2026
EDITORA JusPODIVM
www.editorajuspodivm.com.br

KELVIANE DE ASSUNÇÃO FERREIRA
BARROS MACHADO

SOB VIGILÂNCIA

O EQUILÍBRIO ENTRE SEGURANÇA E PRIVACIDADE NA GESTÃO DE DADOS

3

REGIME JURÍDICO DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NO BRASIL

3.1. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

A proteção de dados pessoais foi alçada a direito fundamental expresso na Constituição da República por meio da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, após aprovação e promulgação da Proposta de Emenda à Constituição (PEC) nº 17/19.

A Emenda alterou o artigo 5º para incluir no rol de direitos fundamentais o direito à proteção de dados, inclusive nos meios digitais. Modificou também os artigos 22 e 23, estabelecendo como competência de a União legislar sobre, organizar e fiscalizar a proteção e o tratamento de dados pessoais.

Antes de se chegar à alteração formal do texto constitucional, porém, a discussão acerca do conceito e âmbito de proteção de direitos previstos na Constituição diante dos novos desafios e transformações das relações sociais seguiu caminho semelhante àquele traçado no ambiente estrangeiro acima descrito.

É importante que se destaque, ainda, que, mesmo com a previsão expressa de um direito à proteção de dados, ainda exsurgem dúvidas acerca de sua extensão e real potencialidade diante da

dinâmica das relações estabelecidas na vida em sociedade. Disso se extrai a importância de analisar a construção doutrinária, legislativa e jurisprudencial em ambiente nacional, a fim de se perquirir o que pode ser esperado da aplicação dos princípios e regras que giram em torno da proteção de dados.

Inicialmente, observa-se que a Constituição da República de 1988 reproduziu, em seu texto original, a ideia de proteção da vida privada e das comunicações na forma estática sugerida nos estudos de Warren e Brandeis, como um direito negativo, um direito à não intervenção. Essa leitura é extraída do texto do artigo 5º, no qual se lê a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (inciso X), bem como do sigilo da correspondência e das comunicações (inciso XII). Nesse contexto, também é clara a dicotomia entre as esferas pública e privada, percebendo-se no texto um indicativo a partir da enumeração de situações que ocorrem em um ambiente marcadamente privado (correspondências e comunicações).

Na doutrina, o estudo do direito à privacidade seguiu rota semelhante, como expressão da tendência externa e análise preliminar do próprio texto constitucional. Tércio Ferraz Júnior, em clássico artigo publicado em 1993, largamente citado em diversos julgados do Supremo Tribunal Federal, em que aborda o direito à privacidade e os limites à ação fiscalizadora do Estado, expressa essa propensão. No texto, expõe o jurista a correlação entre o sigilo de dados e o direito fundamental à privacidade, identificando-o como "o direito de o indivíduo excluir do conhecimento de terceiros aquilo que a ele só é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada.[1]"

1. FERRAZ JÚNIOR, Tércio. **Sigilo de dados**: o direito à privacidade e os limites da função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 430-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em 11 de novembro de 2023.

Essa posição foi adotada também na jurisprudência do Supremo Tribunal Federal que, em mais de uma oportunidade, interpretou de maneira bastante limitada o conteúdo do direito à privacidade. No ano 2001, o Tribunal reconheceu a possibilidade de o Ministério Público solicitar informações bancárias de beneficiários de auxílio governamental no Mandado de Segurança 21.729/DF.

Veja-se resumo do caso:

> "O Banco do Brasil ajuizou mandado de segurança arguindo como ato de constrangimento o ofício do Procurador-Geral da República de folha 21, reclamando o atendimento a pedidos anteriores, da Coordenadoria da Defesa dos Direitos da Pessoa Humana da Procuradoria da República no Distrito Federal, visando ao fornecimento da lista dos beneficiários de liberação de recursos, em caráter emergencial ao setor sucroalcoleeiro, bem como dados sobre encontrarem-se, ou não, os favorecidos com os créditos em débito para com o Banco, pedindo-se deste, ainda, esclarecimentos sobre a natureza das operações e as respectivas situações."[2]

No processo em análise, o Ministro relator, Marco Aurélio Mello, pontuou que o direito à preservação da intimidade mostrava-se de forma alargada e que, nos termos do texto constitucional, o sigilo de dados somente poderia ser excepcionado mediante ordem judicial para fins de investigação criminal ou instrução processual penal, não sendo possível solicitação por órgão não investido no ofício judicante. Ventilou, ainda, a limitação ao próprio acesso em razão do texto do artigo 5º, XII, da Constituição, e que a expressão "no último caso" para muitos estaria ligada apenas ao

2. BRASIL. Supremo Tribunal Federal. **Mandado de Segurança 21.729**. Distrito Federal. Relator: Ministro Marco Aurélio. Redator do acórdão: Ministro Néri da Silveira. DJ PP-00033. VOL-02048-01. PP-00067, 19 de outubro de 2001. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599. Acesso em: 11 de novembro de 2023.

sigilo das comunicações. Com esse fundamento, concedeu a ordem solicitada.

Contudo, prevaleceu, no Tribunal, entendimento divergente, no sentido de que seria possível a cessão das informações dos usuários ao Ministério Público Federal para os fins visados. O ministro redator do caso foi Néri da Silveira, que proferiu voto no sentindo vencedor.

Silveira fundamentou voto aduzindo que "não cabe chegar ao ponto de afirmar que a mera referência ao nome de quem teria sido beneficiado ou contratante, em um determinado empréstimo subsidiado pelo erário federal, em razão de um plano de Governo, constituiria matéria encoberta pelo sigilo bancário". Há destaque no voto ao fato de haver envolvimento de recursos públicos na análise. Com base nesse fundamento, indeferiu a segurança pleiteada.

Vale destacar, ainda, nesse julgamento, manifestação do Ministro Maurício Corrêa, o qual defendeu que o direito à privacidade, destinado a proteger indivíduos, "não protege operações bancárias praticadas em contas fictícias – que não têm privacidade a ser juridicamente protegida – nem pode acobertar crimes ou outros ilícitos, sejam administrativos ou civis". Ademais, ressaltou que o direito individual tem por limite interesses maiores, que dizem respeito ao interesse público. O ministro concluiu seu voto deferindo a segurança apenas por entender que não pode haver a solicitação referida por autoridade administrativa, sendo impositiva intervenção e autorização judicial como moderadora na resolução dos litígios em que se observe conflito de interesses; neste caso, o interesse individual de privacidade e o interesse do órgão do Ministério Público de limitá-la para exercício de suas funções.

Interessa nesse julgado a posição bastante conservadora do STF no que respeita à privacidade do indivíduo, a qual é vista como passível de afastamento diante de "interesse público maior". No caso, não houve, por parte dos Ministros, problematização

quanto ao alcance específico das normas do artigo 5º, X e XII, mas a observação de que não existem direitos de caráter absoluto.

Veja-se, ainda, que o pedido realizado pelo Ministério Público para o Banco do Brasil, e referendado pelo Tribunal, foi bastante genérico, requerendo-se informações de todos os favorecidos pela política pública, não apenas daqueles sobre os quais recaía alguma suspeita de fraude ou possível prática de crime aptas a serem investigadas. Essa questão, porém, não foi enfrentada no voto de qualquer dos Ministros julgadores, mas foi um dos elementos decisivos em decisão futura, quando o STF declarou inconstitucional decreto que determinava às empresas de telefonia a entrega de informações de cadastros dos consumidores no período da pandemia da Covid-19, como será visto a seguir.

Em 2006, o tema voltou à tona no Supremo Tribunal Federal no julgamento do Recurso Extraordinário 418.416-8/SC[3]. Eis um resumo do caso:

> Em juízo federal, foi deferido pedido de busca e apreensão na sede de duas empresas, das quais o recorrente era sócio-gerente, sob o fundamento de que documentos que instruíam requerimento do Ministério Público – autos de reclamação trabalhista e declaração de importação e fatura – indicavam a existência de "caixa 2", "falta de registro de empregados" e "sonegação de tributos.
>
> Após a apreensão, o juízo determinou a extensão dos efeitos do decreto de busca e apreensão para que a Receita Federal e a fiscalização do INSS tivessem acesso aos dados, documentos e informações fiscais, bancárias, financeiras e eleitorais das empresas.

3. BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 418.416-8/SC**. Distrito Federal. Relator: Ministro Sepúlveda Pertence. Redator do acórdão: Ministro Sepúlveda Pertence. Julgamento em 10 de maio de 2006. DJ 19 de dezembro de 2006. Ementário n° 2261-6. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. Acesso em: 11 de novembro de 2023.

> O recorrente foi condenado criminalmente, com decisão confirmada em segunda instância. Interpôs o recurso extraordinário alegando: 1) omissão na análise de teses de defesa e 2) equívoco da condenação, que teria sido baseada em prova obtida por meio ilícito, alegando que a decisão que determinou a busca e apreensão violou a proteção constitucional ao sigilo das comunicações (artigo 5º, X, XI, XII, LIV, LV e LVI).
>
> O recorrente também impetrou habeas corpus (HC 83.168-1/SC) com o objetivo de cassar a decisão que autorizou a quebra da confidencialidade de elementos sigilosos obtidos na busca e apreensão, ao estender à Receita Federal e à Fiscalização do INSS o acesso a todos os dados obtidos.

Foi relator do processo o Ministro Sepúlveda Pertence, que emitiu voto vencedor no sentido de negar provimento ao recurso extraordinário e julgar prejudicado o HC 83.168-1/SC, que transcorria apensado. Assim, foi mantida a condenação sob o fundamento de não ter havido ofensa à norma constitucional do sigilo de dados. Foi voto vencido apenas o Ministro Marco Aurélio Mello, que deu provimento ao recurso acolhendo a primeira tese defendida de ausência de análise, pelo tribunal de origem, de teses relevantes da defesa.

Asseverou o Ministro Sepúlveda Pertence, acompanhado dos demais, que a proteção a que se refere o artigo 5º, XII, da Constituição "é da comunicação 'de dados' e não os dados, o que tornaria impossível qualquer investigação administrativa, fosse qual fosse". Ademais, destacou que as instâncias de mérito não valoraram nenhum dado resultante da busca e apreensão e, portanto, não teria havido, no ponto, prejuízo concreto ao recorrente.

No julgamento, o Ministro Cezar Peluso reforçou a tese ao pontuar que a norma do artigo 5º, XII, quando alude ao sigilo das correspondências e das comunicações telegráficas, refere-se não propriamente ao que constitua o objeto das comunicações, "ou seja, os registros ou o conteúdo dos relatos da comunicação considerados em si mesmos, mas à integridade do processo de

comunicação ou de relacionamento intersubjetivo". Observa-se, portanto, que se considerava a proteção voltada apenas ao processo de transmissão de informações, mas não aos dados em si mesmos considerados.

Por fim, insta realçar que somente o Ministro Ricardo Lewandowski demonstrou reprovação quanto ao envio dos dados apreendidos para a Receita Federal e a fiscalização do INSS. Assim, votou com o relator no recurso extraordinário, concedendo parcialmente a ordem no *habeas corpus* para que os dados não fossem utilizados por terceiros, salvo para fins específicos de processo criminal.

Nesta fase, o Supremo Tribunal Federal demonstrou, portanto, não considerar os dados objetos passíveis de proteção por si, mas somente a sua transmissão. Considera-se pertencente à esfera privativa esta última, a qual não seria passível de violação por terceiros estranhos à comunicação. Outrossim, não se problematizou questão referente ao compartilhamento de dados e ao uso específico que se poderia fazer deles, nem mesmo o impacto que esta conduta poderia causar à esfera de privacidade dos usuários do serviço, questões de extrema relevância no estágio atual da disciplina normativa.

Num passo seguinte, tem-se uma guinada na posição do Tribunal. Esta foi observada nos autos da ADI 6.387 MC-Ref/DF, na qual, em decisão paradigmática do plenário, chancelou-se provimento monocrático da ministra Rosa Weber para reconhecer a necessidade de proteção de dados como garantia do direito à privacidade, à autodeterminação informativa e ao livre desenvolvimento da personalidade. O teor do julgamento merece destacada atenção, uma vez que traz importantes reflexões e o posicionamento da Suprema Corte acerca dos limites de atuação do Estado para persecução de seus fins diante da necessidade de proteção de dados e informações pessoais dos administrados[4].

4. A Medida Provisória n° 954/2020, foi objeto, ainda, das ADIs n° 6388, 6389, 6390 e 6393, propostas, respectivamente, pelo Partido da Social

Tenha-se presente o caso:

> Foi proposta ADI pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB contra o inteiro teor da Medida Provisória (MP) n° 954, de 17 de abril de 2020, a qual dispunha sobre "*o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei n° 13.979, de 6 de fevereiro de 2020*".
>
> Para atendimento dos fins visados na norma, as empresas telefônicas deveriam disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, números de telefone e endereços dos consumidores, pessoas físicas ou jurídicas. Ressaltava a MP, outrossim, que o procedimento seria aplicado por prazo determinado – duração da situação de emergência de saúde pública decorrente do coronavírus, que os dados não seriam disponibilizados para quaisquer empresas públicas ou privadas ou a órgãos da administração pública de quaisquer entes federativos, bem como que seria realizado e divulgado relatório de impacto à proteção de dados pessoais nos termos preconizados pela LGPD e que, superada a situação de emergência de saúde pública, as informações seriam eliminadas das bases de dados da Fundação IBGE.

Apesar da demonstração de cuidado, por parte do Executivo quando da edição da Medida provisória, com algumas normas preconizadas pela LGPD acerca do tratamento adequado de dados, como realização de relatório de impacto, limitação do compartilhamento dos dados e sua eliminação após cessados os

---

Democracia Brasileira (PSDB), Partido Socialista Brasileiro (PSB), Partido Socialismo e Liberdade (PSOL) e Partido Comunista do Brasil (PCB).

motivos que justificaram a coleta no formato apresentado, a ministra relatora concedeu medida cautelar suspendendo a eficácia da Medida Provisória, o que foi confirmado pelo plenário do Tribunal.

Destacou a Ministra Rosa Weber a especial proteção que a Constituição da República conferiu à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade. Ademais, realçou que, a fim de instrumentalizar tais direitos, a Constituição previu, no artigo 5°, XII, a inviolabilidade do sigilo de dados, direitos que seriam malferidos caso as informações solicitadas fossem repassadas.

Ponto relevante, ainda, do voto, consiste na afirmação de que o respeito à privacidade e à autodeterminação informativa foram positivados no artigo 2°, I e II, da LGPD, como fundamentos específicos da disciplina de dados pessoais. Por fim, ressaltou a ausência de indicação precisa da finalidade da coleta das informações, a falta de mecanismo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, bem como o equívoco de se realizar relatório de impacto após o início da coleta e do tratamento dos dados.

Os fundamentos utilizados pela relatora foram acolhidos pelos demais ministros da Corte, ressalvado o voto divergente do ministro Marco Aurélio Mello, o qual negou referendo à medida cautelar concedida, entendendo hígida a Medida Provisória em referência. Ressaltou o Ministro a importância dos dados para a execução da política pública, bem como a confiabilidade a ser conferida ao Instituto Brasileiro de Geografia e Estatística.

Na votação do plenário, merecem destaque, ainda, os votos dos Ministros Luiz Fux e Gilmar Mendes, que pontuaram de forma enfática a necessidade de a Corte aprofundar a identificação, na ordem constitucional brasileira, de um autônomo direito à proteção de dados pessoais, a fim de se estabelecer o âmbito de

resguardo de direitos e os limites constitucionais à intervenção do Estado nessa esfera.

Dessa forma, ainda que não tenha constado expressamente na ementa do julgado, discutiu-se na ADI – com defesa expressa nos votos mencionados – a existência, no Brasil, de um implícito direito à proteção de dados pessoais, autônomo em relação ao direito à privacidade, mas consectário deste e do princípio da dignidade da pessoa humana.

Destaca-se, nesta oportunidade, trecho do voto do Ministro Gilmar Mendes, que expressa opinião relevante no presente estudo. Nos termos de sua manifestação, o direito fundamental à proteção de dados estaria lastreado em três bases fundamentais: (i) no direito fundamental à dignidade da pessoa humana; (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, X, da CF/88) diante dos novos riscos derivados do avanço tecnológico; e (iii) no reconhecimento da centralidade do *habeas data* enquanto instrumento de tutela material do direito à autodeterminação informativa.

Objetiva-se analisar neste trabalho os riscos decorrentes da coleta e tratamento de dados realizados para fins de segurança pública e de atividade de investigação e repressão de infrações penais, as quais não possuem delimitação precisa no ambiente normativo já elaborado no país. Relembra-se que a LGPD, no artigo 4º, inciso III, traz expressa exceção à aplicação do diploma, não havendo ainda sido produzido qualquer documento normativo que visa à regulação da proteção de dados nesse setor.

Diante do vácuo legislativo, faz-se mister o recurso às normas constitucionais e legais já existentes, que deverão guiar o Poder Público na atividade de coleta, tratamento, uso e compartilhamento de dados para fins de segurança e investigação penal. Ressalta, assim, a importância do destaque feito no voto do Ministro Gilmar Mendes à força normativa da Constituição, com a

necessidade de exercício de uma interpretação das normas constitucionais que lhes garanta uma concretização ótima, adaptando-a aos fatos concretos da vida.

Esta foi, pois, a evolução do tratamento jurisprudencial dado à privacidade e à proteção de dados no direito brasileiro, ao qual foi somada a promulgação da Emenda Constitucional n° 115, de 10 de fevereiro de 2022, e da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei n° 13.709, de 14 de agosto de 2018.

Além da Constituição e da LGPD, há proteção adicional à privacidade e aos dados em diversos outros diplomas legais do país, os quais, de maneira setorial, regularam a matéria. Entre estes: o Código de Defesa do Consumidor (Lei n° 8.078/90 – Seção VI – Dos Bancos de Dados e Cadastros de Consumidores); a Lei do Cadastro Positivo (disciplina a formação e consulta a bancos de dados com informações de adimplemento para formação de histórico de crédito); a Lei de Acesso à Informação (Lei n° 9.507/97); o Marco Civil Internet (Lei n° 12.965/2014).

A importância do conhecimento do arcabouço normativo relativo à proteção de dados é essencial para garantir proteção adequada aos direitos e liberdades individuais. Outrossim, merece destaque a determinação expressa no artigo 5º, §2º, da Constituição da República, que dispõe que direitos e garantias nela expressos não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais de que o Brasil faça parte. Fazem parte do bloco de constitucionalidade, contudo, apenas tratados e convenções internacionais sobre direitos humanos aprovados em regime equivalente ao de emendas constitucionais, nos termos do art. 5º, § 3º.

Visto o histórico estrangeiro e brasileiro da evolução do direito à privacidade e à proteção de dados pessoais, passa-se à análise específica do regime jurídico aplicado ao Poder Público no Brasil nesta seara.

3.2. ANÁLISE PRINCIPIOLÓGICA DA PROTEÇÃO DE DADOS NO SETOR PÚBLICO

A Lei Geral de Proteção de dados (LGPD), promulgada em 2018, tem como objetivo declarado regulamentar a atividade de tratamento de dados pessoais e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Observa-se, portanto, um grande direcionamento da lei para proteção do indivíduo em sua esfera privada.

No texto, são minudenciados os fundamentos da disciplina da proteção de dados, os princípios aplicáveis, as hipóteses em que o tratamento de informações é permitido, bem como regras específicas aplicadas ao setor público, entre outras.

Dentre as normas de realce, está aquela que veicula a base principiológica para tratamento de dados, a qual se direciona ao ambiente privado e ao público. Os princípios aplicados às atividades de tratamento estão descritos no artigo 6º, nomeadamente: I – finalidade; II – adequação; III – necessidade; IV – livre acesso; V – qualidade dos dados; VI – transparência; VII – segurança; VIII – prevenção; IX – não discriminação; e X – responsabilização e prestação de contas.

É preciso que se ressalte, nesta oportunidade, que o fato de existir na LGPD normas voltadas com objetivo confesso de realização de proteção de dados pessoais, com princípios e regras a esse fim destinados, não significa que a disciplina da matéria tenha estado em completo vácuo no período anterior à sua promulgação. A LGPD veio, em verdade, complementar um sistema esparso e difuso de proteção de dados pessoais expresso em leis nacionais anteriores, as quais, de forma pontual, veiculavam normas em certa medida absorvidas pela nova legislação.

Cuidaram da proteção de dados pessoais, em alguns termos, a Lei do *Habeas Data* (Lei nº 9.507/97), a Lei de Arquivos Públicos (Lei nº 8.159/91), o Código Civil (Lei nº 10.406/2002), o Código

de Defesa do Consumidor, (Lei nº 8.078/90) a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet (Lei nº 12.965/2014) – este último trazendo a proteção de dados pessoais como um princípio do uso da internet no Brasil. Os diplomas mencionados veicularam já princípios e regras de proteção de dados, direcionando, de alguma forma, os trabalhos que culminaram com a edição da Lei n º 13.709/2018.

No plano constitucional, já se observava a previsão do *habeas data* como instrumento legítimo para manejo de informações pessoais. Na lei que o disciplina (Lei n º 9.507/97), já se dispõe acerca do direito ao acesso a informações, assegurando o direito ao conhecimento, à retificação e ao esclarecimento, com prioridade de tramitação em caso de necessidade de uso de instrumento processual para proteção adequada do direito.

A Lei de Arquivos Públicos (Lei nº 8.159/91) igualmente prevê o direito a receber dos órgãos públicos informações, ressalvados os casos de sigilo, que, se violados, ensejarão responsabilização do agente infrator da norma.

Outro diploma relevante no tratamento da matéria foi o Marco Civil da Internet (Lei nº 12.965/2014), que, entre os itens de relevo, mencionou que a disciplina do uso da internet no país tem como princípios, entre outros, a proteção dos dados pessoais, na forma da lei (art. 3 º, III). Entre os direitos dos usuários, enumera a inviolabilidade da intimidade e da vida privada (art. 7º, I), bem como do fluxo de informações (art. 7º, II); informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, realçando a necessidade de justificativa da coleta (art. 7º, VIII), o que antecipa princípio exposto na LGPD.

Mais voltados para o ambiente privado, também merecem destaque o Código de Defesa do Consumidor – CDC (Lei nº 8.078/90) e o Código Civil (Lei nº 10.406/2002). No CDC, regras relativas a consentimento informado, transparência, segurança, acesso e direito a retificação de dados revelam tratamento

assemelhado ao posto na LGPD (veja-se seção "Dos Bancos de Dados e Cadastros de Consumidores). Bem assim, o Código Civil traz normas referentes à intimidade e vida privada com possibilidade de adoção de medidas que impeçam ou façam cessar possível lesão.

Essa pulverização do tratamento da proteção de dados incentivava a elaboração de um diploma que organizasse formalmente o sistema, o que culminou com a edição da LGPD, a qual absorveu em parte princípios e regras disciplinados no corpo formal exposto, sem prejuízo de inovações que aperfeiçoaram o sistema de proteção de dados no país, a exemplo da previsão de entidades responsáveis por zelar, implementar e fiscalizar o cumprimento das normas em todo o país. Assim, foram elencados e especificados no diploma os princípios que devem reger as atividades de tratamento de dados pessoais, assim expostos:

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

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Os princípios mencionados devem ser respeitados em todas as atividades que envolvem o gerenciamento de dados, sendo aplicáveis mesmo nas hipóteses em que a LGPD ressalva sua aplicação. Na norma do artigo 4º estão situações de exceção da aplicabilidade da Lei, entre as quais o tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. No §1º do dispositivo, porém, vê-se a expressa menção à aplicação dos princípios gerais da proteção de dados mesmo nos casos de segurança nacional e instrução penal, devendo, nessa hipótese, serem atendidos, ainda, o devido processo legal, os direitos do titular previstos na Lei e comedimento na adoção de medidas para atendimento do interesse público.

Destaca-se a enorme importância de proteção adequada por meio das normas postas, dado o potencial tecnológico na coleta, armazenamento, tratamento e análise de dados, que possibilita a empresas e governos elevado grau de perfilhamento e identificação de indivíduos em grupos sociais. Observado, ainda, o uso efetivo dessas informações para delineamento de estratégias e tomada de decisões, estas passíveis de interferência por vieses e inconsistências, essencial o arcabouço principiológico delineado na LGPD. A própria Lei, ao enumerá-los, define seu conteúdo, fixando limites de conduta e garantias dos indivíduos no processo de tratamento de dados pessoais.

Referidos princípios, que possuem grande foco no sujeito individual – mas não apenas – devem conviver e se harmonizar com outros que circundam a atuação do Poder Público, expostos na Constituição, em leis esparsas e na doutrina especializada. Nestes últimos, de maneira geral, ganham destaque aqueles que interessam à coletividade, em grande medida imperativos diante de interesses privados. Nesse contexto, surge a questão de como harmonizar, na seara pública, princípios que, ao menos de início, parecem caminhar em direções opostas.

Na Constituição, no capítulo que trata da administração pública, lê-se que esta obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência. A Lei nº9.784/99, que regula o processo administrativo no âmbito da União, indica outros tantos: finalidade, motivação, razoabilidade, proporcionalidade, interesse público.

Destes, percebe-se que alguns convergem de forma imediata para aqueles previstos na LGPD. O princípio da legalidade amolda-se com perfeição, vez que, na proteção de dados pessoais, cuida-se das bases legais que autorizam o tratamento no âmbito do Poder Público. O princípio da impessoalidade se avizinha ao da não-discriminação, o qual determina a impossibilidade de realização de tratamento de dados para fins discriminatórios ilícitos ou abusivos. A razoabilidade e a proporcionalidade aproximam-se