Edson Pires da Fonseca

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD

2021

EDITORA JusPODIVM
www.editorajuspodivm.com.br

5

TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

A LGPD permite o tratamento de dados pessoais de crianças e adolescentes desde que seja feito em seu **melhor interesse** e que receba, no caso das crianças, **consentimento inequívoco** de um de seus pais ou responsáveis. A **proteção integral** é um dos fundamentos do Estatuto da Criança e do Adolescente, lei especial que deve ser observada no tratamento de dados de criança ou adolescente. A própria LGDP menciona que o tratamento dos dados será feito considerando a legislação específica (art. 14).

De acordo com Pinheiro[1], "Os dados relacionados a menores de idade estão classificados em uma categoria de dados especiais (pois exigem um tratamento diferenciado em termos de cuidados)". Dessa maneira, a LGPD não proíbe que haja o tratamento de dados da criança e do adolescente, mas o condiciona ao atendimento do seu melhor interesse e, no caso das crianças, ao consentimento dos pais ou responsáveis.

Enquanto o tratamento de dados de adultos está lastreado em dez bases legais, o de **criança** está fundamentado no **consentimento** de ao menos um dos pais ou responsáveis. Portanto, a base legal que permite o tratamento de dados de criança é o **consentimento**, dado não pelo titular do direito, mas por um de seus pais ou representantes (art. 14, §1º)[2].

---

1. PINHEIRO, 2018, op. cit., p. 74.

2. Art. 14, §1º: "O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal".

Quanto ao **adolescente**, a LGPD não foi suficientemente clara. Como o artigo 14, §1º, trata especificamente da criança, parte da doutrina tem entendido que o tratamento de dados do adolescente pode ser feito com fundamento em qualquer uma das dez bases legais do artigo 7º da LGPD[3]. Contudo, se a necessidade de consentimento dos pais ou representantes se restringe às crianças, aos doze anos o adolescente pode consentir sobre o tratamento dos seus dados pessoais, sem a interveniência dos seus pais ou responsáveis, o que pode violar o seu melhor interesse, cuja proteção é uma exigência da própria LGPD, tanto para crianças quanto para adolescentes: "O tratamento de dados pessoais de crianças e de **adolescentes** deverá ser realizado em seu **melhor interesse**, nos termos deste artigo e da legislação pertinente"[4].

Paula Lopes adverte que "Tal fato, ao nosso ver, ocasiona uma desproteção dos adolescentes que, tal como as crianças, assim se tratam de pessoas em desenvolvimento e que, portanto, continuam vulneráveis. Questiona-se, até mesmo, se esses, de fato, possuem condições de observar com clareza o que estão consentindo e as consequências dessa escolha. Acreditamos que não"[5].

Trata-se de tema que merece a atenção da ANPD, que deve aclarar as bases legais nas quais o tratamento de dados do adolescente poderá se fundamentar, preservando o seu melhor interesse e a sua proteção integral[6].

Quando houver o tratamento de dados de criança ou adolescente, o controlador tornará "pública a informação sobre os tipos de dados

---

3. Maia e Yun asseveram que a previsão do consentimento prevista no artigo 14, §1º é exclusiva para crianças, "não fazendo qualquer referência aos dados pessoais dos adolescentes". Diante disso, as autoras entendem que as dez bases legais previstas no artigo dispostas na lei, incluindo o legítimo interesse, poderá ser adotada quando a atividade de tratamento envolver dados pessoais de adolescente". MAIA e YUN, 2020, op. cit., p. 200.

4. Artigo 14, *caput*, da LGPD (sem grifos no original).

5. LOPES, Paula Ferla. **Tratamento de dados pessoais de crianças e adolescentes na lgpd: primeiras impressões.** IBDFAM. Disponível em: https://www.ibdfam.org.br/artigos/1518/Tratamento+de+dados+pessoais+de+crian%C3%A7as+e+adolescentes+na+lgpd%3A+primeiras+impress%C3%B5es, acessado em 16 de setembro de 2020, às 18h.

6. Estatuto da Criança e do Adolescente, Artigo 1º: "Esta Lei dispõe sobre a proteção integral à criança e ao adolescente".

coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei" (art. 14, §2º).

Quando o tratamento de dados é pautado no consentimento do titular, a LGPD já obriga que o controlador demonstre que a autorização para o tratamento de seus dados foi inequívoca, porém no caso do consentimento dos pais ou responsáveis pela criança e pelo adolescente este cuidado deve ser ainda mais acentuado, para que possa assegurar, sem sombra de dúvidas, que foram os pais ou responsáveis que consentiram para o tratamento. De acordo com a LGPD, "O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis" (art. 14, § 5º).

A LGPD permite o tratamento de dados de criança sem o consentimento dos pais ou responsáveis apenas se isso for necessário para contatá-los ou para a proteção da criança. Cuida-se de **hipótese excepcional**, que poderá ser utilizada apenas **uma vez** e sem o armazenamento dos dados. Veda-se, ainda, o compartilhamento desses dados com terceiros, exceto se autorizado pelos pais ou responsáveis (art. 14, § 3º).

Os controladores não poderão condicionar a participação de crianças e adolescentes a jogos, aplicações da internet ou outras atividades "ao fornecimento de informações pessoais além das estritamente necessárias às atividades" (art. 14, § 4º). Nesse ponto, o legislador reforçou a necessidade de observância estrita do princípio da **necessidade**, que limita o tratamento de dados "ao mínimo necessário para a realização de suas finalidades" (art. 6º, II).

A LGPD assevera que as informações sobre o tratamento de dados de crianças e adolescentes devem ser fornecidas de maneira simples, clara e acessível, proporcionando as informações necessárias aos pais e responsáveis e adequadas ao entendimento da criança. Para isso, devem ser "consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado" (art. 14, §6º)[7].

7. Art. 14, § 6º: "As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso

O **GDPR** aborda o tratamento de dados das crianças e adolescentes no **Considerando nº 38[8] e no artigo 8º**. Uma diferença em relação à LGPD diz respeito à idade para que o adolescente possa consentir validamente, sem a necessidade de interveniência de seus pais ou responsáveis. Enquanto no Brasil isso só é possível a partir dos dezoito anos, na União Europeia o adolescente pode consentir a partir dos dezesseis anos. Ressalva-se a possibilidade de os Estados-Membros, em suas legislações locais, reduzirem essa idade para treze anos, mas nunca para menos do que isso (art. 8º, nº 1, GDPR).

---

de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

8. GDPR, Considerando nº 38: "As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança".

6

DIREITOS DO TITULAR DE DADOS PESSOAIS

O titular dos dados pessoais protegidos pela LGPD é a pessoa natural, o que exclui os falecidos e as pessoas jurídicas[1]. Assegura-se a toda pessoa natural a titularidade dos dados pessoais e os direitos fundamentais de liberdade, de intimidade e de privacidade (art. 17).

Garante-se ao titular dos dados o direito de obter do controlador, a qualquer tempo e mediante requisição, as seguintes medidas:

(i) confirmação da existência de tratamento;

(ii) acesso aos dados pessoais que estão sendo tratados;

(iii) correção de seus dados, em caso de completude, inexatidão ou desatualização;

(iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidades com a LGPD;

(v) portabilidade dos dados a outro fornecedor;

(vi) eliminação dos dados tratados, exceto nas hipóteses legais;

1. O GDPR é expresso quanto à sua inaplicabilidade aos dados de pessoas falecidas. A LGPD não trata do tema de maneira expressa, o que deixa margem para divergência. Considerando nº 27 – "O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas";

(vii) informação das entidades públicas ou privadas com as quais o controlador compartilhou os seus dados;

(viii) informações sobre o fornecimento de consentimento e as consequências de não consentir;

(ix) revogação do consentimento a qualquer tempo e por procedimento facilitado (art. 18 e incisos).

Em caso de **discordância** com o controlador, o titular dos dados pode **peticionar** contra ele perante a ANPD (art. 18, §1º) ou perante os órgãos de defesa do consumidor (art. 18, § 8º). Quando a base legal que fundamenta o tratamento de dados não for o consentimento, o titular tem o direito de opor-se a ele em caso de descumprimento do disposto na LGPD (art. 18, §2º).

Para exercer os direitos assegurados pela LGPD o titular dos dados pessoais encaminhará requerimento expresso aos agentes de tratamento, o que, em sua impossibilidade, poderá ser formulado por seu representante legal (art. 18, §3º). Se o controlador não puder adotar imediatamente a providência requerida pelo titular responderá:

(i) que não é o agente de tratamento;

(ii) apontar as razões de fato e de direito que o impedem de adotar a medida requerida pelo titular (art. 18, §4º).

A LGPD ressalta que o requerimento encaminhado aos agentes de tratamento para exercício dos direitos do titular previstos na Lei não terá custo para ele e será respondido nos prazos e termos previstos em regulamento próprio (art. 18, §5º).

Quando o controlador tiver compartilhado os dados do titular, deverá informar imediatamente os agentes de tratamento que receberam os dados para que adotem igual procedimento sobre a correção, a eliminação, a anonimização ou o bloqueio dos dados, exceto quando isso for impossível ou desproporcionalmente oneroso (art. 18, § 6º).

Anota-se que o direito de **portabilidade** dos dados pessoais não poderá ser exercido se os dados já tiverem sido anonimizados pelo controlador, pois, nesta hipótese, pela própria natureza da anonimização, os dados não podem mais ser identificados (art. 18, § 7º).

6.1 DIREITO DE REVISÃO DE DECISÕES AUTOMATIZADAS

Com o avanço da capacidade computacional, da inteligência artificial, do *Big Data* e dos algoritmos cada vez mais, em várias esferas da vida, as decisões são tomadas de maneira automatizada. Alguns algoritmos são tão sofisticados e complexos que compreender os seus processos decisórios é tarefa hercúlea.

O sistema bancário, por exemplo, em seu cotidiano operacional, avalia os dados financeiros das pessoas para estabelecer o risco de crédito de suas operações. Esses cálculos são feitos de maneira automatizada, por algoritmos, oferecendo rápido retorno à solicitação, porém, no mais das vezes, sem que o titular dos dados saiba como esse processo foi realizado e quais os parâmetros utilizados para sustentar a decisão. Dessa maneira, a automatização de alguns procedimentos pode trazer significativas contribuições, gerando agilidade e precisão nos processos decisórios, porém, se não usada com ética, pode gerar decisões enviesadas e discriminatórias.

Diante desse contexto, a LGPD assegurou ao titular o direito de revisão da decisão tomada unicamente com base em **processos automatizados** e que contrariem os seus interesses. Incluem-se decisões destinadas a definir o seu perfil pessoal, profissional, de crédito, de consumo ou que tratem de aspectos de sua personalidade (art. 20).

A LGPD estabelece que o controlador deverá fornecer informações claras e adequadas a respeito dos critérios e procedimentos utilizados para decisões automatizadas, resguardados os sigilos comercial e industrial (art. 20 § 1º). Se não houver um mecanismo adequado e ético de acompanhamento dos processos decisórios automatizados os algoritmos podem chegar a decisões discriminatórias. O esclarecimento de como os algoritmos chegaram a determinada conclusão é tarefa cada vez mais complexa, o que ensejará muitos desdobramentos a partir dos casos concretos que certamente surgirão.

Se o controlador alegar **segredo industrial e comercial** para não fornecer as informações sobre os processos decisórios automatizados a ANPD "poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais" (art. 20 § 2º).

Havia previsão de que a revisão das decisões automatizadas seria feita por **pessoa natural**, contudo o Presidente da República vetou esta medida e o veto foi mantido pelo Congresso Nacional. Argumentou-se que em alguns casos, com enormes fluxos de dados, a revisão da decisão por humanos seria impossível. Dessa maneira, embora assegurado o direito à revisão, ela pode ser feita de maneira automatizada.

O **GDPR** regulamenta as decisões automatizadas em seu **artigo 22**, que reconhece o direito do titular dos dados de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, desde que isso produza efeitos em sua esfera jurídica ou o afete significativamente. O Regulamento europeu prevê três exceções nas quais é possível o tratamento exclusivamente automatizado (GDPR, art. 22, nº 2):

(i) quando a decisão for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento (controlador);

(ii) for autorizada pelo direito da União Europeia ou dos Estados-Membros, desde que presentes medidas de salvaguarda dos direitos do titular;

(iii) for baseada no consentimento explícito do titular.

Nas hipóteses (i) e (iii) o GDPR é expresso ao afirmar que o controlador deve aplicar medidas adequadas para proteger os direitos, liberdades e legítimos interesses do titular dos dados, assegurando-lhe o direito de obtenção de intervenção humana, isto é, de ter a decisão automatizada revisada por humanos, de manifestar o seu ponto de vista sobre o assunto e de contestar a decisão (art. 22, nº 3).

O **Considerando nº 71** do GDPR traz importante contribuição para a temática das decisões automatizadas:

> O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito

> por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana[2].

Nesse particular, como visto, o veto à LGPD fez com que a abrangência da proteção na lei brasileira ficasse inferior à do Regulamento europeu, que manteve o direito à revisão por humanos.

As decisões automatizadas são um ponto sensível na política de proteção de dados e se não forem tratadas com extrema cautela e dentro de robustas balizas éticas podem perpetuar desigualdades e discriminações, tais quais as denunciadas por Eubanks, que demonstrou os perigos de decisões automatizadas e os seus impactos na acentuação das desigualdades sociais[3].

Para além disso, excluir dos seres humanos determinadas decisões, atribuindo-as exclusivamente às máquinas, pode, em futuro próximo, representar alguns perigos civilizatórios[4].

No âmbito do GDPR, o Grupo de Trabalho do Art. 29 (**WP Art. 29**), teceu orientações importantes sobre o uso de decisões automatizadas.

> Os sistemas de controlo de algoritmos e as revisões periódicas da exatidão e relevância das decisões automatizadas, incluindo a definição de perfis, são outras medidas úteis.
>
> Os responsáveis pelo tratamento devem introduzir medidas e procedimentos adequados para prevenir a ocorrência de erros, imprecisões ou a discriminação com base nos dados de categorias especiais.

---

2. As palavras estão grafadas em português de Portugal.

3. EUBANKS, Virginia. **Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor.** St Martin's Press, 2018.

4. Um caso emblemático de viés algoritmo que provocou intenso debate foi o ***Caso Eric L. Loomis***, que teve a sua *periculosidade* analisada pelo algoritmo ***COMPAS***, *Correctional Offender Management Profiling for Alternative Sanctions.* O COMPAS faz uma série de perguntas para estabelecer a probabilidade de reincidência. Ocorre que uma pesquisa feita pela organização independente destinada ao jornalismo investigativo ProPublica detectou que os negros têm 45% mais chance de receber uma pontuação alta do que um branco, mesmo não havendo pergunta específica sobre raça no questionário. Sobre o Caso Loomis conferir: https://www.bbc.com/portuguese/brasil-37677421, acessado em 31.05.2020; https://harvardlawreview.org/wp-content/uploads/2017/03/1530-1537_online.pdf, acessado em 31.05.2020.

> Estas medidas deverão ser utilizadas de modo cíclico, ou seja, não apenas na fase de conceção, mas também permanentemente enquanto for aplicada uma definição de perfis às pessoas. O resultado destas análises deverá ser refletido na conceção do sistema[5].

Embora seja inegável a importância dos algoritmos na atualidade, havendo quem defenda que o seu uso torna as decisões menos subjetivas do que as tomadas por seres humanos, combater o viés algorítmico é uma obrigação no Brasil, pois a não discriminação é um dos princípios da LGPD, que assenta a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (art. 6º, IX).

6.2 OUTROS DIREITOS DO TITULAR: A TUTELA COLETIVA DA PROTEÇÃO DOS DADOS PESSOAIS

Além dos direitos já mencionados, a LGPD assegura ao titular que "Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo" (art. 21).

A LGPD traz, ainda, importante questão processual na defesa dos direitos nela previstos, enfatizando "A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva". Dessa maneira, não resta dúvida de que além da tutela individual da proteção de dados a LGPD também trouxe expressamente a tutela coletiva dos direitos e garantias nela contidos.

Ao debruçar-se sobre a tutela coletiva da proteção de dados, Roque relembra a classificação trazida pelo Código de Defesa do Consumidor, CDC, que divide os direitos coletivos em três categorias: (i) direitos difusos; (ii) direitos coletivos em sentido estrito e (iii) direitos individuais homogêneos. Nas duas primeiras hipóteses,

5. GRUPO DE TRABALHO DO ARTIGO 29 PARA A PROTEÇÃO DE DADOS. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679.** WP 251rev. 01. Revisado em 6 de fevereiro de 2018. Grafia original, da tradução portuguesa.

trata-se da tutela de direitos coletivos (essencialmente coletivos), enquanto na última, dos direitos individuais homogêneos, trata-se de tutela coletiva de direitos acidentalmente coletivos (individuais homogêneos). O autor destaca que a definição da categoria de tutela coletiva à proteção de dados pessoais é importante em razão de o CDC estabelecer "regimes jurídicos distintos para cada uma delas"[6].

Roque esclarece que é um equívoco atribuir *a priori* a categoria de direitos coletivos a alguma matéria em abstrato, como a tutela dos dados pessoais, pois algumas nuances do caso concreto podem fazer incidir uma espécie ou outra de direito coletivo. Para Roque, a tutela coletiva dos dados pessoais pode envolver:

> direitos difusos (por exemplo, no caso em que se pretende corrigir algum tratamento inadequado de dados pessoais realizado por autoridades públicas, relativamente a todos os que vivem em certa localidade – tutela indivisível e sem que exista uma relação jurídica base prévia que delimite o grupo), coletivos em sentido estrito (ilustrativamente, na hipótese em que se pede a adequação do tratamento de dados pessoais realizado por uma empresa, relativamente a seus consumidores – tutela também indivisível, mas referente a uma relação jurídica de consumo base) e individuais homogêneos (por exemplo, pleito de danos morais e materiais veiculado contra certa empresa decorrente do vazamento de dados de um grupo de pessoas – tutela que poderia ser postulada em ações individuais, existindo uma origem comum para os danos alegados)[7].

Roque assevera que "a categorização de um direito coletivo, portanto, dependerá invariavelmente da análise da causa de pedir e do pedido de tutela jurisdicional concretamente formulado". Para identificar qual categoria de direito coletivo incide em cada caso, Roque acentua que devem ser respondidas duas perguntas:

---

6. ROQUE, André. **A Tutela Coletiva dos Dados Pessoais na Lei Geral de Proteção de Dados.** *In* Revista Eletrônica de Direito Processual – REDP. Rio de Janeiro. Ano 13. Volume 20. Número 2. Maio a Agosto de 2019. Periódico Quadrimestral da Pós-Graduação Stricto Sensu em Direito Processual da UERJ, (p. 1-19), p. 8 e 9.

7. ROQUE, 2019, op. cit., p. 10.

(i) a tutela é divisível, isto é, "passível de cisão em processos individuais, sem repercutir necessariamente na esfera jurídica de outros titulares"? Se a resposta for positiva, está-se diante de direitos individuais homogêneos; caso a resposta seja negativa, deve ser feita uma segunda pergunta:

(ii) "sendo a tutela indivisível, existe alguma relação jurídica base responsável pela conformação do grupo"? Se a resposta for positiva, estará configurada a presença do direito coletivo em sentido estrito, se for negativa, ou seja, se a formação do grupo estiver baseada em meras circunstâncias fáticas, estará presente o direito difuso[8].

Concluindo a análise da tutela coletiva da proteção dos dados pessoais, indaga-se quem seriam os legitimados para a propositura das respectivas ações. Como a LGPD não fez menção, deve-se utilizar as duas **principais fontes do processo coletivo**: a Lei da Ação Civil Pública, Lei 7.347/1985 (art. 5º), e o CDC (art. 82).

Em síntese, são legitimados o Ministério Público, a Defensoria Pública, quando houver hipossuficientes, a Administração Pública, aqui incluindo a ANPD, e as associações civis, nos termos da legislação de regência. Quanto ao indivíduo, Roque destaca que ele só é legitimado para Ação Popular, embora, pelas peculiaridades que revestem esta ação, seja muito difícil imaginar hipótese na qual ela seria cabível. De qualquer modo, Roque vislumbra uma possibilidade remota de legitimidade do indivíduo para deflagração de ações coletivas, quando, no município em que residir, não existirem outros legitimados e a violação for perpetrada pela Administração Pública[9].

8. ROQUE, 2019, op. cit., p. 10 e p. 11.

9. ROQUE, 2019, op. cit., p. 12 e 13.

7

TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

A LGPD não se limitou a regular o tratamento de dados realizado pela iniciativa privada, incumbindo-se, também, do Poder Público. Em vez de elencar sobre quais entes públicos incidiria, a LGPD se valeu do rol trazido pela Lei de Acesso à Informação (Lei 12.527/2011, art. 1º, parágrafo único):

> Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir 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.
>
> 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.

O Estado é o principal controlador de dados pessoais, dispondo de informações sobre a saúde, educação, trabalho e finanças das pessoas. Por esse motivo, andou bem a LGPD ao incluir as pessoas jurídicas de direito público na sua esfera de abrangência. De acordo com Rosso:

> Dentre todos os concentradores de dados pessoais o Estado se sobressai, afinal de contas é ele que controla ainda que indiretamente a vida financeira, o acesso à saúde, eventuais processos judiciais colecionados durante a vida, dados educacionais, dados trabalhistas do cidadão entre outros. Além disso, o Estado é também um empregador gigante, são milhares de pessoas que vendem sua força de trabalho para os entes municipais, estaduais e federais da Administração Direta e Indireta. Mais do que isso, o governo é também o maior acionista de grandes empresas de tecnologia que a pedido dele operam com esses dados: os coletam, armazenam, utilizam, etc. Ou seja, deixar o setor público fora do alcance da LGPD seria um verdadeiro atentado aos direitos fundamentais[1].

O artigo 23 da LGPD estabelece que o tratamento de dados realizado pelas pessoas jurídicas de direito público atenderá a sua "**finalidade pública**, a persecução do **interesse público**, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (grifo nosso). Cots e Oliveira, ao tratarem desse tema, afirmam que o primeiro pressuposto depende do segundo, pois a finalidade somente é pública se o interesse também for público. Para os autores, "ao condicionar o tratamento de dados à perseguição de finalidades e interesses públicos, o legislador está vedando o referido tratamento em atendimento de interesses privados ou particulares"[2].

Para realizar o tratamento de dados as pessoas jurídicas de direito público devem informar as hipóteses nas quais, no exercício da sua competência, realizam o tratamento de dados. Devem informar, de modo claro e atualizado, qual a base legal que autoriza o tratamento de dados, a sua finalidade e quais os procedimentos e práticas utilizados para isso. O tratamento de dados, para que seja legal, deve estar dentro da competência e atribuição legal do órgão

---

1. ROSSO, Angela Maria. **LGPD e Setor Público: aspectos gerais e desafios.** Disponível em: https://www.migalhas.com.br/dePeso/16,MI300585,31047-LGPD+e+setor+publico+aspectos+gerais+e+desafios, acessado em 19.01.2020, às 13h41min.

2. COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais.** 3ª ed. São Paulo: Editora Revista dos Tribunais, 2019, p. 144 e 145.

público. Essas informações devem ser veiculadas em canais de fácil acesso, preferencialmente em suas páginas eletrônicas (art. 23, I).

Cots e Oliveira acentuam que a Administração Pública **possui base legal específica** para tratamento de dados (art. 7º, III, da LGPD), "não dependendo de consentimento ou enquadramento em outras hipóteses, exceto se mais específica, como é o caso da tutela da saúde".[3]

A LGPD estabelece que as pessoas jurídicas de direito público, quando realizarem tratamento de dados, devem indicar um **encarregado** (art. 23, III). Dessa maneira, não resta dúvida que as pessoas jurídicas de direito público **deverão indicar um Encarregado de Proteção de Dados**, um DPO, que fará a ponte entre o controlador, os titulares dos dados e a ANPD, além de ser fundamental na promoção da cultura de proteção de dados, sensibilizando os servidores, indicando e acompanhando a execução de medidas protetivas dos dados pessoais, traçando mecanismos e procedimentos que assegurem a conformidade das ações dos órgãos públicos com o previsto na LGPD e em todo o arcabouço de proteção de dados, sempre à luz dos contornos normativos que delineiam as instituições públicas.

A Lei Geral de Proteção de Dados ressalva que a ANPD poderá dispor sobre as formas de publicidade das operações de tratamento de dados (art. 23, §1º). Esclarece, ainda, que a sua vigência não afasta a incidência de outras normas, como a Lei de Acesso à Informação (Lei 12.527/2011).

No que tange aos prazos e procedimentos para exercício dos direitos do titular dos dados, a LGPD estabelece que devem ser observados os das legislações específicas, em especial a Lei do *Habeas Data* (Lei 9.507/1997), Lei do Processo Administrativo (Lei 9.784/1999) e Lei de Acesso à Informação (Lei 12.527/2011)[4].

Os **serviços notariais e de registro**, embora exercidos em caráter privado, são delegações do Poder Público, incidindo sobre eles o disposto para o Poder Público (art. 23, § 4º).

3. COTS e OLIVEIRA, 2019, op. cit., p. 145.

4. LGPD, art. 23, § 4º.

7.1 TRATAMENTO DE DADOS POR EMPRESAS PÚBLICAS E SOCIEDADES DE ECONOMIA MISTA

As empresas públicas e sociedades de economia mista atuam de maneira ambivalente. Quando atuam em regime de concorrência, são regidas pelas mesmas regras que regem as empresas privadas (art. 173 da CF/88)[5]; por sua vez, "quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público" (art. 24, par. único, LGPD).

7.2 INTEROPERABILIDADE E COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO

Entende-se por interoperabilidade a capacidade de dois sistemas de se interconectarem, de trocarem informações entre si. Esse conceito é muito importante no âmbito da LGPD, seja porque, como será tratado neste tópico, os sistemas do Poder Público devem ser interoperáveis para facilitar o compartilhamento de dados e informações, seja porque, com o direito de portabilidade de dados de que goza o titular, a interoperabilidade será muito

5. Art. 173. Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei. § 1º A lei estabelecerá o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias que explorem atividade econômica de produção ou comercialização de bens ou de prestação de serviços, dispondo sobre: I – sua função social e formas de fiscalização pelo Estado e pela sociedade; II – a sujeição ao regime jurídico próprio das empresas privadas, inclusive quanto aos direitos e obrigações civis, comerciais, trabalhistas e tributários; III – licitação e contratação de obras, serviços, compras e alienações, observados os princípios da administração pública; IV – a constituição e o funcionamento dos conselhos de administração e fiscal, com a participação de acionistas minoritários; V – os mandatos, a avaliação de desempenho e a responsabilidade dos administradores. § 2º As empresas públicas e as sociedades de economia mista não poderão gozar de privilégios fiscais não extensivos às do setor privado. § 3º A lei regulamentará as relações da empresa pública com o Estado e a sociedade. § 4º – lei reprimirá o abuso do poder econômico que vise à dominação dos mercados, à eliminação da concorrência e ao aumento arbitrário dos lucros. § 5º A lei, sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica, estabelecerá a responsabilidade desta, sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular.

importante para que os dados que estavam sendo tratados por um controlador possam ser transferidos para outro controlador, atendendo direito do titular.

A **interoperabilidade** dos sistemas aumenta a segurança dos dados, evitando, por exemplo, que a descontinuidade de um banco de dados torne inacessíveis os dados nele contidos.

A LGPD estabelece que os dados devem ser mantidos "em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral" (art. 25). Se cada órgão público utiliza um sistema diferente, que não se comunica com o de outro órgão, o uso compartilhado dos dados fica inviabilizado. Fundamental, portanto, que haja esse cuidado com a interoperabilidade dos bancos de dados, proporcionando maior eficiência e segurança ao tratamento de dados realizado pelo Poder Público.

Quanto ao compartilhamento de dados pelo Poder Público, a LGPD determina que ele "deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei". Veda-se, expressamente, o compartilhamento de dados com entidades privadas, ressalvadas as hipóteses que a própria Lei autoriza, quais sejam (art. 26):

- **(i)** "em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)";
- **(ii)** Quando os dados forem acessíveis publicamente, respeitadas as disposições presentes na Lei;
- **(iii)** "Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres". Destaca-se que a existência desses contratos ou convênios deve ser comunicada à ANPD (art. 26, §2º);

(iv) Para prevenir fraudes e irregularidades ou proteger a segurança e a integridade do titular, sendo expressamente proibida a utilização para outras finalidades.

Ressalta-se que a ANPD deve ser informada do uso compartilhado ou da comunicação de dados de pessoa jurídica de direito público para pessoa de direito privado, exceto nas seguintes hipóteses (art. 27):

(i) Quando a LGPD dispensa expressamente o consentimento;

(ii) "Nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei" (art. 27, II);

(iii) "nas exceções constantes do § 1º do art. 26 desta Lei" (art. 27, III).

Destaca-se que a ANPD poderá solicitar ao Poder Público, a qualquer tempo, "a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei" (art. 29 da LGPD).

A ANPD também poderá, no uso de seu poder normativo, estabelecer normas complementares para disciplinar "as atividades de comunicação e de uso compartilhado de dados pessoais" (art. 30). Cots e Oliveira enaltecem essa previsão normativa, argumentando que ela dará maior dinamismo "para o tratamento de questões que serão levantadas durante a adaptação da sociedade à nova lei, impedindo que a sociedade tenha que aguardar em cenário de frequente insegurança jurídica até que a lei seja adaptada, complementada ou corrigida". Os autores destacam que à luz do disposto no mencionado artigo 30, a ANPD "poderá emitir regulamentos complementares apenas no caso de comunicação e uso compartilhado de dados, não alcançando outras modalidades de tratamento"[6].

6. COTS e OLIVEIRA, 2019, op. cit., p. 157.

7.3 RESPONSABILIDADE DO PODER PÚBLICO NO TRATAMENTO DE DADOS

O Poder Público tem atuação de destaque no tratamento de dados pessoais, razão pela qual foi acertada a incidência da LGPD sobre ele, com alguns ajustes necessários à condição jurídica especial que caracteriza muitas pessoas jurídicas de direito público.

A abrangência e capilaridade da atuação do Poder Público o coloca em posição de potencial violador de dados caso os ditames previstos na LGPD não sejam fielmente cumpridos, podendo causar sérios danos aos direitos do titular, pela amplitude dos dados tratados e, ainda, pela dificuldade de tratamento homogêneo e regular em todos os órgãos públicos, inclusive em razão dos contrastes existentes entre as diferentes regiões do Brasil.

O artigo 31 da LGPD, trata da responsabilidade do Poder Público no tratamento de dados pessoais, estabelecendo que "Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação".

Embora o presente título fale em responsabilidade, o artigo parece direcionar a ANPD para uma postura mais educativa, estabelecendo que ela poderá enviar informe orientando o órgão público acerca das medidas que ele pode adotar para cessar a violação à LGPD.

Cots e Oliveira afirmam que esse dispositivo só tratou das atribuições da ANPD, quando deveria ter se aprofundado na responsabilidade do Poder Público por violação à LGPD, inclusive nas esferas criminal e civil. Os autores destacam que fazer cessar a violação à LGPD, como está descrito no artigo, é diferente de punir os responsáveis pelo tratamento ilícito de dados [7]. Também asseveram que o artigo 31 não faz menção direta de vinculação às sanções administrativas previstas no artigo 52 da LGPD, o que não significa que estas sanções não se apliquem ao Poder Público. De acordo com Cots e Oliveira, "O expediente parece ter por base a

7. COTS e OLIVEIRA, 2019, op. cit., p. 158.

boa-fé das ações governamentais e no interesse dos gestores públicos em corrigir procedimentos que violem a LGPD"[8].

7.3.1 A publicação de relatório de impactos à proteção de dados pelo Poder Público e adoção de padrões e boas práticas

O artigo 32 da LGPD estabelece que a Autoridade Nacional de Proteção de Dados **poderá solicitar** a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados. Diante disso, surge a dúvida acerca da obrigatoriedade de elaboração do RIPD, pois se a ANPD poderá solicitá-lo, pode se entender que ele já deva estar pronto.

A **doutrina diverge** sobre esse assunto, o que demandará esclarecimentos da ANPD. Cots e Oliveira defendem que "os entes públicos são obrigados à elaboração do referido relatório, ainda que não o torne público, aguardando deliberação da autoridade". Para eles, "se a autoridade nacional pode pedir a sua publicação é porque ele existe. Diferente seria se a autoridade pudesse exigir a elaboração, o que são coisas diferentes"[9].

Tasso, por sua vez, entende que "a interpretação sistemática da LGPD resulta na mera facultatividade de elaborar o RIPDP, imposta ao Poder Público". De acordo com ele, a obrigatoriedade de elaboração do relatório "não se coaduna com o regime jurídico administrativo, pois conquanto esteja alinhado com a maior transparência que se demanda do Poder Público como forma de equilibrar a assimetria de poder, não comunga do conceito de legalidade segundo o qual a administração pública deve agir *secundum legem*".

A manifestação da ANPD dará maior segurança jurídica aos agentes públicos, afastando as divergências sobre o tema. Diante da quantidade de dados tratados pelo Poder Público e da principiologia que rege a LGPD, se o tratamento de dados gerar riscos às liberdades civis e aos direitos do titular parece mais adequado que

8. COTS e OLIVEIRA, 2019, op. cit., p. 158.

9. COTS e OLIVEIRA, 2019, op. cit., p. 159.

o RIPD seja elaborado previamente. Embora um comando expresso trouxesse maior segurança jurídica, a interpretação favorável à elaboração prévia não parece transcender os limites do princípio da legalidade, que rege os atos da Administração Pública, ao mesmo tempo que atende aos princípios da eficiência e da publicidade, isto sem falar na maior proteção aos diretos fundamentais dos titulares, que estarão mais protegidos se o Poder Público, principal controlador de dados pessoais, tiver a clareza dos processos de tratamento sob sua responsabilidade, o que será proporcionado pela elaboração do Relatório de Impacto à Proteção dos Dados Pessoais.

Como salientado em outras partes da obra, a doutrina diverge sobre a necessidade de elaboração prévia do RIPD, o que reforça a importância de manifestação da ANPD esclarecendo as hipóteses nas quais o Relatório deve ser elaborado previamente, proporcionando maior segurança jurídica aos agentes de tratamento, em especial aos controladores.

Quanto à **sugestão** de boas práticas de tratamento de dados feita pela ANPD, entende-se que o acatamento não será obrigatório, eis que se trata de sugestão e não de determinação. Todavia, se o Poder Público não acatar as sugestões de boas práticas feitas pela ANPD deverá fundamentar adequadamente o motivo, pois a **eficiência** é um dos princípios da Administração Pública. Caso os agentes públicos, sem justo motivo, não acatem as sugestões da ANPD e disso resulte algum incidente, podem ter a responsabilidade agravada, porquanto houve alerta expresso da Autoridade Nacional de Proteção de Dados sobre os riscos e os caminhos para a superação dos vícios, mas foram ignorados, conscientemente, pelo controlador.