimitada, não podendo ser vaga. A título de exemplo, uma empresa pode coletar o CPF de seus empregados com a finalidade de conferir o destino correto de pagamento de suas remunerações. A mesma empresa não pode, no entanto, coletar o CPF desses empregados adotando como finalidade "o atendimento às atividades da área de recursos humanos". Mesmo tratando de um propósito legítimo, tal finalidade é muito abstrata e ampla, suportando excessivas possibilidades, dentre as quais poderiam configurar abusos aos direitos dos titulares.

Havendo uma finalidade apropriada, a atividade dependerá de uma "base legal". Para identificá-la, é necessário analisar antes se o dado pessoal em questão é sensível ou não. Os dados pessoais sensíveis são apontados por Rony Vainzof como aqueles que:

> (...) em linhas gerais, são dados pessoais que possam trazer algum tipo de discriminação quando do seu tratamento (...) Ou seja, são dados pessoais que poderão implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais dos titulares.

[24] A finalidade é listada no primeiro inciso do artigo 6º da LGPD como um de seus onze princípios. Junto a ela estão presentes o da boa fé no caput e 9 outros, cada um com um inciso próprio. Embora todos eles devam ser respeitados, a finalidade é condição primária e basilar, não sendo possível medir quantitativamente sua qualidade, como outros princípios. A finalidade é ou não existente e adequada. Caso não seja, ou deixe de ser, o tratamento de dados não pode começar ou se prolongar, respectivamente.

O inciso II do artigo 5º da Lei Geral de Proteção de Dados traz um rol exemplificativo, que qualifica essa categoria como "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".

Tratando-se de um dado sensível, a atividade só poderá ocorrer caso haja previsão dentre as hipóteses dos incisos I e II do artigo 11 da referida lei. Se não for sensível, por eliminação o dado pessoal será "padrão", só podendo ser tratado de acordo com as hipóteses dos incisos do artigo 7º. Assim, determina a LGPD que:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
>
> [...]
>
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

Em resumo, um tratamento só pode ocorrer se for apontada uma finalidade com as características descritas e caso a atividade esteja em conformidade com as hipóteses previstas pela lei. Verificados esses dois requisitos essenciais, o tratamento torna-se possível. A partir disso é necessário: (i) examinar se é devido um tratamento especial, conferido aos casos em que há dados sensíveis; (ii) averiguar se os titulares são crianças ou adolescentes, aplicando a esses casos, procedimentos específicos; (iii) implementar as medidas de segurança previstas no capítulo VII, entre os artigos 46 e 51; e (iv) buscar os meios logísticos para atender aos direitos dos titulares, enunciados no capítulo III, entre os artigos 17 e 22, complementados pelas disposições do artigo 9º. Qualquer tratamento que desrespeite esses parâmetros é considerado ilícito.

Durante todas as fases do tratamento, os princípios enunciados no artigo 6º da LGPD devem reger as atividades relacionadas aos dados pessoais, em consonância com o conceito de "privacidade desde a concepção" ou "privacy by design", criado por Ann Cavoukian[25], conceituado pela Autoridade de Proteção de Dados do Reino Unido - ICO (Information Commissioner's Office) como "uma abordagem que garante a consideração de questões de privacidade e proteção de dados na fase de criação/ concepção de qualquer sistema, serviço, produto ou processo e, em seguida, ao longo do ciclo de vida"[26]. Essa noção foi incorporada pela Lei Geral de Proteção de Dados, especificamente no §2º do artigo 46.[27]

---

[25]Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Acesso em 5 out. 2021

[26]"What is data protection by design? Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle". Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default. Acesso em 5 out. 2021

[27] "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Conclui-se, portanto, que os princípios apresentados pelo artigo 6º da LGPD detêm uma relevância especial. Além de serem necessários em todas as fases do tratamento, a fim de se garantir uma efetiva proteção aos dados pessoais dos titulares envolvidos diante das previsões da lei, serve também para direcionar as ações dos agentes diante de suas lacunas. Como já mencionado, a LGPD possui estrutura similar à da GDPR, estabelecendo uma série normas, conceitos, obrigações e previsões explícitas, resguardando-se também, em paralelo, de um forte caráter principiológico[28].

Tal equilíbrio contribui para que a regulação, intimamente vinculada à tecnologia e seu constante avanço, não se torne obsoleta, tanto do ponto de vista dos direitos dos titulares, quanto pela perspectiva do desenvolvimento econômico e tecnológico, da inovação, da livre iniciativa e da livre concorrência, fundamentos da proteção de dados, positivados nos incisos V e VI do artigo 2º da LGPD[29].

[...]
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução"

[28] Mario Viola e Chiara Spadaccini de Teffé citam a "densa carga principiológica" como uma das características da Lei Geral de Proteção de Dados. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario; Tratamento de Dados Pessoais na LGPD: Estudo Sobre as Bases Legais dos Artigos 7º e 11. In: Tratado de Proteção de Dados. In: DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang (Org). Tratado de Proteção de Dados.

[29] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
[...]
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
[...]"

2. PREVISÕES ACERCA DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

2.1. Importância da Proteção de Dados na Atividade Pública

Como discorrido no tópico anterior, a LGPD inaugurou uma série de requisitos e regras para o tratamento de dados pessoais, a serem incorporados pelo ordenamento jurídico brasileiro. A adequação à legislação é um processo desafiador e complexo, que, como já exposto, atinge não somente as pessoas jurídicas de direito privado, como também as pessoas jurídicas de direito público. Nesse sentido, o tratamento de dados praticado pelo Estado, executado diretamente por pessoas jurídicas de direito público e de direito privado por delegação do Poder Público, está vinculado às normas da LGPD, que possui um capítulo específico para as atividades dos agentes públicos. Embora haja um capítulo exclusivo para o Poder Público, compreendido entre os artigos 23 e 32, os demais dispositivos da LGPD devem ser igualmente observados diante da execução de atividades relativas a dados de pessoas naturais, realizadas por seus agentes.

No processo de adequação há dificuldades comuns a todos os tipos de agentes, como por exemplo, a falta de uma cultura e de consciência da importância da proteção de dados[30], que comprometem a adesão de colaboradores e funcionários de todos os níveis, envolvidos nas atividades com dados pessoais, à causa. No contexto atual, com o constante crescimento da necessidade da proteção de dados, cada vez mais importante em relação aos demais direitos da personalidade, tanto a atuação privada como a pública que não estiverem em conformidade com a lei representam um risco à sociedade, capaz de causar danos de acordo com a quantidade ou qualidade dos dados tratados.

Ocorre que o âmbito público possui algumas peculiaridades que ensejam maior preocupação e responsabilidade. Além da extensão e da qualidade dos dados tratados[31], muitas vezes sensíveis, pode-se destacar o vínculo entre os agentes de tratamento e os titulares, dentre

---

[30] No documento "Planejamento Estratégico 2021-2023", elaborado pela Autoridade Nacional de Proteção de Dados, a promoção e o fortalecimento da cultura de Proteção de Dados Pessoais figuram como primeiro objetivo estratégico a ser atingido nesse período. Documento disponibilizado em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf. Acesso em 5 out. 2021

[31] O Poder Público trata uma série de dados sensíveis. Como exemplo, o Sistema Único de Saúde - SUS que armazena o histórico de saúde de milhões de brasileiros e já teve seu banco de dados pessoais vazado em 2020: Disponível em :https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml - Acesso em 5 out. 2021

outras características. Enquanto as relações privadas, são em regra voluntárias, muitas vezes dispensáveis, a relação dos indivíduos com o poder público é inafastável, como ensina Miriam Wimmer:

> Com efeito, a natureza da relação entre cidadão e Poder Público, diferentemente da relação com atores privados, é compulsória e se configura como pré-condição para o exercício da cidadania. O tratamento de dados pessoais pelo Estado é imprescindível para o desempenho de seu mandato constitucional [...] De fato, a concretização do princípio da igualdade dos cidadãos perante o governo e a participação política depende de sua identificação individual e do registro das inúmeras interações entre indivíduos e Poder Público.

Essa obrigatoriedade imposta aos titulares, que têm seus dados tratados, geralmente, independentemente de consentimento ou escolha, contribui para o fortalecimento da assimetria informacional estabelecida entre o Estado e os cidadãos[32]. Nesse contexto, é comum que os cidadãos sequer tenham ciência sobre o fluxo de seus dados.

O destaque conferido ao Poder Público pela LGPD confirma a importância dos agentes de tratamento públicos, figuras centrais dos primeiros regulamentos sobre proteção de dados. A primeira geração de normas acerca da matéria[33] tinha como escopo a regulação do tratamento realizado pelo Estado, como relata Danilo Doneda:

> Os primeiros sistemas de proteção de dados pessoais preocupavam-se basicamente com o Estado, como administrador dos dados de seus cidadãos [...] Estas leis propunham-se a regular um cenário no qual centros de tratamento de dados, de grande porte, concentrariam a coleta e a gestão dos dados pessoais. O núcleo destas leis era a concessão de autorização para a criação destes bancos de dados e do seu controle a posteriori por órgãos públicos. Estas leis também enfatizam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (senão os únicos) destas normas. Esta primeira geração de leis segue aproximadamente até Bundesdatenschutzgesetz.

Diante do impacto do tratamento de dados pessoais pelo Poder Público sobre a vida privada, a adesão de seus entes aos preceitos da proteção de dados pessoais é imprescindível à

---

[32] É intrínseca à atividade de tratamento de dados a existência de uma assimetria tanto informacional quanto técnica, entre o agente de tratamento e o titular de dados, assim como ocorre entre os atores das relações de consumo, ou no direito trabalhista, como aponta Bruno Bioni, ao tratar de assimetria e (hiper)vulnerabilidade próprias no âmbito da proteção dos dados pessoais. BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento – Rio de Janeiro: Forense, 2019.

[33] Priscilla Silva Laterça ensina que a primeira geração de normas sobre proteção de dados tinha como preocupação a concentração do processamento de dados e diante disso demandava que houvesse uma autorização prévia para a criação de banco de dados. Na primeira geração destacam-se a Lei alemã de Hesse, de 1970, a Lei Nacional de proteção de dados da Suécia (Estatuto para banco de dados) de 1973 e o PrivacyAct dos Estados Unidos da América, de 1974.

garantia efetiva de um dos direitos da personalidade mais caros à sociedade contemporânea. Nesse sentido, é fundamental que se compreenda como a esfera pública deverá adequar suas atividades atuais e futuras à luz da LGPD e das demais normas de proteção de dados, não só em relação às atividades de armazenamento e eliminação de dados, mas principalmente no tratamento específico de compartilhamento de dados pessoais.

2.2. Incidência das normas de proteção de dados no Poder Público

A expressão "Poder Público" adotada pela Lei Geral de Proteção de Dados não é conceituada explicitamente, como ocorre com outros termos definidos pelo artigo 5º da norma. No entanto, a lei aponta os atores ligados à administração pública que são regulados. Inaugurando o capítulo IV, o artigo 23 da LGPD dita os requisitos para o tratamento de dados pessoais pelas pessoas jurídicas de direito privado, estipulando, em seu caput, a lista fornecida pelo parágrafo único do 1º artigo da LAI como parâmetro de identificação desses agentes, conforme o texto que segue:

> Parágrafo único. Subordinam-se ao regime desta Lei:
> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Em complemento ao caput, o parágrafo 4º do artigo 23 da LGPD determina que "os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei".

Em relação às previsões da LGPD sobre a incidência no "Poder Público", Daniel Fortes Aguilera e Nicholas Furlan Di Biase ensinam que:

> para a aplicação do regime específico direcionado ao tratamento de dados pelo Poder Público, deve ser mais importante verificar se a manipulação de informações está sendo realizada com base nos propósitos previstos nos arts. 7º, inciso III, e 23 da LGPD, do que aferir a natureza jurídica do agente. Em uma palavra: a incidência das normas pertinentes ao tratamento de dados pelo Poder Público deve ser apurada a partir do

> propósito e da natureza do tratamento realizado; e não apenas com base em quem está realizando esse tratamento.[34]

Como já exposto, as regras da LGPD válidas para os agentes privados são igualmente aplicáveis aos agentes públicos, havendo condições e diretrizes extras a serem observadas pelos segundos. Dessa forma, diante dos requisitos básicos explorados no tópico *Estrutura da LGPD e nova dinâmica para o tratamento de dados*, o Poder Público tem suas finalidades e bases legais limitadas. As finalidades específicas necessárias para a existência do tratamento devem derivar das hipóteses, mais genéricas, trazidas no caput do artigo 23 da lei, as quais são: "para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público".

Com as restrições acerca da finalidade, consequentemente, as possibilidades quanto às bases legais são reduzidas. O legítimo interesse, previsto no inciso X do artigo 7º, é um exemplo claro de base legal incompatível com quaisquer finalidades possíveis para o tratamento de dados pelo poder público. Do mesmo modo, as qualidades do consentimento[35] tornam-se questionáveis[36], como aponta Miriam Wimmer:

> O consentimento é uma hipótese normalmente tratada com desconfiança no contexto do tratamento de dados pessoais pelo Poder Público, dados o desbalanceamento na relação entre cidadão e Poder Público e a consequente dificuldade de se caracterizar tal consentimento como livre.

A proteção de dados, como já mencionado, é considerada pelo ordenamento jurídico brasileiro um direito fundamental. Ao tratar dados pessoais, no entanto, o Poder Público depara-se com diversos outros direitos fundamentais. Para a aplicação da LGPD é necessário, portanto,

---

[34] AGUILERA, Daniel Fortes; BIASE, Nicholas Furlan Di. *Dificuldades interpretativas no regime de tratamento de dados pelo poder público: Lacunas, Contradições E Atecnias Na LGPD*. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro -PGE-RJ, Rio de Janeiro, v. 4n.2, maio/ago. 2021. Disponível em https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/238/182. Acesso em 4 out.2021. p.10

[35] O inciso XII do artigo 5º define as características do consentimento, considerando-o: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;".

[36] Sobre isso, o considerando 43 da GDPR aborda que: "A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução".

verificar a compatibilidade com os demais direitos a serem tutelados, pois como ensina Marmelstein: “as normas constitucionais são potencialmente contraditórias, já que refletem uma diversidade ideológica típica de qualquer Estado democrático de Direito. Não é de se estranhar, dessa forma, que elas frequentemente, no momento aplicativo, entrem em rota de colisão”. Diante da relação com os demais direitos, deve-se buscar identificar pontos de convergência e de divergência, bem como quais atritos são reais ou apenas aparentes, a fim de se garantir uma atuação do Poder Público baseada na harmonia entre direitos e princípios fundamentais.

Sobre a expectativa dessa adversidade, o Ministro Gilmar Mendes reforça em seu voto, no julgamento das ADIs 6387, 6388, 6380 e 6390 sobre a suspensão da MP nº 954, o seguinte entendimento de Miriam Wimmer (2020, p. 28):

> A aplicação da legislação de proteção de dados no tratamento de dados pelo Poder Público – tanto no caso de atos individuais e concretos como também na edição de atos normativos – traz, portanto, o desafio de conciliação entre os princípios tradicionalmente aplicáveis à Administração Pública e aqueles contidos na própria LGPD, sem que se determina a precedência prima facie de um interesse público abstratamente caracterizado e reconhecendo também a importância da proteção de dados pessoais para além da sua dimensão individual. A eficiência demandada da Administração Pública e o interesse público tutelado pelo Estado devem, portanto, ser compreendidos no contexto de um conjunto mais amplo de princípios e com elementos integrantes do compromisso que o Estado deve ter com a democracia e com a concretização de direitos fundamentais.

É comum que o direito à proteção de dados seja analisado a partir da dicotomia entre o direito de acesso à informação e o direito à proteção ao sigilo, ambos previstos pela Constituição Federal como direitos fundamentais[37]. De fato, os três direitos em questão possuem uma relação indissociável, porém, diferente do que se poderia concluir a partir de uma análise superficial, a proteção de dados não se resume a um direito pró sigilo e contrário ao direito de informação.

---

[37]Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
[...]
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)
[...]
XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
[...]
XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (Regulamento) (Vide Lei nº 12.527, de 2011)

Deve-se compreender que nem sempre haverá conflitos de normas, e quando houver, em determinados casos, a proteção de dados pode se valer do direito de acesso à informação, afastando o direito ao sigilo, bem como também pode recorrer ao sigilo, afastando o direito de acesso à informação. A partir da assimilação da dinâmica entre esses direitos fundamentais, os limites da aplicação do direito à proteção de dados tornam-se mais perceptíveis.

2.3. Direitos Fundamentais que dialogam com a proteção de dados no âmbito público

Para uma aplicação harmônica da proteção de dados com os demais direitos, é necessário entender as características destes direitos fundamentais. Quanto maior o domínio sobre as propriedades destes na atividade de tratamento de dados pessoais, maiores as chances de se alcançar um equilíbrio entre as normas. A partir do diálogo entre esses direitos fundamentais, tornam-se mais evidentes os fundamentos que determinam os limites das atividades do Poder Público. Nesse sentido, uma análise dos aspectos da privacidade, do sigilo de dados e do acesso à informação, direitos relevantes para a proteção de dados, pode auxiliar na busca pela harmonização e consequente adequação dos limites examinados.

2.3.1. A privacidade – origem da proteção de dados

A proteção de dados tem sua origem no direito à privacidade[38]. Um dos marcos iniciais da concepção do direito à privacidade como o entendemos hoje é a publicação pela Harvard Law Review, do renomado artigo "The Right to Privacy" de Samuel Warren e Louis D. Brandenis, em 1890. A partir desse texto acadêmico, o debate sobre a importância desse direito evoluiu, sendo incorporado em diversas normas internacionais e nacionais, como apontado no tópico que tratou do *Contexto legislativo no qual a LGPD foi elaborada*. O referido artigo já associava a necessidade da regulação da privacidade ao avanço tecnológico (à época a evolução da tecnologia estava ligada ao aprimoramento das máquinas fotográficas, que facilitavam a obtenção de imagens, que expunham as pessoas fotografadas, contra suas vontades).

[38] Esse processo de derivação é abordado detalhadamente pela obra "Da Privacidade à Proteção de Dados", do Professor Danilo Doneda, maior referência em relação ao estudo da evolução da privacidade desde a sua concepção até o surgimento da proteção de dados. Nesse trabalho, o autor afirma que se pode dizer que a proteção de dados é a "continuação por outros meios" da privacidade (P. 44 do referido livro)

A privacidade foi constituída como um direito individual, numa lógica ainda patrimonialista, baseado na proteção da propriedade privada. Incialmente foi entendida como o "direito de ser deixado só" (tradução de "right to be let alone"), direito negativo, por meio do qual se buscava uma obrigação de não interferência na vida privada, não demandando uma postura ativa dos seus sujeitos de direito, para sua garantia na prática. Uma importante referência normativa é a previsão do "direito ao respeito pela vida privada e familiar", trazida pelo texto do artigo 8º da Convenção Europeia de Direitos Humanos, que assegura que "(q)ualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência"[39].

A existência do avanço tecnológico, elemento que amparou a regulação sobre a privacidade, foi também o fator que a tornou uma ferramenta normativa insuficiente em relação à proteção dos indivíduos, de suas informações e dos direitos à personalidade, de forma mais ampla. O conceito de privacidade foi sofrendo alterações conforme as possibilidades de violação aos diretos individuais aumentavam, diante do processo evolutivo da tecnologia. Como afirma Rony Vainzof: "o conceito expandiu-se a ponto de ser tutelado como um direito que importa à coletividade também, na medida em que a evolução tecnológica passou a reinventar modelos de negócios cada vez mais baseados em dados dos indivíduos"[40].

Desde a concepção do direito à privacidade, diversos fatores sociais e econômicos deram início à transição para a sociedade da informação. Stefano Rodotà defende que a dinâmica "pessoa-informação-sigilo" foi substituída pela estrutura "pessoa-informação-circulação-controle". Diante dessa mudança, ao gerar informações pessoais, o sujeito necessita de uma postura ativa, que possibilite o controle de seus dados pessoais, para garantir a proteção de sua personalidade. Assim, o direito à privacidade isolado, como um direito negativo, é incapaz de preservar os indivíduos da sociedade. Dessa insuficiência emerge a proteção de dados, que engloba outros direitos e garantias que atentam ao empoderamento e controle necessários para salvaguardar os indivíduos e a sociedade como um todo. Em consonância com essa inédita

---

[39] "Artigo 8º(Direito ao respeito pela vida privada e familiar)
1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros". Disponível em https://www.echr.coe.int/documents/convention_por.pdf. Acesso em 5 out. 2021

[40]VAINZOF, Rony. *Capítulo I – Disposições Preliminares*. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega; (coords.). *LGPD: Lei Geral de Proteção de Dados comentada*. Ed: 2ª. rev., atual. e ampl. São Paulo. Thomson Reuters Brasil, 2019. p.25

necessidade de controle por parte dos sujeitos de direito, destaca-se o surgimento do instituto da "autodeterminação informacional", originado de uma decisão do Tribunal Constitucional Federal em 1973.

Deve-se observar, que diante do surgimento e da relação destes direitos, a defesa da proteção de dados engloba e ultrapassa o direito à privacidade. No entanto, somente as previsões de tutela da privacidade são insuficientes à garantia da proteção de dados. Essa distinção é de suma importância, pois nota-se que atualmente, no ordenamento jurídico brasileiro, a privacidade está positivada em diversos dispositivos legais, figurando, em alguns casos, como fundamento para a não ocorrência do tratamento de dados pessoais. Observar-se-á, mais à frente, que, para regular a matéria, A LAI menciona em seu artigo 31 apenas a privacidade, abstendo-se de mencionar a proteção de dados pessoais. Assim os cidadãos podem ter seus dados tratados, desde que a privacidade não seja violada, sendo afastados quaisquer mecanismos de controle do fluxo de dados pessoais, e, consequentemente, a proteção de dados, como uma proteção mais abrangente.

Diante dessa aparente insuficiência normativa, questiona-se, portanto, se não seria cabível uma atualização legislativa quanto às proteções da personalidade, considerando o que de fato se pretendia tutelar com a inserção do direito à privacidade, nas normas anteriores à LGPD, uma vez que somente a partir desta, ampliou-se de maneira expressiva a noção da necessidade da proteção de dados, como um direito positivo, para a proteção da personalidade, tornando-se mais evidente a importância e a devida incidência da proteção de dados. Desse modo, em relação ao Código Civil vigente, Anderson Schreiber aponta[41]:

> Em vez de se concentrar sobre a pluralidade de remédios exigidos para a proteção da privacidade e dos dados pessoais, em face destas novas controvérsias, o Código Civil de 2002 preferiu fazer constar de seu art. 21 o retumbante preceito de que "a vida privada da pessoa natural é inviolável". Não é. A mera observação da vida cotidiana revela a violação sistemática da privacidade.

Por fim, é importante destacar que como se abordará no próximo tópico, o direito à privacidade e o direito ao sigilo de dados também não se confundem. O direito à privacidade está

[41] SCHREIBER, Anderson. *Os Direitos da Personalidade e o Código Civil de 2002*. Disponível em http://schreiber.adv.br/downloads/os-direitos-da-personalidade-e-o-codigo-civil-de-2002.pdf. Acesso em 3 out. 2021. pp. 24-25

ligado ao conteúdo, enquanto a inviolabilidade do sigilo diz respeito aos meios de comunicação ou de envio dessas informações.

2.3.2. A inviolabilidade do sigilo de dados no direito brasileiro

O sigilo em sentido amplo está presente no ordenamento jurídico brasileiro desde os tempos do Império. A título de exemplo, é possível observar a aplicação desse direito no artigo 17 do Código Comercial de 1850 – Lei nº 556/1850[42], que trazia a seguinte previsão:

> Nenhuma Autoridade, Juizo ou Tribunal, debaixo de pretexto algum, por mais especioso que seja, póde praticar ou ordenar alguma diligencia para examinar se o commerciante arruma ou não devidamente seus livros de escripturação mercantil, ou nelles tem commettido algum vicio.

É possível notar a evolução da tutela do sigilo a partir da inserção, ao longo do tempo, dos tipos penais no Decreto-Lei Nº 2.848/1940 – Código Penal, que no título de crimes contra a pessoa, trata na seção IV dos crimes contra a inviolabilidade dos segredos, que traz os artigos 153 e 154. O primeiro prevê a proibição de divulgação de "segredo", conceituado como conteúdo de documento particular ou de correspondência confidencial, cuja divulgação possa produzir dano a outrem. O artigo 154, por sua vez, trata da violação ao segredo profissional.

A lei 9.983/2000 alterou tais dispositivos, acrescentando no parágrafo 1º–A, o tipo penal relativo à divulgação sem justa causa "de informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública". Em 2012, a Lei 12.737/2012 que dispõe sobre a tipificação penal de delitos informáticos introduziu a pena em relação à invasão de dispositivo informático e a Lei nº 14.155/2021, promulgada em 27 de maio de 2021, aumentou as penas relativas à invasão de dispositivo informático, considerando-os mais graves.

A regulação sobre a inviolabilidade do sigilo acompanhou os avanços tecnológicos contemporâneos às suas normas, como é possível notar a partir das previsões constitucionais, que ao versarem sobre direitos e garantias individuais, trataram da matéria. O sigilo à correspondência esteve presente em todas as Constituições desde a "Constituição da República

[42] A Lei 556/1850 está disponível em: https://www2.camara.leg.br/legin/fed/leimp/1824-1899/lei-556-25-junho-1850-501245-publicacaooriginal-1-pl.html. Acesso em 5 out. 2021

dos Estados Unidos do Brazil De 1891"[43], mantendo-se como única hipótese de sigilo até a CRFB de 1946, que previa no parágrafo 7º do artigo 141 que: "É inviolável o sigilo da correspondência". Na Constituição Federal seguinte, promulgada em 1967, tal previsão sobre o sigilo foi ampliada pelo parágrafo 9º do artigo 150, que determinou que "São invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas."

Diante do progresso tecnológico dos meios de comunicação e do desenvolvimento da informática[44], o sigilo de dados, especificamente, foi incorporado a partir da Constituição Federal atual[45], que a consagrou como um direito fundamental, a partir do inciso XII do artigo 5º, o qual prevê de forma inédita a inviolabilidade do sigilo de dados, além dos objetos de inviolabilidade do sigilo já estabelecidos na Constituição Federal anterior – correspondência, comunicações telegráficas e comunicações telefônicas. O inciso mencionado também inova ao indicar que o sigilo quanto às comunicações telefônicas é afastado diante de "ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". As hipóteses de afastamento do sigilo trazidas pelo inciso são reguladas pela Lei nº 9.296/1996, que trata dos procedimentos de interceptação de comunicações telefônicas.

Com base no referido dispositivo normativo, surge a controvérsia acerca de sua interpretação textual[46]. Embora o inciso XII do artigo 5º da CRFB mencione expressamente o termo "dados" ao tratar da inviolabilidade do sigilo, o direito tutelado em questão é relativo aos processos de comunicação e não às informações comunicadas[47]. Como destaca Tércio Sampaio Ferraz Júnior, especialista do tema:

---

[43] Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao91.htm. Acesso em 5 out. 2021.

[44] Manoel Gonçalves Ferreira Filho aponta que a hipótese de sigilo de dados "veio a ser prevista, sem dúvida, em decorrência do desenvolvimento da informática. FILHO, Manoel Gonçalves Ferreira. Comentários à Constituição Brasileira de 1988, São Paulo, 1990, vol. 1 p.38)

[45]Nesse sentido, afirma Tania Nigri: "A inviolabilidade do sigilo de dados foi introduzida apenas na última Constituição brasileiras, sendo comemorada por muitos, já que a inovação tecnológica, com a difusão da Internet e da telefonia celular, trouxe consigo a necessidade de proteção dessas novas formas de comunicação". NIGRI, Tânia. O Sigilo Bancário e a Jurisprudência do Supremo Tribunal Federal – STF.

[46] O Professor Técio Sampaio aponta que: "o sigilo de dados é uma hipótese nova, trazida pela Constituição Federal de 1988 (art. 5º, XII). A inovação trouxe com ela dúvidas interpretativas que merecem, por isso mesmo, uma reflexão mais detida.

[47]"A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação. Doutro modo, se alguém, não por razões profissionais, ficasse sabendo legitimamente de dados incriminadores relativo a uma pessoa, ficaria impedido de cumprir o seu dever de denunciá-lo!" (FERRAZ JR., Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 447, 1993)

> É hoje pacífico na jurisprudência constitucional que a inviolabilidade do sigilo (da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas) refere-se ao fluxo da comunicação. No RE 418.416-8/SC, de 10/05/2006, afirmou o relator (Min. Pertence) que o inc. XII do art. 5º da CF não se refere a informações comunicadas em correspondências, mensagens tele gráficas, dados e telefonemas em si, mas à comunicação, ao seu fluxo enquanto ocorrem.

No acórdão do RE 418.416, responsável pela fixação do entendimento do STF sobre o caso, o Ministro Cezar Peluso afirma em seu voto que:

> o inviolável, nos termos da Constituição, não são quaisquer elementos da informação ou de informática, mas os processos de comunicação em si. O objeto tutelado, portanto, é o processo de comunicação, enquanto restrito aos comunicantes, independentemente do conteúdo da comunicação, porque se trata, na verdade, de resguardar a privacidade dos interlocutores em ato típico de intersubjetividade.

A partir das considerações do Ministro, compreende-se que embora o objeto do sigilo não seja a informação, sua inviolabilidade serve como uma proteção anterior à privacidade. Nessa perspectiva, trata-se de um direito mais amplo, que acaba por garantir a proteção de outro. É possível, no entanto, violar o sigilo sem necessariamente atingir a privacidade de um sujeito, como aponta Tércio Sampaio Ferraz Júnior, ao afirmar que a interceptação de uma mensagem viola o sigilo ainda que o conteúdo dela seja integralmente público[48].

Conclui-se que, em relação à proteção de dados, tema central desse estudo, que o sigilo tem a função de resguardar a privacidade dos titulares, em consonância com o entendimento proferido pelo STF por meio do voto do Ministro Cezar Peluso. O direito à privacidade, um dos elementos centrais da proteção de dados, encontra amparo em outro elemento desta, a inviolabilidade do sigilo de dados. Dessa forma, é necessário compreender como tais direitos fundamentais garantem que os tratamentos de dados pessoais pelo Poder Público sejam realizados adequadamente, visando a proteção da personalidade dos titulares.

2.3.3. O Acesso à Informação – A evolução de um direito caro à consolidação da democracia

[48] "Quando, por outro lado, alguém - um outro - intercepta uma mensagem, por exemplo abre uma carta que não lhe foi endereçada, ocorre violação de sigilo. Não importa o conteúdo da comunicação epistolar; não importa, pois, que na carta esteja apenas a reprodução de um artigo de jornal publicado na véspera. O sigilo terá sido violado de qualquer modo, mesmo se o conteúdo da correspondência é público, pois a proteção não é para o que consta da mensagem (tecnicamente, o chamado relato ou conteúdo comunicado), mas para a ação de enviá-la e recebê-la". Disponível em http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/98. Acesso em 4 out. 20211

O direito de acesso à informação, qualificado pela Constituição Federal como fundamental, e sustentado pelo princípio da publicidade, obrigatório à Administração Pública em sua atuação, como determina o caput do artigo 37 da Carta Magna, é extremamente caro à estrutura da República Federativa do Brasil. No processo de evolução da democracia brasileira, é clara a tendência à expansão da publicidade e da transparência quanto aos atos da administração pública, previstas múltiplas vezes na Constituição Federal[49] e reguladas pela Lei de Acesso à Informação. Tais atributos são essenciais à garantia da soberania popular, positivada no parágrafo único da Constituição da República Federativa do Brasil, que determina que "(t)odo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição". Nesse sentido, o Ministro Roberto Barroso, em decisão em 2017, da Ação Originária 2367/DF ressalta:

> Como venho afirmando nesta Corte, a transparência se impõe porque decorre (i) do princípio democrático (CF/1988, art. 1º, caput), (ii) do sistema representativo (CF/1988, art. 1º, parágrafo único), (iii) do regime republicano (CF/1988, art. 1º,caput), e (iv) do princípio da publicidade (CF/1988, art 37, caput..

A Lei de Acesso à informação[50], voltada a regular previsões da Constituição Federal relativas ao direito de acesso à informação, é um marco importante na defesa desse direito fundamental, assim como a LGPD é para o direito à proteção de dados. Diferentemente da Lei 13.709/2018, que apenas acrescentou dois incisos ao texto do MCI[51], a LAI revogou integralmente a Lei 11.111/2005[52] e o capítulo relativo ao acesso e sigilo dos documentos

[49]A LAI aponta para os dispositivos da Constituição Federal que versam sobre o tema. O inciso XXXIII do artigo 5º dispõe sobre o direito a receber informações de interesse partciular, coletivo ou geral, dos órgãos públicos. O inciso II do parágrafo 3º do artigo 37 prevê que o acesso a registros administrativos e a informações sobre atos do governo seriam disciplinados por lei. O inciso IX do artigo 93 determina a publicidade de todos os julgamentos dos órgãos do Poder Judiciário, com as devidas ressalvas. Por fim, o parágrafo 2º do artigo 216 dispõe que em relação ao patrimônio cultural brasileiro "(c)abem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem".

[50] "Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências" - Lei LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011.

[51] A única alteração sob outra lei realizada pela LGPD está disposta em seu artigo 60, que adiciona o inciso X ao artigo 7º do MCI "X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais", e o inciso II ao artigo 16 da mesma norma: "II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais."

[52] "Regulamenta a parte final do disposto no inciso XXXIII do caput do art. 5º da Constituição Federal e dá outras providências." - Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11111.htm. Acesso em 4 out. 2021

públicos (artigos 22 a 24) da Lei 8.159/1991[53], que dispunha sobre a política nacional de arquivos públicos e privados. Além disso, alterou a Lei 8.112/1990[54], acrescentando dois dispositivos ao regulamento no sentido de incumbir os servidores públicos a denunciarem irregularidades que tiverem ciência em razão do cargo, resguardados de qualquer responsabilização civil, penal ou administrativa por fazê-lo.

Em contraste com a incidência nos âmbitos público e privado, elemento do caráter "Geral" da LGPD, a LAI é voltada exclusivamente para as atividades vinculadas ao interesse público ou à administração pública, que passam a ter de respeitar o artigo 3º, nos seguintes moldes:

> Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:
> I - observância da publicidade como preceito geral e do sigilo como exceção;
> II - divulgação de informações de interesse público, independentemente de solicitações;
> III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
> IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
> V - desenvolvimento do controle social da administração pública.

A partir desse artigo, extrai-se a positivação da publicidade como regra e do sigilo como exceção. Em voto, no acórdão do ARE 652777/SP, a Ministra Cármen Lúcia se posiciona no seguinte sentido:

> considero, como bem-dito pelo Professor Celso Antônio Bandeira de Mello, que esta Lei de acesso à informação é uma lei que muda a Administração Pública. Ela ajuda, se ela não é perfeita, como nenhuma lei é, depende exatamente da interpretação e da aplicação. E é por isso que, neste caso, o provimento deste recurso se faz exatamente no sentido de garantir a efetividade e a mudança de uma tônica e de um modelo de Administração Pública, no que me parece tornar cada vez mais republicano.

A LAI e a LGPD não são leis incompatíveis. Ainda que seus objetivos diretos sejam aparentemente contraditórios, as duas são instrumentos voltados a reforçar a democracia. Enquanto os princípios da necessidade e da minimização, originários do inciso III do artigo 6º da LGPD a norteiam, em sentido contrário, a LAI determina que a regra é o acesso às informações e o sigilo a exceção. Apesar de estabelecer a preponderância da publicidade na atividade pública, a própria LAI traz limites à aplicação do direito de acesso à informação, da mesma forma que a

[53] Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L8159.htm#art26. Acesso em 4 out 2021
[54] Disponível em http://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Acesso em 4 out 2021

LGPD prevê os casos em que não há incidência da lei. Os limites do acesso à informação são apontados nos capítulos IV - "Das restrições de acesso à informação" (artigos 21 a 30), que trata basicamente sobre o sigilo à informação, e V - Das Informações Pessoais" (artigo 31), como se observa:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
>
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
>
> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
> I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
> II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
> III - ao cumprimento de ordem judicial;
> IV - à defesa de direitos humanos; ou
> V - à proteção do interesse público e geral preponderante.

A partir desse trecho original da lei, percebe-se uma preocupação do legislador, ainda em 2011, acerca das informações pessoais tratadas pelo Poder Público, ao demandar o consentimento dos titulares dos dados para o compartilhamento com terceiros. Analisando o dispositivo através do histórico normativo do ordenamento brasileiro, é possível notar uma evolução da consciência sobre a importância do tratamento de dados adequado, ao ponto do marco legislativo do direito ao acesso à informação, responsável por expandir a transparência e publicidade no âmbito público, estipular as condições e limitações em relação ao tratamento de informações pessoais, atividade conceituada, antecipadamente, de maneira similar à LGPD[55].

Apesar de prever elementos que viriam a ser incorporados posteriormente pela LGPD, a LAI regulamentou o tratamento de informações pessoais com base exclusivamente nos direitos

[55] O conceito expansionista de "informações pessoais" foi reforçado pela LGPD, a partir da definição de "dados pessoais", como "informação relacionada a pessoa natural identificada ou identificável".

fundamentais positivados pela Constituição Brasileira à época de sua elaboração. Desse modo, a proteção de dados não foi contemplada expressamente, restando protegidos apenas alguns direitos e princípios que a compõem. O caput do artigo 31 menciona a transparência, o respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais, antecipando um dos princípios listados no artigo 6º (transparência) e três fundamentos da proteção de dados, positivados no artigo 2º (respeito à privacidade, a liberdade de expressão, de informação, de comunicação e de opinião e a inviolabilidade da intimidade, da honra e da imagem) da LGPD.

Sendo considerada uma garantia individual, a proteção de dados poderia ser invocada de acordo com o texto do caput do artigo 31 da LAI, que prevê que o tratamento das informações pessoais deve ser feito com respeito às garantias individuais. Nessa perspectiva, o Ministro Ricardo Lewandowski, ao votar sobre ADI 6.387 cita os ensinamentos do Professor Danilo Doneda, ratificados então pelo STF, que passa a entender que:

> (A) resposta se aproxima da constatação de que a proteção de dados pessoais seria uma garantia de caráter instrumental, derivada da tutela da privacidade, mas que não poderia estar limitada por esta, ao mesmo tempo em que faz referência a todo leque de garantias fundamentais que se encontram no ordenamento brasileiro.

Nesse sentido, é possível uma construção hermenêutica que contemple uma aplicação harmônica das leis em questão. Havendo interesse público na publicidade de dados pessoais, pode-se entender que é possível a existência de uma finalidade legítima, compatível com uma base legal prevista pela lei, que possibilite o tratamento, desde que observadas as demais normas decorrentes da LGPD, com destaque para o princípio da necessidade. Em paralelo, quando há o tratamento de informações pessoais, nos moldes do parágrafo artigo 31 da LAI, há limitações ao acesso e divulgação, como previsto nos incisos 1 e 2 do referido dispositivo, voltadas a proteger os dados numa perspectiva apenas da tutela à privacidade, sendo necessária uma análise sobre a possibilidade de expansão interpretativa quanto aos demais elementos da proteção de dados.

Além da defesa à proteção de dados incorporada pela Lei de Acesso à Informação ser insuficiente e frágil, o que propicia uma aplicação da lei contra tal direito fundamental, outro ponto que pode causar atrito entre a LAI e a LGPD é a previsão do afastamento do consentimento com base na privacidade diante do “interesse público”, conceito amplo e ainda

nebuloso. No artigo "Diálogos entre a Lei Geral de Proteção de Dados", Ana Carla Harmatiuk Matos e Carlos Eduardo Pianovski Ruzyk pontuam que:

> Ambas as leis aqui examinadas empregam, em momentos diversos, o conceito indeterminado de interesse público a justificar o acesso de terceiros a dados pessoais-inclusive, em certas hipóteses, de dados sensíveis. São exemplos disso: (a) o disposto no inciso II do artigo 3º da Lei de Acesso à Informação, ao definir a divulgação de informações de interesse público como diretriz da lei; (b) o inciso V do § 3º do artigo 31 da mesma lei, ao versar sobre dispensa de consentimento para tratamento de informações pessoais; (c) o§ 3° do artigo 7° da Lei Geral de Proteção de Dados, que vincula o tratamento de dados pessoais de acesso público ao interesse público que justifica sua disponibilização; (d) o artigo 23 da mesma lei, ao autorizar o tratamento de dados pessoais pelo poder público - com referência expressa, na norma, ao escopo da Lei de Acesso à informação - para a persecução do interesse público.

A partir dessas considerações, concluem a autora e o autor que "(a) chave hermenêutica para uma possível harmonização dos direitos fundamentais em jogo pode ser um conceito de interesse público, vinculado, ele próprio, a direitos fundamentais".

A harmonização dos direitos da proteção de dados com o do acesso à informação torna-se ainda mais urgente no contexto da atual sociedade guiada por dados. Como aponta Vanessa Barbosa Figueiredo de Azevedo, com base no texto "The information society", de Nick Moore[56], "a ampliação do acesso do público em geral à informação, o qual passa a desempenhar com maior consciência os seus direitos de consumidor perante os serviços públicos e privados" é uma das três principais características da sociedade da informação[57].

Diante do exposto, faz-se necessária uma reavaliação acerca da estrutura pública de compartilhamento e disponibilização de dados pessoais. A publicidade e transparência no âmbito público devem continuar a ser estimuladas, porém, a partir de uma cultura de proteção de dados,

---

[56] Disponível em https://files.dnb.de/EDBI/www.unesco.org/webworld/wirerpt/wirenglish/chap20.pdf - Acesso em 5 out. 2021

[57] "Estudos mais aprofundados apontam como sendo 3 (três) as principais características da "sociedade da informação": (1) a informação vista como recurso financeiro ou mercadoria apta a estimular o mercado empreendedor a dela fazer melhor uso, com a finalidade de potencializar a eficiência, estimular a inovação e aumentar a eficácia e posição competitiva; (2) a ampliação do acesso do público em geral à informação, o qual passa a desempenhar com maior consciência os seus direitos de consumidor perante os serviços públicos e privados; e (3) a criação de um setor econômico destinado aos produtos e serviços informáticos." - A Proteção dos Dados Pessoais na Sociedade Da Informação e Suas Implicações no Direito Notarial e Registral: Um Percurso Dogmático Evolucional da Estônia ao Brasil com Escalas em Espanha e Portugal - DE AZEVEDO, Vanessa Barbosa Figueiredo. Disponível em https://www.google.com/url?q=https://eg.uc.pt/bitstream/10316/90251/1/Dissertacao%2520de%2520Mestrado%2520-%2520Vanessa%2520Azevedo%252013.07.2019%2520.pdf&sa=D&source=editors&ust=1632783366711000&usg=AOvVaw1kbE5Ep4SlBs6dgNi3E660. Acesso em 5 out. 2021.

observando sempre o princípio da necessidade e com atenção maior ainda à finalidade do compartilhamento e da disponibilização de dados pessoais.

2.3.3.1 Jurisprudência do Supremo Tribunal Federal acerca da publicação da remuneração de servidores públicos em site na internet

O STF já decidiu múltiplas vezes sobre a possibilidade de divulgação de dados pessoais referentes à remuneração de servidores públicos. O ARE 652.777/SP tratou do caso de uma servidora do Município de São Paulo, que contestava o compartilhamento de sua remuneração, vinculado ao seu nome, no site "De Olho Nas Contas". Antes de chegar ao STF, o Colégio Recursal de São Paulo proferiu acórdão determinando a exclusão do nome da requerente e da respectiva vinculação aos vencimentos do site, com base nos seguintes entendimentos:

> a) a publicação na rede mundial de computadores do nome do funcionário com seu respectivo salário não encontra apoio infraconstitucional e tampouco na Constituição; (b) a publicidade deve ser limitada à divulgação dos salários correspondentes aos cargos, sem vinculação direta com o nome do servidor, sob pena de ofensa ao direito à intimidade; (c) a divulgação de informações pessoais dos servidores mostra-se infrutífera e desarrazoada e submete a risco a segurança do servidor, que vê sua privacidade exposta publicamente; e (d) critérios da razoabilidade e da proporcionalidade balizam a preponderância do interesse público sobre o particular.

O Município de São Paulo recorreu, buscando a reforma do acórdão. O STF deu provimento ao recurso, fixando o entendimento de que tratando-se de remuneração de servidor público, o direito à privacidade seria mitigado, diante das previsões normativas constitucionais e infraconstitucionais de divulgação dessas informações, além do interesse público dos cidadãos, que só podem exercer o direito de denunciar irregularidades ou ilegalidades perante o Tribunal de Contas da União, previsto no artigo 72 da CRFB, se obtiverem as informações transparentes quanto aos gastos dos entes federativos.

Na AO 2367 / DF, a Associação dos Juízes Federais do Rio e Janeiro e Espírito Santo – AJUFERJES tentou afastar a incidência da resolução 215/2015 do CNJ, que alterou a resolução 151/2015 do CNJ, no sentido de ampliar a disponibilização detalhada de informações sobre a remuneração dos magistrados. O pedido foi julgado improcedente, considerando que

> 1. Não há violação à intimidade ou à vida privada na divulgação nominal e pormenorizada da remuneração de magistrados, pois os dados são de interesse público e a transparência se impõe. Precedentes. 2. A jurisprudência do STF entende prevalecer, no caso, o princípio da publicidade administrativa, que concretiza a República como forma de governo.

Tratando-se de informação sobre servidor público relativa ao exercício de sua função e havendo um interesse público, principalmente no sentido de garantir o controle dos indivíduos da sociedade, o STF compreende que o direito à privacidade não pode comprometer a divulgação de tais dados, ainda que incidam de alguma forma na esfera particular dos servidores. Deve-se empregar, como pontuado, o princípio da necessidade, de modo a divulgar o mínimo de dados pessoais possíveis para o alcance do objetivo de permitir o controle dos cidadãos. Essa hipótese, pelo menos, encontra-se, até o momento, pacificada. O interesse público sobre os dados pessoais dos servidores, relativos às atividades públicas, seria suficiente para a divulgação destes.

Por ser um tratamento de dados pessoais, independentemente do entendimento acerca da necessidade de sua ocorrência, a disponibilização de tais dados deve observar as regras da LGPD, sendo necessário apontar a finalidade e a base legal que possibilitam a ocorrência da atividade. Nesse caso concreto, a finalidade seria viabilizar o acesso dos dados aos cidadãos a fim de garantir o controle sobre os gastos públicos. A hipótese de permissão do tratamento prevista em lei seria a do inciso II do artigo 7º, de cumprimento de obrigação legal ou regulatória, a partir do entendimento de que esse compartilhamento seria uma obrigação legal que alcança todos aqueles que tratam esse tipo de dados pessoais, com base na Constituição e na jurisprudência do STF. Por fim, deve-se atentar ao princípio da necessidade, disponibilizando apenas o necessário para atingir a finalidade, dispensando dados pessoais excessivos.

Superado esse caso, consolidado pela jurisprudência do STF, deve-se buscar compreender como o interesse público incide sobre os dados pessoais dos demais cidadãos, principalmente nos casos em que não são servidores públicos.

3. APLICAÇÃO PRÁTICA DA PROTEÇÃO DE DADOS PELO PODER PÚBLICO

A partir das questões normativas e principiológicas expostas, é necessário compreender como a tutela da proteção de dados ocorre ou deveria ocorrer na prática. Para tanto, analisar-se-á, de maneira breve, sua aplicação na dinâmica do Poder Judiciário, observando a evolução percorrida pelo direito da proteção de dados desde a apresentação da LGPD e sua incidência nas decisões da Controladoria-Geral da União acerca dos recursos de negativa de acesso à informação, previstos na LAI.

3.1 Proteção de Dados no Poder Judiciário

Uma das atividades que mais evidenciam os conflitos entre a publicização e a garantia à proteção de dados é a jurisdicional. Em regra, os atos processuais devem ser publicamente acessíveis, como prevê a Constituição Federal, no inciso LX do artigo 5º. Tanto o código de processo penal em seu artigo 792[58], quanto o código de processo civil, em seu artigo 189[59] enfatizam a necessidade da publicização dos atos processuais. A Resolução 215/2015 do Conselho Nacional de Justiça (CNJ)[60] estipula parâmetros para o cumprimento da LAI no âmbito do Judiciário.

Como aponta o Ministro do Superior Tribunal de Justiça Ricardo Villas Bôas Cueva[61], essa regra originalmente aplicável aos atos processuais sofreu uma expansão por meio da Lei

[58]Art. 792: As audiências, sessões e os atos processuais serão, em regra, públicos e se realizarão nas sedes dos juízos e tribunais, com assistência dos escrivães, do secretário, do oficial de justiça que servir de porteiro, em dia e hora certos, ou previamente designados.§ 1º Se da publicidade da audiência, da sessão ou do ato processual, puder resultar escândalo, inconveniente grave ou perigo de perturbação da ordem, o juiz, ou o tribunal, câmara, ou turma, poderá, de ofício ou a requerimento da parte ou do Ministério Público, determinar que o ato seja realizado a portas fechadas, limitando o número de pessoas que possam estar presentes.§ 2º As audiências, as sessões e os atos processuais, em caso de necessidade, poderão realizar-se na residência do juiz, ou em outra casa por ele especialmente designada

[59]Art. 189: Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos: I - em que o exija o interesse público ou social; II - que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes; III - em que constem dados protegidos pelo direito constitucional à intimidade; IV - que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.§ 1º O direito de consultar os autos de processo que tramite em segredo de justiça e de pedir certidões de seus atos é restrito às partes e aos seus procuradores.§ 2º O terceiro que demonstrar interesse jurídico pode requerer ao juiz certidão do dispositivo da sentença, bem como de inventário e de partilha resultantes de divórcio ou separação.

[60]Resolução 215/2015 do Conselho Nacional de Justiça (CNJ)

[61] CUEVA, Ricardo Villas Bôas. A Incidência da Lei Geral de Proteção de Dados Pessoais nas Atividades do Poder Judiciário. In: *CUEVA. Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel; Lei Geral de Proteção*

13.793/2019, que incluiu o §7º ao artigo 11[62] da Lei 11.419/2006 – Lei do Processo Eletrônico, passando a valer também para os documentos presentes nos autos. Essa dilatação da norma resulta na disponibilização massiva de dados pessoais, sendo muitos deles sensíveis.

Ao ingressar numa ação, por vontade própria, figurando o polo ativo, ou de maneira involuntária, como réu, o titular de dados entrega ao site do Tribunal, no mínimo, nome, CPF, RG, endereço, endereço eletrônico, imagem do rosto, data de nascimento, nomes dos ascendentes que constarem na carteira de identidade, dentre diversas outras informações pessoais, que ficam acessíveis a quaisquer profissionais da advocacia cadastrados nos sites dos tribunais. Como defende o Professor Filipe Medon, o problema não está na disponibilidade dos dados em si, uma vez que é prevista em lei, mas sim na facilidade ao acesso, que muitas vezes pode servir para tratamentos com outras finalidades[63].

Na teoria, para se realizar o acesso aos autos de processos alheios, é necessário demonstrar "interesse para fins apenas de registro", como previsto no §7º ao artigo 11 da Lei do Processo Eletrônico[64]. Na prática, ainda que possa haver o registro de quem acessou os autos de um processo, não há um controle efetivo sobre a finalidade com a qual os sujeitos habilitados acessam e até mesmo coletam os dados pessoais disponíveis, o que afasta a transparência sobre o tratamento de compartilhamento dos dados dos titulares, envolvidos nos processos.

O Conselho Nacional de Justiça tem elaborado recomendações, resoluções e portarias a fim de consolidar a garantia do direito à proteção de dados na atividade jurisdicional. Em abril

---

de Dados (Lei nº 13.709/2018) A Caminho da efetividade: contribuições para a implementação da LGPD. São Paulo. Thomson Reuters Brasil, 2020. p. 204.

[62] Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais."(...)"§ 7º Os sistemas de informações pertinentes a processos eletrônicos devem possibilitar que advogados, procuradores e membros do Ministério Público cadastrados, mas não vinculados a processo previamente identificado, acessem automaticamente todos os atos e documentos processuais armazenados em meio eletrônico, desde que demonstrado interesse para fins apenas de registro, salvo nos casos de processos em segredo de justiça

[63] Citação ao artigo "Quem precisa de vazamento de dados que já estão disponíveis no processo eletrônico?" de Filipe Medon. Disponível em https://www.jota.info/opiniao-e-analise/artigos/quem-precisa-de-vazamento-de-dados-que-ja-estao-disponiveis-no-processo-eletronico-14062020. Acesso em 4 out. 2021.

[64]Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.
[...]
§ 7º Os sistemas de informações pertinentes a processos eletrônicos devem possibilitar que advogados, procuradores e membros do Ministério Público cadastrados, mas não vinculados a processo previamente identificado, acessem automaticamente todos os atos e documentos processuais armazenados em meio eletrônico, desde que demonstrado interesse para fins apenas de registro, salvo nos casos de processos em segredo de justiça."

de 2019, a portaria 63/2019 do CNJ[65] instituiu o "Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais", revogada em outubro de 2020, pela portaria 212/2020 do CNJ[66], que com foco ainda maior à proteção de dados, instituiu o "Grupo de Trabalho destinado à elaboração de estudos e de propostas votadas à adequação dos tribunais à Lei Geral de Proteção de Dados".

A Recomendação 73/2020[67], em 20 de agosto de 2020, sugere aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições da LGPD. No ano seguinte, o CNJ emitiu as Resoluções 363 de 2021[68] e 389 de 2021[69]. A primeira estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. A segunda, altera a Resolução do CNJ nº 215/2015[70], relativa à aplicação das disposições da LAI nos tribunais. Considerando a data de promulgação da LGPD e a previsão inicial para o início integral de sua vigência, tais recomendações e resoluções exemplificam bem a demora dos sujeitos envolvidos no tratamento de dados para começarem a tratar da adequação de suas normas.

Enquanto não são estabelecidos parâmetros mais claros para a limitação da atividade de compartilhamento de dados pessoais por parte do Poder Público, ou mais especificamente pelo Poder Judiciário, o engajamento dos servidores e dos próprios cidadãos, titulares desses dados é essencial, não só para a criação da cultura de proteção de dados, mas para a efetivação da tutela desse direito fundamental. Nesse sentido, o trabalho do Tribunal de Justiça do Estado de Santa Catarina em relação à matéria tem sido um exemplo para os demais Tribunais.

O Tribunal de Justiça de Santa Catarina - TJSC tornou-se referência nacional em relação à adequação da LGPD, sendo pioneiro na busca pela construção de uma cultura da proteção de dados e na implementação de suas normas. Desde 12 de junho de 2019, muito antes da promulgação da Recomendação 73/2020 do CNJ, o Tribunal conta com um Comitê Gestor de

---

[65] Disponível em https://atos.cnj.jus.br/files/compilado043105202008065f2b8789824e1.pdf. Acesso em 5 out. 2021
[66] Disponível em https://atos.cnj.jus.br/files/compilado1822532021053160b5297d85126.pdf. Acesso em 5 out. 2021
[67]Disponível em https://atos.cnj.jus.br/files/compilado135819202102266038fe7b3b752.pdf. Acesso em 5 out. 2021
[68]Resolução nº 363, de 12 de janeiro de 2021. Disponível em: https://atos.cnj.jus.br/files/original181204202101196007 20f42c02e.pdf. Acesso em 5 out. 2021
[69]Resolução 389 de abril de 2021. Disponível em: https://atos.cnj.jus.br/files/original131551202105056092 9a87e9e88.pdf Acesso em 5 out. 2021
[70]Disponível em https://atos.cnj.jus.br/files/compilado1434312021050360900 9f71d939.pdf. Acesso em 5 out. 2021.

Proteção de Dados - CGPD, instituído pela Resolução GP nº 28 de 12 de junho de 2019[71], que além de criar o Comitê, designou sua estrutura e suas atribuições[72].Em 17 de julho de 2020, de forma antecipada à entrada em vigor da LGPD por completo, a desembargadora Denise de Souza Luiz Francoski foi nomeada, conforme previsto no inciso III do artigo 23 da lei[73], encarregada do TJSC, por meio da Portaria GP nº 1.481[74].

O TJSC vem buscando uma aproximação com os titulares de dados por meio dos canais disponibilizados pela Ouvidoria. Na seção da Ouvidoria, no site do Tribunal, há diversas informações, explicadas de maneira didática sobre a LGPD. Além disso, o site disponibiliza a política de privacidade do Tribunal e traz as informações sobre a encarregada, conforme o artigo 41 da LGPD[75]. Em parceria com o Instituto de Tecnologia e Sociedade – ITS, o TJSC desenvolveu o LGPDJus, um aplicativo disponível para sistemas Android e IOS, por meio do qual qualquer cidadão consegue solicitar a consulta, modificação e a exclusão de seus dados, podendo acompanhar pelo próprio aplicativo seus requerimentos. O aplicativo ainda apresenta as informações sobre LGPD que constam no site, incluindo os contatos da encarregada.

Diante de todo trabalho e da prática observada desde o início das atividades do CGPD do TJSC, a encarregada desembargadora Denise de Souza Luiz Francoski participou do processo de

---

[71]Resolução GP. nº 28/2019. Disponível em: http://busca.tjsc.jus.br/buscatextual/integra.do?cdSistema=1&cdDocumento=174510&cdCategoria=1&q=&frase=&excluir=&qualquer=&prox1=&prox2=&proxc=Acesso em 4 out. 2021

[72]As atribuições são descritas no Artigo 3º da portaria que constituiu o CGPD:
"Art. 3º São atribuições do CGPD:
I - avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade do Poder Judiciário do Estado de Santa Catarina com as disposições da Lei n. 13.709, de 14 de agosto de 2018;
II - formular princípios e diretrizes para a gestão de dados pessoais e propor sua regulamentação;
III - supervisionar a execução dos planos, dos projetos e das ações aprovados para viabilizar a implantação das diretrizes previstas na Lei n. 13.709, de 14 de agosto de 2018;
IV - prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na Lei n. 13.709, de 14 de agosto de 2018 e nas normas internas; e
V - promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos."

[73] "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
[...]
III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;"

[74] "Portaria disponível em: http://busca.tjsc.jus.br/dje-consulta/rest/diario/pagina?edição=3347_cd_Caderno=4página=1 - Acesso em 5 out. 2021

[75] "Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador."

elaboração da Resolução 363/2021 do CNJ, utilizando as experiências da adequação às normas de proteção de dados do TJSC a fim de alcançar uma padronização no processo dos demais tribunais pelo Brasil[76].

Reforçando a ideia de que LGPD e LAI podem ser compatíveis, a Resolução nº 389/2021[77] do CNJ realizou alterações na Resolução nº 215/2015 (que trata exclusivamente da LAI), que passou a ter o seguinte texto no artigo 1º:

> Art. 1º O acesso à informação previsto na Lei no 12.527/2011, Lei de Acesso à Informação (LAI), e a transparência na divulgação das atividades dos órgãos do Poder Judiciário e serviços auxiliares seguem o disposto nesta Resolução, sem prejuízo da observância dos ditames da Lei nº 13.709/2018 e das medidas preconizadas pela Resolução CNJ nº 363/2021.

Por fim, é interessante observar algumas práticas implementadas nos tribunais internacionais. O Ministro Ricardo Villas Bôas Cueva aponta para o engajamento sobre a proteção de dados pessoais de alguns outros tribunais[78], com destaque para a adoção da anonimização de dados pessoais nos processos, realizada na França.

3.2 A proteção de dados nas decisões da CGU quanto à solicitação de acesso à informação aos órgãos e entes públicos

A Lei de Acesso à Informação estabelece que os cidadãos têm o direito de solicitar informações aos órgãos ou entes públicos, os quais devem analisar a possibilidade de disponibilização dos dados públicos requeridos, podendo decidir por apresentá-los ou não diante

---

[76] Como a própria desembargadora relata no evento "LIVE DPBR: Lei Geral de Proteção de Dados e Poder Judiciário", aos 41 minutos e 56 segundos do vídeo do evento disponível em https://www.youtube.com/watch?v=wGEsB82_eUE&t=2071s. Acesso em 5 out. 2021

[77] Disponível em https://atos.cnj.jus.br/files/original131551202105056092 9a87e9e88.pdf. Acesso em 6 out. 2021

[78] "Outros países europeus também têm se adaptado ao novo regime de proteção de dados pessoais. A Corte de Cassação da França, por exemplo, desde 2016 já conta com software para efetuar a anonimização de suas decisões. O Judiciário da Inglaterra já tem, desde maio de 2018, um órgão encarregado de processar as reclamações relativas ao tratamento de dados pessoais pelos tribunais, magistrados e servidores da justiça ingleses. Na Espanha, o Conselho Geral do Poder Judiciário tem um delegado de proteção de dados pessoais e disponibiliza em seu sítio na internet um minudente registro de atividades de tratamento, com descrição, para cada uma das atividades, da finalidade do trata mento, de base jurídica, das categorias de dados e de destinatários atingidos. sua do prazo de conservação e das medidas de segurança requeridas, entre outras informações úteis para que se proceda ao tratamento de dados pessoais no âmbito dos tribunais de forma segura e em conformidade com a lei nacional e com o RGPD." – CUEVA, Ricardo Villas Bôas. *A Incidência da Lei Geral de Proteção de Dados Pessoais nas atividades do Poder Judiciário*. In: In: CUEVA, Ricardo Villas Bôa; DONEDA, Danilo; MENDES, Laura Schertel (Org.). *Lei Geral de Proteção de Dados (Lei nº 13.709/2018) A caminho da efetividade: contribuições para a implementação da LGPD*. São Paulo. Thomson Reuters Brasil, 2020. p. 208

de determinados critérios previstos pela lei. Érica Bezerra Queiroz Ribeiro e Bruno Amaral Machado apontam que:

> Ao analisar um pedido de acesso a informações, cabe à autoridade pública demonstrar que a informação solicitada está sujeita a uma das hipóteses de restrição, uma vez que a presunção estabelecida pelo regime jurídico de acesso a informações é a de que a negativa é uma exceção ao princípio da máxima divulgação (CUNHA FILHO; XAVIER, 2014, p. 114). Desse modo, cabe ao Estado justificar eventual negativa de acesso a informações, e não ao solicitante comprovar que não incide hipótese para restrição do acesso (HERMANY; BOLESINA, 2015, p. 74; MENDEL, 2009, p. 32).

Como exposto anteriormente, quando as informações solicitadas forem relativas a dados pessoais, a LAI prevê no artigo 31 que a privacidade é um dos elementos que pode ensejar a necessidade do consentimento do titular de dados para o compartilhamento pelo poder público com aqueles que o requererem. O interesse público, no entanto, pode ser o suficiente para afastar esse requisito ligado à proteção da vida privada.

Dessa forma, a fim de evitar irrazoabilidades e irresponsabilidades, não se deve invocar o interesse público para compartilhar dados pessoais a qualquer custo, deixando de observar as garantias à proteção dos dados. Afinal, havendo informações pessoais, torna-se imprescindível a observação da LGPD e demais normas afins. Assim, para analisar a possibilidade da concessão ou negação das solicitações que dizem respeito a informações pessoais, é preciso compreender o caso concreto, considerando o equilíbrio entre a proteção da personalidade dos indivíduos detentores dos dados e a garantia do cumprimento do interesse público.

Em relação à decisão de atendimento ou não das solicitações, são previstas pela LAI algumas instâncias recursais. O artigo 16 da lei institui que "(n)egado o acesso à informação pelos órgãos ou entidades do Poder Executivo Federal, o requerente poderá recorrer à Controladoria-Geral da União, que deliberará no prazo de 5 (cinco) dias (...)".

Nesse cenário, diante dos processos decisórios que envolvem dados pessoais, a CGU adotou, sob influência da Rede de Transparência e Acesso à Informação (RTA), um método de análise que consiste na realização de testes de dano e do interesse público, com base no "princípio do escopo limitado de exceções", apresentado pelo documento "The Public's Right to Know: Principles on Right to Information Legislation ", desenvolvidos originalmente em 1999 e atualizados em 2015 pela organização não-governamental Article 19 .

No artigo que investiga a aplicação de tal técnica pela CGU, Érica Bezerra Queiroz Ribeiro e Bruno Amaral Machado trazem a tradução de parte do referido documento na qual a Article 19 demonstra como se deve empregar o método em análise:

> PRINCÍPIO 4. ESCOPO LIMITADO DE EXCEÇÕES
>
> As exceções devem ser clara e estritamente delineadas e sujeitas a testes estritos de dano e interesse público.
>
> Todas as solicitações individuais de informações de órgãos públicos devem ser atendidas, a menos que o órgão público possa mostrar que as informações estão dentro do escopo do regime limitado de exceções. A recusa em divulgar informações não se justifica, a menos que a autoridade pública possa demonstrar que as informações atendem a um rigoroso teste de três partes.
> O teste de três partes:
> • a informação deve estar relacionada a um objetivo legítimo listado na lei;
> • a divulgação deve ameaçar causar danos substanciais a esse objetivo; e
> • o dano ao objetivo deve ser maior que o interesse público em ter a informação

Os testes, implementados em diversos países, com destaque para o México, consistem numa importante ferramenta de controle, que possibilita à sociedade a obtenção de decisões fundamentadas com base em critérios técnicos, comprometidos com a harmonia entre os direitos fundamentais. A partir de tais testes, evidenciam-se os parâmetros adotados para a disponibilização de informações públicas, principalmente aquelas relativas a dados pessoais, que necessitam de maior maturidade, dada a importância da matéria, conforme já explanado.

CONCLUSÃO

A proteção de dados é um direito fundamental, que, no cenário atual, diante da formação da "data driven society", demonstra-se indispensável à manutenção e evolução da democracia, sendo essencial também à defesa da personalidade dos indivíduos que a compõem.

Os tratamentos realizados pelo Poder Público representam uma parcela considerável de todo o fluxo de dados pessoais existente e demandam uma análise mais profunda, diante da inafastável e compulsória relação estabelecida entre o Estado e os indivíduos. Ao se aplicar a LGPD e as demais normas de proteção de dados na esfera pública, observa-se uma pluralidade de direitos fundamentais com os quais a proteção de dados deve se adequar. Dentre eles, destacam-se o direito de acesso à informação e o direito ao sigilo de dados, previstos no artigo 5º da Constituição Federal, que devem ser explorados, visando a harmonia na aplicação conjunta de múltiplas normas, de caráteres diferentes.

Nesse sentido, a Administração Pública precisa criar seus parâmetros limitantes ao processamento de dados de seus cidadãos, estabelecendo, por exemplo, guias vinculantes, para garantir a aplicação harmônica dos direitos fundamentais. Faz-se necessário afastar termos "genéricos" e apoiar-se em medidas específicas, visando uma maior segurança jurídica aos titulares dos dados para que detenham controle sobre eles e possam confiar no poder público. Deve-se compreender os elementos que compõe o interesse público e buscar técnicas que identifiquem sua existência e sua necessidade frente à exposição de dados pessoais. A prática aplicada nas decisões da CGU, adotada a partir da Rede de Transparência e Acesso à Informação, dos testes de dano e do interesse público deve ser estimulada e aprimorada, para que o conceito amplo de "interesse público" seja mais bem definido e cada vez melhor compreendido frente aos tratamentos de dados pessoais.

A partir da compreensão de que a tutela da proteção de dados pessoais tem como objetivo a proteção de seus titulares, os direitos previstos pela LGPD devem ser amplamente disponibilizados. Para tanto, é necessária a construção de um canal aberto e bem estruturado para atender às dúvidas e aos requerimentos dos titulares de dados, assim como implementado pelo Tribunal de Justiça de Santa Catarina.

Diante de todas as considerações expostas, o Poder Público deve se ater principalmente ao fato de que, tanto a aplicação excessiva quanto a aplicação insuficiente da proteção de dados de dados representam um risco à democracia, motivo pelo qual os limites dos tratamentos, principalmente a disponibilização e o compartilhamento, de dados pessoais devem ser estipulados com clareza, por meio da adoção de normas com conceitos bem definidos e de orientações calcadas na interpretação harmônica dos direitos fundamentais.

Referências Bibliográficas

AGUILERA, Daniel Fortes; BIASE, Nicholas Furlan Di. *Dificuldades interpretativas no regime de tratamento de dados pelo poder público: Lacunas, Contradições E Atecnias Na LGPD*. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro -PGE-RJ, Rio de Janeiro, v. 4n.2, maio/ago. 2021. Disponível em https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/238/182. Acesso em 4 out. 2021

ARTICLE 19. *The Public's Right to Know: Principles on Right to Information Legislation*. London, United Kingdom. 2016. Disponível em https://www.article19.org/data/files/RTI_Principles_Updated_EN.pdf. Acesso em 6 out. 2021

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

COHEN, Julie E. *What Privacy is For*. Harvard Law Review, Vol. 126, 2013, p. 1931

CUEVA, Ricardo Villas Bôa. A incidência da Lei Geral de Proteção de Dados Pessoais nas atividades do Poder Judiciário. In: CUEVA, Ricardo Villas Bôa; DONEDA, Danilo; MENDES, Laura Schertel (Org.). *Lei Geral de Proteção de Dados (Lei nº 13.709/2018) A caminho da efetividade: contribuições para a implementação da LGPD*. São Paulo. Thomson Reuters Brasil, 2020.

DE AZEVEDO, Vanessa Barbosa Figueiredo. A Proteção dos Dados Pessoais na Sociedade da Informação e Suas Implicações no Direito Notarial e Registral: Um Percurso Dogmático Evolucional da Estônia ao Brasil com Escalas em Espanha e Portugal. Disponível em: https://eg.uc.pt/bitstream/10316/90251/1/dissertacao%20de%20mestrado%20-%20vanessa%20azevedo%2013.07.2019%20.pdf

DONEDA, Danilo. *Da privacidade à proteção de dados*. Editora Revista dos Tribunais. Ed: 2ª

GALLINDO, Sergio Paulo Gomes. *A Era Digital e a Economia Intensiva em Dados*. In: CUEVA. Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel; *Lei Geral de*

Proteção de Dados (Lei nº 13.709/2018) A Caminho da efetividade: contribuições para a implementação da LGPD. São Paulo. Thomson Reuters Brasil, 2020.

MACHADO, Bruno Amaral; RIBEIRO, Érica Bezerra Queiroz. *Privacidade e transparência: aplicação dos testes de dano e interesse público em recursos da LAI*. Revista Jurídica da Presidência. V. 21. Nº 125. Out 2019/Jan 2020. Publicado em 30 de janeiro de 2020. Disponível em https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/2028/1307. Acesso em 6, out. 2021

MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. *Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação*. In: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. (Org). *Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileio*. Ed: 2ª.

MEDON, Filipe. *Quem precisa de vazamento de dados que já estão disponíveis no processo eletrônico*. Jota. 14/06/2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/quem-precisa-de-vazamento-de-dados-que-ja-estao-disponiveis-no-processo-eletronico-14062020. Acesso em 4 out. 2021

MOORE, Nick. The information society - Nick Moore Policy Studies Institute, United Kingdom. Disponível em: https://files.dnb.de/EDBI/www.unesco.org/webworld/wirerpt/wirenglish/chap20.pdf. Acesso em 4 out. 2021

NIGRI, Tânia. *O Sigilo Bancário e a Jurisprudência do Supremo Tribunal Federal – STF*. Ed. 1ª. São Paulo. Editora IASP, 2017

OCDE. *The Path to Becoming a Data-Driven Public Sector*. OECD Publishing: Paris, 2019

SAAD, Andreia. Ela, a LGPD, vista pelas empresas: uma proposta de visão prática – e otimista" –. In: CUEVA, Ricardo Villas Bôa; DONEDA, Danilo; MENDES, Laura Schertel (Org.). Lei Geral de Proteção de Dados (Lei nº 13.709/2018) A caminho da efetividade: contribuições para a implementação da LGPD.

SCHREIBER, Anderson. *Os Direitos da Personalidade e o Código Civil de 2002.* Disponível em http://schreiber.adv.br/downloads/os-direitos-da-personalidade-e-o-codigo-civil-de-2002.pdf. Acesso em 3 out. 2021.

TEFFÉ, Chiara Spadaccini de; VIOLA , Mario; *Tratamento de Dados Pessoais na LGPD: Estudo Sobre as Bases Legais dos Artigos 7º e 11*. In: Tratado de Proteção de Dados. In: DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang (Org). *Tratado de Proteção de Dados*.

UNIÃO EUROPEIA. [RGPD (2016)]. Regulamento (UE) 2016/679 do Parlamento europeu e do Conselho, de 27 de abril de 2016. Bruxelas, BE: Parlamento Europeu e Conselho da União Europeia, [2016]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 3 outubro 2021.

VAINZOF, Rony. *Capítulo I – Disposições Preliminares*. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega; (coords.). *LGPD: Lei Geral de Proteção de Dados comentada*. Ed: 2ª. rev., atual. e ampl. São Paulo. Thomson Reuters Brasil, 2019.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. *The right to privacy*. Harvard Law Review, Boston, v.4, n.5, p.193-220, dez. 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 3 out. 2021.

WIMMER, Miriam. Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang (Org). *Tratado de Proteção de Dados*.