

# EVIDÊNCIAS E DADOS NAS POLÍTICAS PÚBLICAS: O FALSO EMBATE ENTRE TRANSPARÊNCIA E PRIVACIDADE<sup>1</sup>

Denise do Carmo Direito<sup>2</sup>

Fernanda Teixeira Reis<sup>3</sup>

## SINOPSE

A produção de evidência necessita do acesso a dados de qualidade, e o Estado é produtor e fornecedor relevante desses para balizar a ação pública. A manipulação dos dados – para torná-los compreensíveis para o processo analítico e decisório – utiliza ferramentas cada vez mais avançadas e complexas do ponto de vista tecnológico e estatístico. Este texto analisa políticas públicas em diferentes etapas do ciclo de implementação, apontando caminhos, riscos e limites para o estabelecimento de formas adequadas para se compatibilizar transparência – conforme normatizado pela Lei de Acesso à Informação (LAI) de 2011 – e privacidade – reafirmada na Lei Geral de Proteção de Dados Pessoais (LGPD) de 2018. Conclui-se pela necessidade de instituir mecanismos transparentes de coleta e uso de dados e, ao mesmo tempo, estabelecer tratamentos necessários, utilizando-se tecnologia e estatística avançada, como rotinas de anonimização e pseudoanonimização, para disseminarem-se dados sem renunciar à proteção dos cidadãos.

**Palavras-chave:** políticas públicas; evidências; transparência; privacidade.

## 1 INTRODUÇÃO

O conceito de evidências é aplicado às análises de políticas públicas em um processo que busca imprimir racionalidade à formulação, à implementação e à avaliação de políticas. As evidências são um recurso de um campo de conhecimento. Na atenção primária à saúde, por exemplo, essa prática agrega evidências científicas (com análises experimentais, aleatorizadas, grupo controle, efeito placebo, controle de variáveis espúrias) às experiências clínicas e preferências do paciente, com o objetivo de apoiar profissionais e melhorar a efetividade clínica (Schneider, Pereira e Ferraz, 2020). Trata-se da busca da redução de intuição e achismos por meio do uso de práticas rigorosas baseadas em dados, modelos estatísticos e econométricos robustos e capacidades analíticas requintadas ao processo de tomada de decisão.

O debate relacionado a políticas públicas baseadas em evidências (PPBEs) é amplo e foi abordado em literaturas anteriores (Pinheiro, 2020; Koga *et al.*, 2022a). O foco deste artigo são os dados e seus usos, ou seja, a necessidade de que essa unidade que invariavelmente está na base da produção de conhecimento para políticas públicas esteja disponível e de que seus usos sejam transparentes e acessíveis a qualquer interessado, sem colocar em risco o direito à privacidade.

---

1. DOI: <http://dx.doi.org/10.38116/bapi37art11>

2. Especialista em políticas públicas e gestão governamental (EPPGG) em exercício na Diretoria de Estudos e Políticas do Estado, das Instituições e da Democracia do Instituto de Pesquisa Econômica Aplicada (Diest/Ipea).

3. Especialista em financiamento e execução de política educacional no Fundo Nacional de Desenvolvimento da Educação do Ministério da Educação (FNDE/MEC).

Parte-se da premissa de que metodologia, qualidade dos dados, transparência e privacidade são aspectos fundamentais para a produção de evidências adequadas.

O Estado é produtor e fornecedor relevante de dados para balizar a ação pública. As fontes de produção de informação são múltiplas e abarcam estatísticas públicas, como as produzidas pelo Instituto Brasileiro de Geografia e Estatística (IBGE) – Censo Nacional, Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua), Pesquisa de Informações Básicas Municipais (Munic) – e pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) – Censo da Educação Básica e Sistema de Avaliação da Educação Básica (Saeb) –, além de registros administrativos que fornecem informações sobre renda, emprego, infraestrutura educacional e vulnerabilidades sociais, como o Cadastro Único para Programas Sociais (CadÚnico), a Relação Anual de Informações Sociais (Rais), entre tantos outros.<sup>4</sup> Para além desse papel de coletar e armazenar dados, o Estado é usuário ativo desses nas mais diferentes etapas das políticas públicas, desde a definição até a análise dos resultados alcançados, passando pela implementação e pela execução.

O processo de manipulação dos dados – com o objetivo de torná-los compreensíveis para o processo analítico e decisório – utiliza ferramentas cada vez mais avançadas e complexas do ponto de vista tecnológico e estatístico. Por exemplo, o uso de *data warehouse* para centralizar o armazenamento de dados públicos; o uso de plataformas de *business intelligence* (BI) para disseminar aos tomadores de decisões e executores das políticas informações importantes, a exemplo das disponibilizadas para secretários municipais de educação, ou mesmo diretores de escolas, para que saibam o tamanho do seu alunado, suas características e repasses de verbas previstas para programas educacionais. Na última década, o aumento da capacidade computacional tornou corriqueiras palavras como algoritmos, inteligência artificial (IA) e aprendizado de máquina (*machine learning*) como soluções possíveis de serem utilizadas nas variadas etapas das políticas públicas.

Todos esses processos utilizam larga e majoritariamente dados pessoais sensíveis dos cidadãos.<sup>5</sup> Há um imbricado complexo composto por: i) produção de informação para políticas públicas e a melhoria da ação pública; ii) uso crescente de novas e robustas tecnologias de tratamento de dados pessoais; e iii) aparentemente na contramão de tudo isso, a necessidade de preservar a privacidade dos donos dos dados. Este é um tema cada vez mais premente em mundo mediado pela velocidade e pela abrangência da internet, que expõe os sujeitos a um olhar ampliado de uma sociedade amorfa, em que a divulgação de informações pessoais pode causar sérios prejuízos financeiros e morais.

Este texto busca contribuir com o debate sobre a necessidade de a ação pública se basear em evidências, muitas vezes sendo necessários o acesso e a manipulação de dados pessoais, sem que isso signifique risco da exposição indevida. A proposta é transpor o falso dilema entre proteção e transparência. Partimos da premissa de que dados individuais devem ser considerados como um elemento em constante evolução, e não sob uma abordagem punitiva. O governo tem a responsabilidade de gerenciar e reconhecer os possíveis riscos associados ao seu uso. Contudo, não deve adotar soluções simplistas de limitação da informação ou escolher apenas a disseminação agregada, o que inviabiliza análises apropriadas.

4. Para relação de registros administrativos produzidos no âmbito do governo federal para produção de evidências nas mais distintas áreas, consultar Mello (2022).

5. Conforme a Lei Geral de Proteção de Dados Pessoais (LGPD), dados pessoais sensíveis se referem a “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (Brasil, 2018).

O texto se subdivide, além desta introdução, em três etapas. Primeiro, descrevem-se de forma resumida três diferentes políticas do campo social e educacional. São casos reais que exemplificam a complexidade de ter acesso a dados, mas também os cuidados que surgem a partir do uso intenso de ferramentas tecnológicas para decisão, implementação e avaliação das políticas públicas. Na sequência, fazemos breve relato sobre como as leis que tratam da necessidade da transparência da ação pública e da privacidade dos dados pessoais se desenvolveram e priorizaram determinados aspectos em detrimento de outros ao longo do tempo, desde a Constituição Federal de 1988 (CF/1988). Concluímos analisando o aparente paradoxo em que por meio do uso da própria tecnologia se supera o que entendemos ser um falso embate entre privacidade e transparência, questões relacionadas à explosão do uso da tecnologia no mundo das políticas públicas.

## 2 POLÍTICAS PÚBLICAS E O USO INTENSIVO DE DADOS

Conforme dito anteriormente, as políticas públicas utilizam dados pessoais em diferentes etapas e de diferentes formas. Para melhor compreender como isso ocorre no cotidiano da administração, analisamos brevemente três casos, focando no uso de dados e buscando explicitar as tecnologias utilizadas e os diferentes limites decorrentes desse processo.

### 2.1 Prospecção, avaliações e estudos em políticas educacionais

O Inep, do Ministério da Educação (MEC), anualmente coleta, trata e dissemina dados da educação básica por meio do Censo da Educação Básica. Até 2021, sua divulgação costumava ser via microdados, aplicando tratamentos para anonimizar os indivíduos da comunidade educativa, como alunos, professores e técnicos. Essas informações permitiam que se fizessem projeções sobre o alunado, caracterizando-se por ser a linha mestra na condução dos principais programas educacionais brasileiros, a exemplo do Programa Nacional da Alimentação Adequada (PNAE), do Programa Nacional do Livro Didático (PNLD), do Programa Nacional do Transporte Escolar (PNATE) e do Programa Dinheiro Direto na Escola (PDDE). Cabe destacar que esses programas são financiados pelo salário-educação, o qual regulamenta que as quotas desses tributos devem ser proporcionais ao alunado dos entes federativos, “conforme apurado pelo censo educacional realizado pelo Ministério da Educação” (Lei nº 9.766/1998). O Censo Escolar é fundamental para os entes federativos estabelecerem seu público-alvo, para o órgão federal, especialmente o Fundo Nacional de Desenvolvimento da Educação (FNDE), planejar a aplicação dos recursos e assistência técnica e para a comunidade educativa efetivar o controle social.

No entanto, em 2022, o Inep limitou o acesso a esses dados, divulgando somente aqueles desagregados do questionário “escola” e parcialmente os dos demais questionários. Esse limite foi imposto inclusive a servidores de órgãos que necessitam de microdados para planejar, monitorar e avaliar repasses para os programas educacionais federais, como os educacionais citados anteriormente, as secretarias estaduais, municipais e distrital de educação e a própria escola. Essa ação também restringiu a possibilidade da elaboração de estudos e avaliações feitas por especialistas, universidades e até por organizações da sociedade civil, entre outros atores. Ao restringir essa divulgação, impede-se ou restringe-se a geração de indicadores, situação que cria uma lacuna na estrutura da política educacional municipal e estadual, não só acarretando prejuízos relevantes para a prestação de apoio técnico e supervisão por parte do órgão federal, mas também inviabilizando iniciativas de planejamento e monitoramento conduzidas pelas prefeituras e suas unidades executoras (Reis e Direito, 2023).

A justificativa recorrente para a limitação da divulgação dos dados pessoais tem sido falta de adesão à LGPD. No caso específico do MEC, foi contratada uma consultoria externa que teria encontrado falhas no processo de não identificação dos indivíduos desse levantamento censitário. É necessário ressaltar que, conforme destacado até por entidades e movimentos de educação, a própria LGPD (art. 7º, incisos II e III) assegura que “a administração pública pode realizar o tratamento de dados pessoais necessários ao cumprimento de obrigação legal e/ou execução de políticas públicas, sem que para isso seja necessário o prévio consentimento da/o titular destes dados”.<sup>6</sup> Quando se trata de dados pessoais sensíveis, deve se operar algum tipo de rotina de anonimização e pseudoanonimização para que não se exponha desnecessariamente o cidadão.

A confusão entre restrição e acesso já foi tratada pela própria Controladoria-Geral da União (CGU), controle interno do Poder Executivo, responsável por zelar pela transparência na gestão pública. Este órgão fez, no início de 2023, estudo detalhado para dirimir dúvidas e retificar posições equivocadas que a própria controladoria havia exarado em processos específicos (Brasil, 2023). A CGU sustenta que a “LAI [Lei de Acesso à Informação] sujeita a restrições apenas informações pessoais sensíveis, que possam vir a prejudicar a intimidade, honra e imagem do seu titular. Mesmo a existência dessa categoria de dados não é motivo para se negar acesso a todo o conteúdo do documento que a contenha” (Brasil, 2023, p. 66). Assim, o texto busca pacificar o entendimento de que a LAI e a LGPD não são incompatíveis.<sup>7</sup>

Ademais, a divulgação adequada dos dados permite que auditorias e avaliações autônomas analisem a adequação da atuação governamental. Vale lembrar que são investidos vultosos recursos em educação e que essas ações de verificação ajudam a reduzir ineficiência e evitar desvios de recursos.

## 2.2 Concessão de benefício

O uso de algoritmos e de aprendizado de máquina (*machine learning*) para simplificar processos internos do Estado, como a concessão de benefícios, se torna cada vez mais corriqueiro no país. O Instituto Nacional do Seguro Social (INSS), por exemplo, incorporou essas técnicas para análise de aposentadorias e Benefício de Prestação Continuada (BPC). No entanto, notícias da imprensa<sup>8</sup> e estudos realizados (Paiva e Pinheiro, 2022) apontam que o processo precisa de revisão e aperfeiçoamento, visto que há indícios de rejeição indevida em larga escala, bem como inadequação de certas rotinas ao processo de digitalização. Para além da análise sem a interferência humana, há relatos sobre dificuldades no tempo de revisão e reanálise da decisão que deveria ser feita prioritariamente pelos canais administrativos tradicionais, mas acabam desaguando na justiça.

O sistema de controle já apontou essas inconsistências. O Tribunal de Contas da União já apontou que o uso de IA para análise e concessão de benefícios previdenciários tem apresentado persistentes problemas, com a negativa indevida de grande parte desses benefícios,<sup>9</sup> tema que ganhou repercussão na mídia e segue sendo questionado.<sup>10</sup>

6. Disponível em: [https://ok.org.br/wp-content/uploads/2022/02/PautasPolíticas\\_Inep\\_Posicionamento\\_MicrodadosEnem\\_2022\\_02\\_22\\_FINAL.pdf](https://ok.org.br/wp-content/uploads/2022/02/PautasPolíticas_Inep_Posicionamento_MicrodadosEnem_2022_02_22_FINAL.pdf).

7. A CGU já havia publicado, no Diário Oficial da União (DOU) de 14 de março de 2022, o Enunciado nº 4 sobre o entendimento da compatibilidade da LAI com a LGPD. Disponível em: [https://repositorio.cgu.gov.br/bitstream/1/67735/3/Enunciado\\_4\\_2022.pdf](https://repositorio.cgu.gov.br/bitstream/1/67735/3/Enunciado_4_2022.pdf).

8. Disponível em: <https://extra.globo.com/economia-e-financas/robo-do-inss-indefere-3-de-cada-4-pedidos-de-aposentadoria-veja-como-aumentar-suas-chances-25588530.html>.

9. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/auditoria-aponta-falhas-do-inss-no-processo-de-analise-de-recursos-previdenciarios.htm>.

10. Disponível em: <https://www1.folha.uol.com.br/mercado/2023/07/inss-aumenta-analise-de-aposentadorias-por-robos-e-nega-beneficio-em-seis-minutos.shtml>.

Esse processo, além de gerar desproteção, gera retrabalho ao transferir a fila da entrada da solicitação para a de revisão da análise, aspecto já sinalizado no caso em que a instituição de aplicativo (*app*) na política da assistência social apenas alterou a fila do presencial para o virtual.<sup>11</sup> Dessa forma, essas soluções precárias merecem avaliação e análise mais detalhadas, primeiro pela opacidade que instituem, pois dificultam que o cidadão compreenda o rito de avaliação e concessão que a suas solicitações são submetidas; e segundo porque uma parcela da sociedade brasileira ainda tem dificuldade de acessar as próprias ferramentas de interação com o Estado.

### 2.3 Auditoria e fiscalização

Outro exemplo de baixa transparência para o cidadão no uso de tecnologia para qualificação de dados e controle de pagamento é a utilização de grandes bases administrativas para qualificar autorizações de benefícios. Por exemplo, o CadÚnico é uma base que reúne informações de 94 milhões de pessoas, ou seja, mais de 42 milhões de famílias,<sup>12</sup> com dados sobre renda, moradia, escolaridade, pertencimento a grupos populacionais tradicionais e específicos, como indígenas, quilombolas, entre outros. No entanto, por ser autodeclaratório, utiliza outras bases de dados em um processo de controle para a concessão de benefícios apenas ao grupo devido. São feitas checagens com um número crescente de outros registros administrativos, como o Cadastro Nacional de Informações Sociais (CNIS),<sup>13</sup> para avaliação de correção das informações prestadas pelos requerentes (Banco Mundial, 2021).

Cabe ressaltar que esse processo apresenta problemas, já que as bases utilizadas muitas vezes são anteriores às informações prestadas ao CadÚnico. Assim, o cidadão é obrigado a comparecer várias vezes ao local de cadastramento, arcando com custos desnecessários. A adoção de batimentos automatizados<sup>14</sup> com número cada vez maior de bases poderia se transformar em uma “espiral rigorosista” (Dubois, 2021, p. 57), que não para de girar e apertar, sendo que esses controles são feitos majoritariamente com políticas destinadas aos mais vulneráveis. A retificação de achados indevidos, ou seja, dos aparentes indícios de inconsistência, oriundos desse processo de checagem de informação, podem ser de difícil execução para uma parcela da população, visto serem necessários recursos financeiros, de tempo e mesmo compreensão do que ocorreu para poder ser feita a oposição ou prestação de esclarecimentos demandados. Vale observar os achados de Virginia Eubanks (2018), que, ao analisar política similar – cadastro para moradia –, identificou uma sensação de injustiça que o excesso de checagens gerava. São necessárias avaliações mais complexas que considerem tanto a redução de pagamentos indevidos quanto o ônus que essas auditorias geram para o todo das famílias.

Os três exemplos mencionados traduzem para a prática duas importantes dimensões. A primeira é a necessidade de se dar acesso aos dados reais, mas não necessariamente identificados, para que seja possível a reprodução das decisões, avaliando acertos e erros nos processos interestado. A segunda dimensão, bastante analisada em literatura específica (Filgueiras, 2023), mas ainda pouco debatida

11. Sobre análise das filas para acesso a benefícios socioassistenciais, consultar: Lício, E.; Direito, D.; Koga, N. A rota da humilhação para acessar os programas sociais. Coluna Diálogos Públicos. *UOL Notícias*, 19 set. 2022. Disponível em: <https://noticias.uol.com.br/colunas/dialogos-publicos/2022/09/19/a-rota-de-humilhacao-para-acessar-os-programas-sociais.htm>.

12. Conforme dados de janeiro de 2023, disponíveis em: <https://aplicacoes.cidadania.gov.br/vis/data3/data-explorer.php>.

13. Conforme relatório do Banco Mundial (2021), algumas bases utilizadas nesse processo de auditoria são: o Imposto de Renda de Pessoa Física da Receita Federal do Brasil (IRPF/RFB), o Sistema Integrado de Administração de Pessoal (Siape), a folha de pagamentos de benefícios assistenciais e previdenciários do INSS (maciça), a Rais, o Cadastro Geral de Empregados e Desempregados (Caged), a Guia de Recolhimento do Fundo de Garantia do Tempo de Serviço e Informações à Previdência Social (GFIP) e o Sistema Integrado de Administração Financeira (Siafi).

14. Batimentos é o nome usual para o processo de checagem de informações de cidadãos feitas por meio de dados disponíveis em duas ou mais bases.

no âmbito da gestão, é a obrigatoriedade de dar transparências aos recursos tecnológicos e métricos usados dentro do Estado para definir políticas, conceder benefícios ou avaliar a ação pública. Para tanto, além de fornecer os dados, é preciso dar transparência à forma como estes foram manipulados.

Entretanto, para garantir que a divulgação de todo esse processo não incorra em exposição indevida de dados pessoais, é necessária a adoção de tratamentos métricos sofisticados, a exemplo da anonimização e pseudoanonimização,<sup>15</sup> para viabilizar o uso dos microdados. Impedir o acesso aos dados não é solução, nem mesmo está previsto em legislação. O pressuposto é a necessidade de garantir transparência ativa para que expertos e sociedade como um todo possam reedificar e reproduzir procedimentos e análises.

Na sequência, analisamos as principais normas editadas nos últimos anos que ora trataram da *transparência* (necessidade de permitir que os processos sejam conhecidos, auditados e reproduzidos), ora da *privacidade* (garantia de que os dados pessoais sejam usados em benefício do cidadão e fora do alcance de transações não autorizadas por lei), deixando, por vezes, um vácuo para equilibrar os dois aspectos na prática das políticas públicas.

### 3 PRIVACIDADE E TRANSPARÊNCIA NA LEGISLAÇÃO BRASILEIRA

No Brasil, a proteção de dados começa a despontar na CF/1988. O título II (Dos Direitos e Garantias Fundamentais), no art. 5º, já apresenta um aparente conflito entre abertura de dados e preservação da pessoa humana.

São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (CF, 1988, art. 5º, inciso X).

Todos têm direito a receber dos órgãos públicos informações de interesse particular, ou de interesse coletivo ou geral, *que serão prestadas no prazo da lei*, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (CF, 1988, art. 5º, inciso XXXIII).

Apesar de o acesso à informação ser um direito fundamental, por ser uma norma de eficácia contida, esse direito precisou de regulamentação para produzir todos os seus efeitos (Ferreira Filho, 2012). Em 1998, ou seja, dez anos após a promulgação da CF, a Emenda Constitucional (EC) nº 19 enfatizou esse caráter limitador ao assegurar:

a lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente: (...) II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII (EC nº 19, art. 37, inciso XXII, § 3º).

Treze anos após à EC nº 19, a LAI (Lei nº 12.571/2011) regulamenta o direito de os cidadãos acessarem essas informações. A lei estabelece que informações são “dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio,

15. Dado anonimizado é aquele em que o indivíduo não pode ser identificável, com aplicação de técnicas que anonimem esse titular, como o não uso de nomes, números de documentos, endereços, nome de mães. Apesar disso, especialmente em tempos de grandes poderios computacionais, apenas anonimizar pode não ser eficaz. Por exemplo, cruzar duas ou mais bases governamentais pode identificar o indivíduo. Assim, ascendem técnicas de pseudoanonimização, que considera o dado pessoal em um contínuo para além do anônimo e não anônimo. Pode, por exemplo, substituir atributos com grandes possibilidades de serem únicos em um registro por outro (Reis e Direito, 2023).

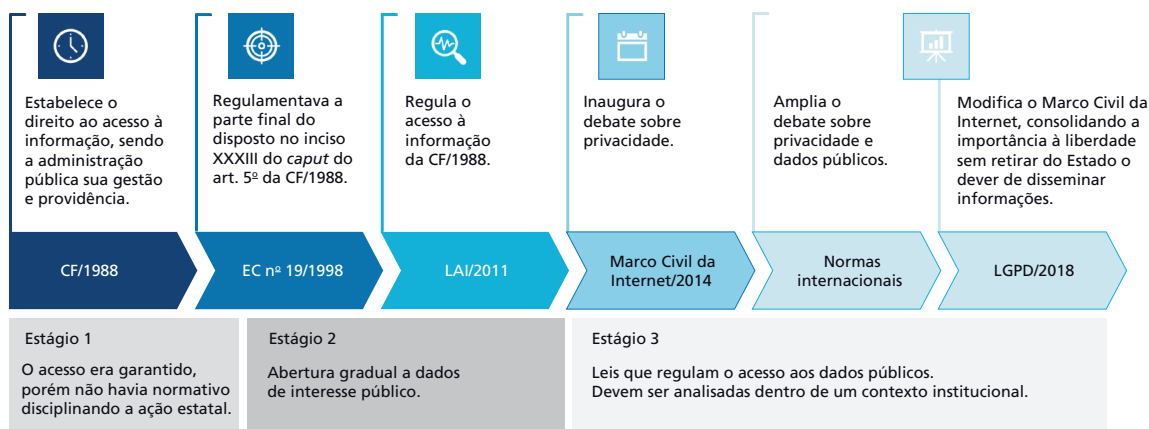
suporte ou formato” (LAI, 2011, art. 4º). Esse passa a ser o marco no tratamento e na disseminação de dados na União, estados, Distrito Federal, municípios e entidades sem fins lucrativos que recebam recursos públicos. É importante ressaltar que, conforme a LAI:

- 1) O sigilo é instaurado como exceção e não regra. Ou seja, se pode ter acesso a qualquer informação pública, exceto as apresentadas em lei.
- 2) A divulgação das informações públicas deve ser ampla, independentemente de solicitação ou justificativa do pedido de acesso (transparência ativa). O órgão não pode, inclusive, perguntar o porquê da solicitação. O diálogo entre órgão e demandante se faz para que se possa entender melhor a demanda deste. Esse serviço tampouco deve gerar custos ao demandante, com exceção daqueles referentes a serviços e materiais.
- 3) Informação pessoal é aquela relacionada à pessoa natural identificada ou identificável, sendo dever do Estado tratá-la para não expor o cidadão, tampouco impedir a disseminação do dado (Brasil, 2011).
- 4) O Estado deve disseminar informações de forma clara, simples e transparente.
- 5) A LAI estabelece prazo de vinte dias, prorrogáveis por mais dez, para a entidade disponibilizar os dados.
- 6) A negativa do acesso, quando não fundamentada, poderá motivar medidas disciplinares.
- 7) Fica estabelecida a obrigatoriedade da criação de Serviço de Informações ao Cidadão (SIC), nos órgãos e entidades do poder público (LAI, art. 9º).

A entrada em vigor da LAI provocou grandes mudanças nas instituições públicas. A obrigação legal, com prazo não superior a trinta dias, coagiu as instituições a se reorganizarem a fim de cumprir tais demandas. No governo federal, por exemplo, se consolidou o Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC). Trata-se de um sistema que centralizou todos os pedidos de entrada e saída de informação ao Poder Executivo federal, organizando e facilitando para os cidadãos o acesso à informação federal.<sup>16</sup> Dotação orçamentária própria e qualificação de pessoal modificaram a forma de as instituições públicas tratarem e disseminarem seus dados.

Esquemáticamente, pode-se compreender essas mudanças, conforme a linha do tempo apresentada na figura 1.

FIGURA 1  
Linha do tempo do acesso à informação



Elaboração das autoras.

16. O e-SIC federal adota o nome FalaBr e está disponível em: <https://falabr.cgu.gov.br/web/home>. Acesso em: 31 mar. 2024.

No estágio 3, identifica-se o crescimento de novas tecnologias de prospecção de dados. O aumento da capacidade de armazenamento e a monetização das informações privadas e pessoais esquentaram o debate entre proteção e acesso aos dados, pendendo para privacidade. No Brasil, em 23 de abril de 2014, a promulgação da Lei nº 12.965, conhecida como Marco Civil da Internet, teve como foco a proteção de dados e a regulamentação da internet no Brasil. Essa legislação apresenta uma seção específica sobre proteção aos registros de dados pessoais e comunicações privadas, garantindo a privacidade, mas regula a disponibilização deles quando houver ordem judicial, bem como o acesso a dados cadastrais às autoridades administrativas que tenham competência legal à requisição.

Vale destacar que a última década é marcada no cenário internacional pelo crescente debate sobre coleta, uso e armazenamento de dados pessoais por empresas e órgãos governamentais. A Comunidade Comum Europeia, por exemplo, cria um grupo independente – Grupo de Proteção de Dados do Artigo 29 – para trabalhar questões referentes à privacidade e à proteção de dados e promulga, em maio de 2018, o Regulamento Europeu de Proteção de Dados, passo inicial para a consolidação do European Data Protection Board.

Inspirado nos debates internacionais, o Brasil institui a Lei nº 13.709 (LGPD), aprovada em 2018, entrando em vigor em 2020. Trata-se de lei que complementa o Marco Civil da Internet, visto que a LGPD amplia o horizonte ao estabelecer diretrizes mais específicas de aplicação e segurança, definindo, por exemplo, como entidades, públicas e privadas, devem coletar, armazenar, utilizar e compartilhar dados pessoais. A lei garante também que os titulares dos dados possam acessá-los, corrigi-los, solicitar portabilidade entre entidades e até mesmo substituí-los.

A LGPD aponta para o remédio que deve ser adotado para proteger os dados individuais: cabe ao Estado utilizar-se de meios técnicos disponíveis e razoáveis para disseminar a informação sem expor o cidadão ao escrutínio público. Trata-se da anonimização dos dados identificáveis (Brasil, 2018, art. 10, inciso III) com outras técnicas específicas que não tornem a pessoa natural identificável. Ou seja, é dever do Estado tratar os dados para não serem identificáveis, bem como elaborar estudos de potenciais riscos (Machado e Doneda, 2018).

#### 4 CONCLUSÕES: FALSO EMBATE ENTRE TRANSPARÊNCIA E PRIVACIDADE

Os exemplos de políticas públicas apresentados nos informam que é importante analisar as distintas hierarquias de acesso aos dados. Atividades de planejamento e avaliação podem tranquilamente trabalhar com dados pseudoanonimizados. Porém, se o objetivo é busca ativa de crianças em situação de abandono escolar, é necessário que parte desses dados seja acessível, a exemplo da identificação da família, a determinados agentes do poder público. O direito à privacidade deve ser relativizado quando há o dever de agir estatal, limitando o acesso aos atores devidos e protegendo a privacidade.

A legislação, por sua vez, permite traçar um histórico apontando que o contexto institucional, político e ideacional influencia a instituição de regras que dão os contornos da ação pública. A partir de um cenário de intensa mudança, vai-se da necessidade de transparência para a premência da defesa da privacidade.

No entanto, a forma de compatibilizar essas contradições que a tecnologia trouxe, em que capacidades computacionais e estatística avançadas colocam em risco a privacidade de cidadãos, que ficam expostos a ter sua vida esquadrihada por uma sociedade ampliada e nem sempre bem-intencionada, é um aparente paradoxo: utilizar mais tecnologia. Afinal, a segurança de dados é



uma ciência “autofágica”: o progresso é determinado pela vulnerabilidade das técnicas atuais e pela substituição por técnicas mais seguras ao novo cenário (Aranha, 2019). Assim sendo, é responsabilidade do Estado testar permanentemente os riscos potenciais de identificações de seus cidadãos em suas bases de dados.

Dessa forma, é necessário seguir trilhando dois caminhos possíveis, superando a aparente contradição. O primeiro é que, para melhoria do desenho, formulação e implementação das políticas públicas, se faz necessária a transparência ativa: o aprendizado do que foi feito com os dados, especialmente por meio da reprodução de suas sintaxes e algoritmos aplicados aos microdados, em consonância com participação social para definir como estes foram e serão usados. É importante lembrar que informação é poder. Acesso a dados é poder. Faz-se necessário estabelecer mecanismos transparentes de coleta e uso de dados, bem como viabilizar mecanismos de controle social das ações do Estado. A segunda questão, mas no mesmo grau de importância, é o dever do Estado de aplicar tratamentos necessários, a exemplo da anonimização e da pseudoanonimização, para disseminar dados sem renunciar à proteção dos cidadãos.

## REFERÊNCIAS

ARANHA, Diego F. O que é criptografia fim a fim e o que devemos fazer a respeito. **Caderno especial: a regulação da criptografia no direito brasileiro**. São Paulo: Editora Revista dos Tribunais, 2019.

BANCO MUNDIAL. **Seleção de beneficiários do Auxílio Emergencial**: estratégias de cadastramento e de verificação de elegibilidade. Washington: World Bank Group, 2021. (Nota Técnica, n. 1). Disponível em: <https://documents1.worldbank.org/curated/en/099205012022129463/pdf/P17483606c29c50ca082ea081e5891caba3.pdf>.

BRASIL. Controladoria-Geral da União. **Acesso à informação pública**: uma introdução à Lei nº 12.527, de 18 de novembro de 2011. Brasília: CGU, 2011. Disponível em: [https://portal.ifrn.edu.br/acessoainformacao/arquivos-importantes/cartilha-da-cgu-sobre-a-lei-de-acesso-a-informacao/at\\_download/file](https://portal.ifrn.edu.br/acessoainformacao/arquivos-importantes/cartilha-da-cgu-sobre-a-lei-de-acesso-a-informacao/at_download/file). Acesso em: 17 mar. 2023.

\_\_\_\_\_. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial**, Brasília, 14 ago. 2018.

\_\_\_\_\_. Controladoria-Geral da União. **Parecer sobre acesso à informação para atender ao Despacho Presidencial de 1º de janeiro de 2023**. Brasília: CGU, 2023. Disponível em: [https://www.gov.br/conarq/pt-br/assuntos/noticias/cgu-concluiu-o-parecer-sobre-acesso-a-informacao-para-atender-ao-despacho-presidencial-de-1o-de-janeiro-de-2023/copy\\_of\\_PARECERFINALSOBREACESSOINFORMAO\\_CGU\\_FEV2023.pdf](https://www.gov.br/conarq/pt-br/assuntos/noticias/cgu-concluiu-o-parecer-sobre-acesso-a-informacao-para-atender-ao-despacho-presidencial-de-1o-de-janeiro-de-2023/copy_of_PARECERFINALSOBREACESSOINFORMAO_CGU_FEV2023.pdf). Acesso em: 21 ago. 2023.

CARVALHO, João Paulo Furtado. História da privacidade de dados e suas legislações. **ZUP**, 2021. Disponível em: <https://www.zup.com.br/blog/historia-da-privacidade-de-dados>. Acesso em: 25 out. 2021.

DUBOIS, Vincent. **Contrôler les assistés**: genèses et usages d’un mot d’ordre. Paris: Eds. Raison d’Agir, 2021.

EUBANKS, Virginia. **Automating inequality**: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 2018.

FERREIRA FILHO, Manoel Gonçalves. **Curso de direito constitucional**. 38. ed. São Paulo: Editora Saraiva, 2012. p. 417-418.

FILGUEIRAS, Fernando. The silent reform: digital governance as a strategy for state reform in Brazil. *In*: LISBOA, Erika; GOMES, Ricardo Corrêa; MARINS, Humberto Falcão (Org.). **The Brazilian way of doing public administration**. 1st ed. Bingley: Emerald, 2023, v. 1, p. 83-95.

KOGA, Natália *et al.* (Org.). **Políticas públicas e usos de evidências no Brasil**: conceitos, métodos, contextos e práticas. Brasília: Ipea, 2022a. Disponível em: [https://repositorio.ipea.gov.br/bitstream/11058/11121/1/Políticas\\_publicas\\_e\\_usos.pdf](https://repositorio.ipea.gov.br/bitstream/11058/11121/1/Políticas_publicas_e_usos.pdf).

KOGA, Natália *et al.* Como os burocratas federais se informam? Uma radiografia das fontes de evidências utilizadas no trabalho das políticas públicas. *In*: KOGA, Natália *et al.* **Políticas públicas e usos de evidências no Brasil**: conceitos, métodos, contextos e práticas. Brasília: Ipea, 2022b.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, v. 12, n. 2, 2020. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/10597/5880>. Acesso em: 25 nov. 2021.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Caderno especial**: a regulação da criptografia no direito brasileiro, p. 99-128. São Paulo: Editora Revista dos Tribunais, dez. 2018.

MELLO, Janine. Produção estatal de evidências e uso de registros administrativos em políticas públicas. *In*: KOGA, Natália *et al.* (Org.). **Políticas públicas e usos de evidências no Brasil**: conceitos, métodos, contextos e práticas. Brasília: Ipea, 2022.

PAIVA, Andrea Barreto de; PINHEIRO, Marina Brito. **BPC em disputa**: como alterações regulatórias recentes se refletem no acesso ao benefício. Brasília: Ipea, 2021. (Texto para Discussão, n. 2703). Disponível em: [https://repositorio.ipea.gov.br/bitstream/11058/10890/1/td\\_2703.pdf](https://repositorio.ipea.gov.br/bitstream/11058/10890/1/td_2703.pdf).

PINHEIRO, Maurício. **Políticas públicas baseadas em evidências (PPBEs)**: delimitando o problema conceitual. Brasília: Ipea, 2020. (Texto para Discussão, n. 2554). Disponível em: [https://repositorio.ipea.gov.br/bitstream/11058/9915/1/td\\_2554.pdf](https://repositorio.ipea.gov.br/bitstream/11058/9915/1/td_2554.pdf).

SANTOS, Maykon Adler Oliveira; ARAÚJO, Jeferson Sousa de; REGO, Ighor Jean. A história brasileira de proteção aos dados: o advento da lei geral de proteção de dados pessoais e a sua influência no acesso aos dados médicos no Brasil. **Revista Científica Multidisciplinar Núcleo do Conhecimento**, v. 1, p. 172-198, dez. 2021. Disponível em: <https://www.nucleodoconhecimento.com.br/lei/advento-da-lei>.

REIS, Fernanda; DIREITO, Denise. Dados pessoais e políticas públicas: o que revelar e o que preservar? **Revista Brasileira de Avaliação**, v. 12, n. 1, 2023. Disponível em: <https://rbaval.org.br/article/10.4322/rbaval202312016/pdf/1598015026-12-1-e121623.pdf>.

SCHNEIDER, Luana Roberta; PEREIRA, Rui Pedro Gomes; FERRAZ, Lucimare. Prática baseada em evidências e a análise sociocultural na atenção primária. **Physis**: Revista de Saúde Coletiva, v. 30, n. 2, jan. 2020. Disponível em: <https://www.scielo.br/j/physis/a/kq66hywGnfmM4JtrftJM4ys/>.

VALADARES, Alexandre *et al.* Políticas sociais: acompanhamento e análise. **Boletim de Políticas Sociais**, n. 29, jun. 2022. Brasília: Ipea, 2022. Disponível em: [https://portalantigo.ipea.gov.br/portal/index.php?option=com\\_content&view=article&id=39098&Itemid=9](https://portalantigo.ipea.gov.br/portal/index.php?option=com_content&view=article&id=39098&Itemid=9).

