Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito

Renato Opice Blum[1]
Advogado

Nuria López[2]
Advogada

Sumário: 1. A construção normativa da proteção de dados no setor público; 2. A nova Lei Geral de Proteção de Dados; 3. Bases legais para o tratamento de dados pessoais; 4. Transparência e fortalecimento das relações democráticas; 5. Novos direitos; 6. Indicação de encarregado pelo tratamento de dados pessoais e outras obrigações; 7. Sanções; Conclusão; Referências.

Resumo: Trata-se da necessária análise dogmática da aplicação ao setor público da nova Lei Geral de Proteção de Dados dentro do contexto de desenvolvimento democrático. A partir da matriz de responsabilidade constitucional, pôde-se traçar uma trajetória crescente de transparência positiva do Poder Público em relação aos dados dos cidadãos, notadamente com a Lei do *Habeas Data* e a Lei de Acesso à Informação. As prestações decorrentes da Lei Geral de Proteção de Dados analisadas somam-se àquelas que as precedem, em uma perspectiva de fortalecimento cada vez maior das relações democráticas de Direito.

Palavras-chave: Lei Geral de Proteção de Dados. Setor Público. Lei de Acesso à Informação.

1. A construção normativa da proteção de dados no setor público

Há um ano da vigência da Lei Geral de Proteção de Dados, a iniciativa privada está tomada por projetos de adequação, palestras, cursos e ferramentas de segurança. Nem poderia ser diferente. No Brasil, apesar de termos trazido nossa matriz normativa do Regulamento Geral sobre Proteção de Dados europeu, desenvolvemos o conteúdo semântico de proteção de dados atrelado fortemente ao direito do consumidor. Muitos dos direitos dos titulares de dados, previstos no artigo 18, Lei Geral de Proteção de Dados, já estavam contidos no Código de Defesa do Consumidor; o nosso precedente explícito sobre acesso

[1] Mestre pela Florida Christian University; Advogado; Economista; Professor coordenador dos cursos de Proteção de Dados e Direito Digital do Insper e do curso Direito 4.0 da Faap; Juiz do Inclusive Innovation Challenge do MIT (Massachusetts Institute of Technology); Presidente da Associação Brasileira de Proteção de Dados (ABPDados); Diretor da Technology Law Association. @renatoopicelum

[2] Doutora em Teoria e Filosofia do Direito pela PUC-SP. Advogada em Direito Digital e DPO no Opice Blum, Bruno, Abrusio, Vainzof Advogados Associados. Professora convidada no Insper, Faap e FGV.

a dados em decisão automatizada é também nessa seara, no caso do *score* de crédito; e todos os casos levantados pelo Ministério Público (alguns, inclusive, judicializados) até o momento referem-se ao direito do consumidor. De fato, trata-se de um viés presente em todo o continente, desde o California Consumer Privacy Act (CCPA) nos Estados Unidos até o serviço No Llame, na Argentina.

O volume do esperado debate na iniciativa privada abafa uma narrativa mais discreta, mas crucial: o desenvolvimento da proteção de dados no Poder Público. Para os europeus, em particular os alemães, trata-se da principal linha de desenvolvimento da proteção de dados. Desde a Lei de Proteção de Dados de Hesse (*Hessisches Datenschutzgesetz*) em 1970, e de forma muito incipiente, o intuito era evitar quaisquer excessos no uso de dados pessoais pelo Poder Público. As leis que vieram posteriormente delimitariam, cada vez mais, um espaço de liberdade individual. É o fundamento da *autodeterminação informativa ou informacional*, que chegou à nossa Lei Geral de Proteção de Dados (art. 2º, II), vinda de um conhecido julgado da Corte Constitucional alemã[3], que garante a extensão do direito geral de personalidade aos dados pessoais, para que o indivíduo possa se determinar sobre eles. A Diretiva 95/46/EC, que antecedeu o Regulamento Geral (GDPR), no mesmo sentido, estabelecia como objetivo "a proteção das liberdades e dos direitos fundamentais das pessoas singulares, notadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais" (artigo 1º, 1). O Regulamento estabelece a relação explicitamente ao colocar que "defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais" (artigo 1º, 2).

A Europa deu, pouco a pouco, o salto de declarar o direito à privacidade como direito humano (artigo 12, Declaração Universal dos Direitos Humanos[4]), em 1948, para considerar a proteção dos dados pessoais a partir dos anos 1970. No Brasil, foi o recente período democrático a inaugurar a previsão legal de inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação (artigo 5º, X, Constituição). O salto para a proteção de dados ainda está por vir, na Proposta de Emenda à Constituição nº 17/2019, que "inclui a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar a matéria"[5]. Ensejada especialmente pelo pragmatismo de evitar a profusão de leis estaduais e municipais, que já estavam sendo aprovadas país afora, e concentrar a proteção de dados como tema da União, a proposta tem um significado mais profundo em termos de desenvolvimento democrático.

É também a redação constituinte que traz o *habeas data* 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 ou para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo" (artigo 5º, LXXII). A Lei viria apenas em 1997 (Lei do *Habeas Data* – Lei nº 9.507/1997), incluindo ainda a possibilidade de "anotação, nos assentamentos do interessado,

[3] Inteiro teor da decisão disponível em: https://bit.ly/36e9uO6. Acesso em: 20 jan. 2020.

[4] "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

[5] Disponível em: https://bit.ly/2G6BQiG. Acesso em: 20 jan. 2020.

de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável" (artigo 7º, III).

Os dados pessoais vêm, em 2011, protegidos, como exceção à transparência intrínseca às democracias, na Lei de Acesso à Informação (Lei nº 12.527/2011). Ela chega a definir "informação pessoal" nos mesmos termos que definimos hoje com a Lei Geral de Proteção de Dados, "dados pessoais", "aquela relacionada à pessoa natural identificada ou identificável" (artigo 4º, Lei de Acesso à Informação). Sem prejuízo de notarmos a distinção entre *dado* e a *informação* que dele pode ser extraída, é digno de nota a introdução normativa do conceito.

Há, além disso, a responsabilização do Poder Público, que retira sua validade da matriz estabelecida pelo artigo 37, 6º, Constituição. A Lei de Acesso à Informação replica a regra constitucional ao estabelecer que "os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso" (artigo 34, *caput*, Lei de Acesso à Informação).

Na Lei de Acesso à Informação incumbe ao Poder Público a proteção da informação pessoal, "observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso" (artigo 6º, III, Lei de Acesso à Informação). A proteção à informação pessoal garante acesso restrito a agentes públicos legalmente autorizados e à **pessoa a quem as informações se referirem**, independentemente da classificação de sigilo, sendo que terceiros poderão ter acesso autorizado pela lei ou em razão de consentimento expresso do titular dos dados (artigo 31, §1º, Lei de Acesso à Informação). O consentimento só é dispensado em caso de prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusiva para o tratamento médico; em caso de realização de estatísticas e pesquisas científicas de evidente interesse público ou geral previstos em lei, sendo vedada a identificação da pessoa titular das informações; de cumprimento de ordem judicial; de defesa de direitos humanos ou de proteção do interesse público e geral preponderante (artigo 31, §3º, Lei de Acesso à Informação).

Ela ainda caracteriza como condutas ilícitas divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido a informação sigilosa ou informação pessoal ou impor sigilo a informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem (artigo 32, IV e V, Lei de Acesso à Informação).

2. A nova Lei Geral de Proteção de Dados

É nesse contexto que chega a nova Lei Geral de Proteção de Dados — como uma nova etapa da relação entre o Poder Público e o cidadão. Tanto que mesmo em casos de aparente não incidência da Lei, ela exige determinados requisitos (portanto, claro, incide). É o caso do artigo 4º, III, Lei Geral de Proteção de Dados, que estabelece que a Lei "não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais", para logo em seguida, em seu parágrafo terceiro, afirmar que a Autoridade Nacional emitirá opiniões técnicas ou recomendações sobre essas exceções e poderá solicitar relatório de impacto à proteção de dados pessoais (artigo 4º, §3º, Lei Geral de Proteção de Dados).

Apesar do paradoxo, a cautela é justificada. Trata-se de relatório descritivo das atividades de tratamento de dados pessoais que podem gerar risco às liberdades civis e aos direitos fundamentais, e das medidas, salvaguardas e mecanismos para mitigação de riscos (na definição legal do artigo 5º, XVII, Lei Geral de Proteção de Dados, e previsto no artigo 38, parágrafo único), importante para realizar uma ponderação sobre a utilização de dados pessoais, notadamente em casos de tecnologias de grande entropia, seus ganhos sociais e seus impactos nas liberdades individuais, com vistas a mitigá-los tanto quanto possível.

O que a Lei Geral de Proteção de Dados aponta ao determinar que "não se aplica" para essas finalidades, não é exatamente sua não incidência, senão incorreria nesse evidente paradoxo, mas sim que não se aplicam todas as suas disposições. Talvez a mais importante delas seja a não fundamentação dessas hipóteses de tratamento de dados em uma das bases legais previstas na Lei. Um dos principais pontos da Lei Geral de Proteção de Dados é a exigência de fundamentar cada atividade de tratamento de dados pessoais em uma base legal autorizadora do tratamento (nos termos do artigo 7º, *caput*, "o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses").

3. Bases legais para o tratamento de dados pessoais

Para as demais hipóteses de atuação do Poder Público, um primeiro ponto é o de saber qual a base legal (fundamento de legalidade) para tratar dados pessoais. Se os artigos 6º, III, e 31, §1º, Lei de Acesso à Informação, estabelecem que, em regra, há necessidade de previsão legal ou consentimento do titular dos dados (a quem o dado se refere), a Lei Geral de Proteção de Dados acrescenta cores a essa disposição.

Evidentemente, em razão do princípio da legalidade (artigo 37, *caput*, Constituição), qualquer órgão do Poder Público acaba por sempre estar amparado em uma disposição legal em suas ações, incluindo a de tratar dados pessoais. O artigo 23, *caput*, Lei Geral de Proteção de Dados, afirma precisamente que todo tratamento de dados pessoais pelo Poder Público "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". É dizer, sempre haverá, no caso do Poder Público, alguma norma legal que fundamente, em algum nível, o tratamento de dados pessoais. Todavia, isso não significa dizer que todo tratamento de dados pelo Poder Público será em *cumprimento de obrigação legal ou regulatória* (artigo 7º, II, Lei Geral de Proteção de Dados). A depender do caso, as demais bases legais poderão ser utilizadas também.

Por exemplo, o artigo 7º, III, Lei Geral de Proteção de Dados, criou uma base legal, não para todo Poder Público, mas especificamente para a 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". Uma interpretação restritiva da expressão "Administração Pública" leva à compreensão de que apenas o Poder Executivo pode utilizar essa base legal. Contudo, há que se notar que a expressão "Administração Pública" tomada em sentido lato autoriza qualquer órgão do Poder Público na execução de políticas públicas a encontrar fundamento legal no artigo 7º, III, Lei Geral de Proteção de Dados. De certo, coaduna-se melhor com a complexidade do Poder Público que cada vez mais atua sob a ótica de suas funções públicas, independentemente de estar inserido no Executivo, Legislativo ou Judiciário.

Sem dúvidas, as demais hipóteses de bases legais são também possíveis para o Poder Público, em casos mais pontuais: a realização de estudos por órgãos de pesquisa, sendo estes sem fins lucrativos (artigo 7º, IV); contrato ou diligência contratual de que é parte um titular de dados pessoais (artigo 7º, V); exercício regular de direitos em processos judicial, administrativo ou arbitral (artigo 7º, VI); proteção da vida ou da incolumidade física de terceiros (artigo 7º, VII); tutela da saúde (artigo 7º, VIII); interesse legítimo do controlador ou de terceiro (artigo 7º, IX) ou mesmo proteção ao crédito (artigo 7º, X).

Na iniciativa privada, de acordo com levantamento realizado em agosto de 2019, 33% das atividades de tratamento de dados pessoais encontram fundamento no legítimo interesse, 32% em execução de contrato, 18% em cumprimento de obrigação legal ou regulatória e 8% no consentimento do titular[6]. Evidentemente, pode-se esperar que a distribuição de bases legais seja diferente no Poder Público, privilegiando, por exemplo, o cumprimento de obrigação legal ou regulatória e a execução de políticas públicas.

4. Transparência e fortalecimento das relações democráticas

Em quaisquer das bases legais utilizadas, é necessário observar: os princípios da proteção de dados (artigo 6º, Lei Geral de Proteção de Dados), como o de minimização dos dados, é dizer, tratar apenas os dados necessários e adequados para a finalidade pretendida; garantia de livre acesso aos titulares dos dados; a qualidade dos dados, isto é, a exatidão, clareza, relevância e atualização; transparência, garantia de informações claras sobre o tratamento, precisas e facilmente acessíveis; segurança e prevenção, que em matéria de dados devem ser lidos conjuntamente; não discriminação; e responsabilização e prestação de contas sobre as atividades. Nessa perspectiva, tem destaque o princípio da transparência para o titular dos dados, sem a qual não é possível que ele exerça a autodeterminação informativa. A GDPR, vale a menção, ainda coaduna a transparência com o princípio da lealdade com o titular de dados. A lealdade não veio expressamente para a Lei Geral de Proteção de Dados, mas representa bem o passo que a nossa lei dá no tratamento de dados pessoais.

No Poder Público, transparência ganha uma dimensão nova, de fortalecimento das relações democráticas com os cidadãos. Se em uma sociedade de informação, como a nossa, *saber é poder*, a transparência sobre os dados pessoais sobre os quais se sabe implica o compartilhamento do poder detido, haja vista que comprova pela clareza a legalidade de suas ações. Por essa razão, o artigo 23, I, Lei Geral de Proteção de Dados, estabelece critérios específicos de transparência para o Poder Público, que deve informar, preferencialmente em seus sítios eletrônicos, as hipóteses em que no exercício de suas competências tratam dados pessoais com informações claras sobre previsão legal, finalidade, procedimento e práticas adotadas. Há ainda a previsão de que a Autoridade Nacional de Proteção de Dados disponha mais detidamente sobre essa forma de publicidade (artigo 23, 1º).

5. Novos direitos

É na relação com o cidadão (titular dos dados) que se dá o desenvolvimento democrático. Se a Constituição previu o *habeas data*, para o acesso aos próprios dados pessoais, a Lei de

[6] Dados disponíveis em: https://www.portaldaprivacidade.com.br. Acesso em: 20 jan. 2020.

Acesso à Informação, anos mais tarde, tornou o caminho para esses dados institucional. Hoje, a Lei Geral de Proteção de Dados solidifica e amplia os direitos do cidadão, que vão muito além do mero acesso. O artigo 18 estabelece os direitos à confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade; portabilidade; eliminação dos dados pessoais; informação das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e revogação do consentimento.

A interpretação conjunta, indicando a evolução democrática aqui apontada, pode ser confirmada a partir da disposição do §3º, artigo 23, Lei Geral de Proteção de Dados, de que os prazos e procedimentos para o exercício desses direitos perante o Poder Público observarão a legislação específica, em especial à Lei do *Habeas Data*, a Lei Geral do Processo Administrativo e a Lei de Acesso à Informação. É dizer que a Lei Geral de Proteção de Dados adentra o ordenamento jurídico como um passo adiante na relação de transparência democrática com os cidadãos.

São, de fato, diversas as referências expressas da Lei Geral de Proteção de Dados a essas outras importantes leis que a precederam, apontando um acréscimo de *prestações positivas* aos cidadãos. Outro exemplo é a instituição de autoridades responsáveis pelo cumprimento das obrigações da Lei de Acesso à Informação, já realizadas pelos órgãos públicos, e a atual necessidade de indicação de um encarregado pelo tratamento de dados pessoais da Lei Geral de Proteção de Dados. Antes que houvesse confusão entre as referidas figuras e seus papéis, o artigo 23, §2º, Lei Geral de Proteção de Dados, faz a distinção e exige ambas as indicações.

6. Indicação de encarregado pelo tratamento de dados pessoais e outras obrigações

Aliás, a Lei é ainda mais rigorosa com o Poder Público. Em regra, a obrigatoriedade da indicação de um encarregado é apenas para os controladores de dados (artigo 41, Lei Geral de Proteção de Dados). Contudo, quando se tratar de Poder Público, mesmo que este esteja no papel de operador (artigo 39, Lei Geral de Proteção de Dados), haverá necessidade da indicação, nos termos do inciso II, artigo 23. Portanto, em quaisquer dos papéis de agente de tratamento de dados, o Poder Público deverá indicar seu encarregado. Como ponto de contato entre o órgão público e os cidadãos, titulares de dados, vê-se que haverá uma forte intersecção entre as autoridades da Lei de Acesso à Informação e da Lei de Proteção Geral de Dados. Ainda que tenham atuação conjunta para alguns pontos coincidentes, existirão como autoridades distintas, com focos e preocupações autônomas, que devem se fortalecer mutuamente.

Da mesma forma, existirão obrigações similares, como a de elaborar relatório anual de cumprimento dessas legislações. O relatório da Lei de Acesso à Informação, previsto no artigo 67, II, Decreto 7.724/2012, e o registro das operações de tratamento de dados pessoais, prevista no artigo 37, Lei Geral de Proteção de Dados, cumulado com o relatório de impacto à proteção de dados pessoais, ademais da hipótese já mencionada do artigo 4º, III, também nos casos de legítimo interesse e de tratamento de dados pessoais sensíveis; e com o monitoramento contínuo e avaliações periódicas da adequação, previstos no artigo 50, §2º, I, "h".

7. Sanções

Também no que concerne às sanções, a Lei Geral de Proteção de Dados é explícita ao somar com demais leis pertinentes. O parágrafo 3º do artigo 52, Lei Geral de Proteção de Dados, que fora vetado pelo Presidente da República e retornou ao ordenamento jurídico com a rejeição legislativa do referido veto, aplica ao Poder Público as sanções da lei (exceto as de multas simples ou diária), expressamente sem prejuízo das sanções do Estatuto do Servidor Público Federal, da Lei de Improbidade Administrativa e da Lei de Acesso à Informação. Dessa forma, é possível *a priori* que um mesmo incidente cumule as sanções dessas legislações específicas, dentro da matriz constitucional de responsabilidade do artigo 37, §6º.

Conclusão

Para qualquer agente de tratamento de dados pessoais, seja ele público ou privado, a proximidade da vigência da Lei Geral de Proteção de Dados representa a oportunidade de ingresso em um novo paradigma de proteção de dados. As exigências da adequação passam necessariamente pela reflexão sobre as atividades cotidianas nas quais se tratam os dados pessoais, a saber se eles são necessários e adequados às finalidades que atendem; e sobre a transparência e a segurança com a qual os tratamos.

Para o Poder Público, particularmente, essa oportunidade insere-se em um contexto macropolítico de relevância. A Lei Geral de Proteção de Dados surge no ordenamento jurídico brasileiro dentro da perspectiva de fortalecimento das relações democráticas com os cidadãos, construídas a partir da Constituição Federal, notadamente com a Lei do *Habeas Corpus* e a Lei do Acesso à Informação. Em uma sociedade de informação, saber é poder. A transparência sobre o tratamento dos dados pessoais sobre os quais se sabe implica necessariamente o compartilhamento do poder detido, pois comprova pela clareza a legalidade das ações realizadas pelo Poder Público. Nessa perspectiva, a Lei Geral de Proteção de Dados é um passo à frente em nossas relações democráticas.

Referências

BRASIL. *Projeto de Emenda Constitucional nº 17/2019*. Disponível em:https://bit.ly/2tArLYP. Acesso em: 20 jan. 2020.

[*Precedente sobre a autodeterminação informativa*]. Disponível em: https://bit.ly/37cJeFn. Acesso em: 20 jan. 2020.