DADOS
dados.iesp.uerj.br

[Artigos Originais]

A Gramática Institucional da Proteção de Dados e da Privacidade no Brasil*

Fernando Filgueiras[1]

[1]Professor do Doutorado Profissional em Políticas Públicas da Escola Nacional de Administração Pública (ENAP). Bolsista de Produtividade do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).
E-mail: fernandofilgueiras@ufg.br ORCID: https://orcid.org/0000-0001-9570-8113

Lizandro Lui[2]

[2]Professor da Escola de Políticas Públicas e Governo da Fundação Getúlio Vargas (FGV). Brasília, DF. Brasil.
E-mail: lizandro.lui@fgv.br Orcid: https://orcid.org/0000-0002-9276-247X

Maria Tereza Trindade Veloso[3]

[3]Graduanda do curso de Administração Pública da Escola de Políticas Públicas e Governo - Fundação Getulio Vargas (FGV). Brasília, DF. Brasil.
E-mail: mariaterezatrindades@gmail.com Orcid: https://orcid.org/0000-0001-7021-1135

DOI: https://doi.org/10.1590/dados.2025.68.1.346

Banco de Dados: https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/LDNLOB

*Este artigo recebeu financiamento do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), processos 303762/2023-3 e 441095/2023-2 e da Fundação de Amparo à Pesquisa do Distrito Federal, processo n. 00193-00000256/2023-65

Resumo

A Gramática Institucional da Proteção de Dados e da Privacidade no Brasil

Este artigo investiga a gramática institucional da proteção de dados e da privacidade no Brasil. Adotando a lente analítica do *Intitutional Grammar Tool* (IGT), desconstruímos os enunciados institucionais dos decretos regulamentadores da Lei Geral de Proteção de Dados dos estados brasileiros, de forma a classificar os diferentes elementos gramaticais que informam as estratégias estaduais de proteção e governança de dados. Examinamos nesse artigo a construção dos conceitos de proteção de dados, governança de dados e privacidade, assim como a construção institucional da proteção de dados no Brasil. O estudo tem um viés empírico, de maneira a responder às seguintes questões: qual o desenho institucional das estratégias adotadas pelos estados, no contexto da federação, para a proteção de dados pessoais e da privacidade dos cidadãos? Quais as implicações desse desenho para a efetividade da proteção de dados no Brasil? O artigo conclui que as estratégias de proteção de dados formuladas nos estados têm mais o viés de controle burocrático do tratamento de dados do que propriamente a efetivação de direitos emergentes de cidadania.

Palavras-chave: proteção de dados; governança de dados; LGPD; gramática institucional; análise institucional

Abstract

The Institutional Grammar of Data Protection and Privacy in Brazil

This article investigates the institutional grammar of data protection and privacy in Brazil. By adopting the analytical lens of the Institutional Grammar Tool (IGT), it deconstructs the institutional statements within the regulatory decrees of the General Data Protection Law (LGPD) in Brazilian states, classifying the different grammatical elements that inform state-level strategies for data protection and governance. It examines how the concepts of data protection, data governance, and privacy are formulated, as well as the institutional construction of data protection in Brazil. By taking an empirical approach, it aims to address the following questions: What is the institutional design of the strategies adopted by Brazilian states, within the federation, to protect personal data and citizens' privacy? What are the implications of this design on how effective data protection is in Brazil? The article concludes that the data protection strategies formulated by the states lean more toward bureaucratic control of data processing than the actual realization of emerging citizenship rights.

Keywords: data protection; data governance; LGPD; institutional grammar; institutional analysis

Résumé

La Grammaire Institutionnelle de la Protection des Données et de la Vie Privée au Brésil

Cet article explore la grammaire institutionnelle de la protection des données et de la vie privée au Brésil. En adoptant la perspective analytique de l'*Institutional Grammar Tool* (IGT), nous déconstruisons les énoncés institutionnels des décrets réglementaires de la Loi Générale sur la Protection des Données des états brésiliens, afin de classifier les différents éléments grammaticaux informant les stratégies étatiques de protection et de gouvernance des données. Nous examinons dans cet article la construction des concepts de protection des données, de gouvernance des données et de vie privée, ainsi que la construction institutionnelle de la protection des données au Brésil. L'étude a une orientation empirique afin de répondre aux questions suivantes: quel est le dessin institutionnel des stratégies adoptées par les états, dans le contexte de la fédération, pour la protection des données personnelles et de la vie privée des citoyens? Quelles sont les implications de ce dessin pour l'efficacité de la protection des données au Brésil? L'article conclut que les stratégies de protection des données formulées au niveau des états sont davantage orientées vers le contrôle bureaucratique du traitement des données que vers la réalisation effective des droits émergents de la citoyenneté.

Mots-clés: protection des données; gouvernance des données ; LGPD ; grammaire institutionnelle ; analyse institutionnelle

Resumen

La Gramática Institucional de la Protección de Datos y de la Privacidad en Brasil

Este artículo investiga la gramática institucional de la protección de datos y de la privacidad en Brasil. Adoptando la perspectiva analítica del *Intitutional Grammar Tool* (IGT), deconstruimos los enunciados institucionales de los decretos reglamentarios de la Ley General de Protección de Datos de los estados brasileros, con el fin de clasificar los diferentes elementos gramaticales que informaron las estrategias estaduales de protección y gobernanza de datos. Examinamos la construcción de los conceptos de protección de datos, gobernanza de datos y privacidad, así como la construcción institucional de la protección de datos en Brasil. El estudio tiene un abordaje empírico, con el fin de responder a las siguientes cuestiones: ¿cuál es el diseño institucional de las estrategias adoptadas por los estados, en el contexto de la federación, para la protección de datos personales y de la privacidad de los ciudadanos? ¿cuáles son las implicaciones de ese diseño para la efectividad de la protección de datos en Brasil? El artículo concluye que las estrategias de

protección de datos formuladas en los estados tienen más un enfoque de control burocrático de tratamiento de datos que propiamente la implementación de derechos emergentes de ciudadanía.

Palabras clave: protección de datos; gobernanza de datos; LGPD; gramática institucional; análisis institucional

Introdução

O avanço de tecnologias disruptivas tem impactado a sociedade, a qual tem testemunhado novas dinâmicas políticas e de poder, utilizando dados como *inputs* para que sistemas computacionais tomem decisão e realizem tarefas de maneira autônoma quando humanos interagem com elas ou a partir delas (Filgueiras, 2022; Almeida, Filgueiras, Mendonça, 2022; Kendall-Taylor, Frantz, Wright, 2020; Manheim, Kaplan, 2019; Frischmann, Selinger, 2018). Tecnologias como inteligência artificial, *blockchain*, internet das coisas e plataformas avançaram inovando e otimizando diversos processos em governos e em organizações privadas, com impactos econômicos, sociais e políticos.

Por exemplo, o avanço de plataformas de redes sociais transformou a comunicação pública, com impactos políticos que mudaram as preferências de eleitores, dinâmicas de protestos e mobilização social, polarização política, xenofobia e o comportamento de políticos profissionais (Zhuravskaya, Petrova, Enikolopov, 2020). No âmbito de organizações privadas, plataformas possibilitaram a otimização de processos e novos modelos de negócios que amplificam oportunidades de mercado e de produção (Zuboff, 2019). As plataformas são desenhadas com diferentes camadas de inteligência artificial que utilizam dados para produzir otimização e reforçar uma lógica consequencialista. Ou seja, sistemas computacionais absorvem dados para produzir *outputs* e constituir agência a partir de uma premissa utilitarista de reforço de benefícios a partir do entendimento e construção de preferências de cidadãos e consumidores (Russell, 2019).

A inovação que avança com as tecnologias digitais é dependente da extração de dados como requisito para o funcionamento das aplicações desenhadas para atingir um objetivo. Todas estas tecnologias dependem de fluxos de *inputs* de dados para que elas possam produzir *outputs* que apoiem a tomada de decisão e a realização de tarefas de maneira autônoma, otimizando a produção de informação e seus impactos sociais, econômicos e políticos (Russell, 2019). O aspecto inovador das tecnologias digitais é dependente da maior disponibilidade e capacidade de extração e armazenamento de dados, referida como a revolução de *big data*.

Big data é o campo que trata das maneiras de analisar e lidar com conjuntos extensivos de dados coletados de diferentes fontes, de forma veloz e complexa. Dentre suas propriedades, *big data* demanda metodologias e tecnologias para coletar, armazenar, processar e compartilhar dados

de várias fontes para criar um domínio de informação expandido para a implantação de diferentes tecnologias computacionais (Kitchin, 2013; Mayer-Schonberger, Cukier, 2013).

O conceito de dado compreende a informação traduzida em uma forma eficiente (binária) para processamento matemático e computacional. Embora esta seja uma definição técnica, dados têm implicações sociais. De acordo com Rosenberg (2013), dados são instrumentos para produzir retóricas, tendo uma natureza reflexiva na construção de fatos e evidências. Dados são produzidos a partir de números, imagens, fala e texto, compreendendo um aspecto expandido de compreensão das preferências, comportamentos, perspectivas, opiniões e expressões de humanos em suas diferentes interações com máquinas. Dados são recursos organizacionais importantes na sociedade contemporânea e sua quantidade expande a partir da extensão da internet e a crescente conexão de humanos no mundo digital (Kitchin, 2013).

Se, por um lado, há todo um processo de inovação por meio das tecnologias digitais, por outro lado, existem novos riscos e impactos negativos para a sociedade. A inovação que culmina com a crescente presença de plataformas digitais no cotidiano da sociedade e o uso de dados para a tomada de decisão e realização de tarefas é justificada e legitimada por uma lógica de conveniência de consumidores e cidadãos. As plataformas exercem um novo tipo de poder político baseado na conveniência e instrumentalização de preferências de consumidores (Culpepper, Thelen, 2021). Tecnologias digitais possibilitaram inovar e otimizar diferentes processos, mudando diversas dinâmicas sociais. Porém, estas tecnologias digitais trazem novos impactos para a sociedade, criando estruturas que possibilitam novas formas de exclusão social e desigualdade (Eubanks, 2018), a reprodução do racismo e a violência racial (Benjamin, 2019; Noble, 2018), a expansão da vigilância e novas dinâmicas de poder no capitalismo (Zuboff, 2019), expansão da polarização política (O'Neil, 2016) e novas práticas colonialistas (Couldry, Mejias, 2019).

Em todas estas situações, podemos ter problemas com relação ao desenho destas tecnologias, mas o principal elemento que explica as falhas de tecnologias computacionais decorre de bases de dados enviesadas ou pobres semanticamente para resolver o problema proposto (Joyce *et al.*, 2021; Gitelman, 2013). Por exemplo, tecnologias de reconhecimento facial utilizam bases de dados racializadas na expectativa de identifi-

car criminosos. Com isso, elas punem mais pessoas pretas reproduzindo e otimizando profecias autorrealizadas de sociedades regidas por estruturas raciais (Crawford, 2021). Da mesma forma, sistemas de policiamento preditivo calculam comportamento criminoso e produzem antecipação das forças de segurança a partir de bases de dados enviesadas que punem mais pessoas pretas e pobres (Amoore, 2014). Aquilo que é entendido como uma inovação, uma vez que tecnologias se apresentam como ferramentas neutras, termina por criar novos riscos para a sociedade ou reproduz velhos problemas estruturais que cristalizam desigualdades diversas.

A vigilância expandida com a crescente coleta, armazenamento, processamento e compartilhamento de dados produz uma nova dinâmica de poder das grandes corporações de tecnologia (Zuboff, 2019). Existem diversas situações nas quais as tecnologias digitais produzem uma nova ordem de problemas e desafios sociais. Nesse sentido, a governança dos dados, associando mecanismos institucionais de proteção de dados e da privacidade de cidadãos e consumidores é uma resposta encontrada para o avanço da vigilância e a necessidade de qualificação e aprimoramento institucional para o uso de dados.

A agenda da proteção de dados e da privacidade foi acelerada com o escândalo Cambridge Analytica e todo o impacto político gerado. Diversos países passaram a adotar leis de proteção de dados e da privacidade como resposta para a crescente vigilância realizada por governos e corporações. Por exemplo, o *General Data Protection Regulation* (GDPR) europeu criou uma série de instituições que regulam todo o processo de coleta, armazenamento, processamento e compartilhamento de dados com o objetivo de proteger conjuntos extensivos de dados coletados por governos e corporações, assim como proteger a privacidade dos cidadãos delineando uma série de procedimentos e regulações para o tratamento de dados.

No caso do Brasil, a aprovação da Lei Geral de Proteção de Dados (doravante, LGPD – Lei nº 13.709, de 14 de agosto de 2018) foi essencial para estabelecer procedimentos para o tratamento de dados, criação de mecanismos regulatórios para proteger a privacidade e liberdade dos cidadãos e assegurar o cumprimento de normas constitucionais e definição de estratégias para governos e corporações. Considerando a importância dos dados no mundo contemporâneo, o objetivo deste artigo é analisar a arquitetura institucional que emerge com a LGPD

para proteger dados e criar mecanismos regulatórios que resultem no respeito à privacidade do cidadão e novos direitos, com especial foco em governos. A LGPD criou regras amplas e mecanismos regulatórios para o tratamento de dados em governos e corporações, demandando deles a criação de estratégias organizacionais para o cumprimento dos termos normativos e produção de resultados em termos de proteção dos dados e da privacidade.

Este artigo analisa a gramática institucional da governança e proteção de dados examinando o processo de regulamentação da LGPD pelas administrações públicas estaduais. A LGPD criou regras gerais e desenhou um novo processo institucional para o tratamento de dados em governos, requerendo que os estados da federação regulamentem os dispositivos normativos e estabeleçam estratégias para a conformidade (*compliance*) com as regras e produção de resultados em termos de avanço tecnológico, ao mesmo tempo que proteja os ativos de dados e a privacidade dos cidadãos. Este artigo analisa os decretos que regulamentam a LGPD em 15 estados e no Distrito Federal por meio do *Institutional Grammar Tool* desenvolvido inicialmente por Crawford e Ostrom (1995) e posteriormente aprimorado por Basurto *et al.* (2010) e Siddiki *et al.* (2012), desconstruindo todos os enunciados institucionais em sentenças para, então, identificar seus elementos sintáticos. Desconstruir as instituições de proteção de dados por meio de sua sintaxe possibilita identificar quais são os sujeitos a quem são atribuídas as regras, os operadores deônticos, o alvo, o objeto, as condições e as consequências que informam a arquitetura institucional e suas derivações no caso brasileiro.

Os problemas que orientam esta pesquisa são: (1) qual o desenho das estratégias adotadas pelos estados, no contexto da federação, para a proteção de dados pessoais e da privacidade dos cidadãos? (2) Quais as implicações desse desenho para a efetividade da proteção de dados em governos no Brasil? Na primeira seção do artigo, tratamos da governança e proteção de dados e seus desafios conceituais. Na segunda seção do artigo tratamos da LGPD e das inovações institucionais que emergem. Na terceira seção tratamos do desenho da pesquisa. Na quarta seção apresentamos os resultados. Na quinta seção discutimos os achados da pesquisa e, por fim, concluímos mostrando como a regulamentação da LGPD foi direcionada mais por uma lógica de controle burocrático dos dados do que por uma lógica de direitos de cidadania relacionados com a proteção de dados e respeito à privacidade.

Governança, proteção de dados e privacidade

Conforme indicam Abraham, Schneider, vom Brocke (2019), a governança de dados é o exercício da autoridade e o controle sobre a gestão dos dados. A governança de dados tem como objetivo implementar uma agenda de dados maximizando o valor dos ativos e realizar a gestão de risco sobre a coleta, armazenamento, uso e compartilhamento de dados. Ainda que a governança de dados sempre tivesse constado como uma dimensão importante ao longo das últimas décadas, contemporaneamente ela está assumindo um nível mais alto de importância em empresas e instituições governamentais (Whitford, Yates, 2022). Apesar da crescente importância da governança dos dados, a visão atual sobre o tema é fragmentada, uma vez que a literatura aborda a governança de dados com foco em domínios de decisão específicos, como qualidade de dados, segurança de dados e ciclo de vida de dados (Abraham, Schneider, vom Brocke, 2019).

A governança de dados assume contornos críticos dada a crescente necessidade de segurança e privacidade de dados dos cidadãos e empresas. A segurança de dados refere-se à preservação dos requisitos de segurança relativos à acessibilidade, autenticidade, disponibilidade, confidencialidade, integridade, privacidade e confiabilidade dos dados (Gunduz, Das, 2020). Estratégias envolvendo a prevenção do vazamento e garantia da privacidade passaram a estar no centro das preocupações da sociedade civil e dos formuladores de políticas devido a diversos episódios recentes de violação e vazamentos em todo mundo.

A definição de governança de dados realizada por Abraham, Schneider, vom Brocke (2019) possui seis dimensões. Em primeiro lugar, a governança de dados é um esforço interorganizacional, ou seja, requer a colaboração entre distintas organizações que realizam algum trabalho com dados. Em segundo lugar, a governança de dados é um *framework*, que fornece estrutura e formalização para a gestão dos dados. Em terceiro lugar, a governança de dados se concentra nos dados como um ativo estratégico da organização (pública ou privada). Em quarto lugar, a especificação de governança de dados regula sobre os direitos de decisão e *accountability* da tomada de decisão de uma organização sobre seus dados. Ela determina quais decisões precisam ser tomadas sobre dados, como essas decisões são tomadas e quem na organização tem o direito de tomar essas decisões. Em quinto lugar, a governança de dados desenvolve políticas, padrões e procedimentos de dados. Esses mecanismos institucionais devem ser coerentes com a estratégia da organização, de modo a promover com-

portamentos desejáveis para o uso de dados. Finalmente, a governança de dados monitora o *compliance*, e inclui a implementação de controles para garantir que as políticas e normas relacionadas a dados sejam cumpridas e produzam o resultado esperado, sendo importante considerar que os autores ressaltam a diferença entre governança de dados e gestão de dados. A governança de dados refere-se a quais decisões devem ser tomadas e quem toma essas decisões, enquanto a gestão de dados é sobre tomar essas decisões como parte da execução diária das políticas de governança de dados (Abraham, Schneider, vom Brocke, 2019).

Governança de dados é um tópico central frente às inovações digitais contemporâneas, mas deve estar apoiada em valores que justificam as arquiteturas institucionais. Nesse caso, o valor público da privacidade dos cidadãos é fundamental para justificar a governança de dados. Privacidade é um conceito normativamente dependente, significando o direito à reserva de informações pessoais como um direito fundamental de liberdade. A privacidade pode ser um conceito indescritível (Hallinan, Friedewald, McCarthy 2012; Hartzog 2021), significando muitas coisas ao mesmo tempo. Como Solove observou, "a privacidade não é uma coisa, mas um conjunto de muitas coisas distintas, porém relacionadas" (Solove, 2008:40)[1]. Em geral, a privacidade de dados envolve a expectativa adequada de privacidade de um indivíduo em relação aos dados pessoais e o controle sobre quem tem acesso a eles, incluindo governos e corporações. Leis de proteção de dados apoiam-se no direito fundamental à privacidade dos cidadãos como um elemento que legitima inovações institucionais frente à inovação tecnológica.

Conceitualmente distinta é a proteção de dados, que se relaciona ao controle e gerenciamento técnico dessas informações (por exemplo, proteção de dados contra acesso não autorizado, gerenciamento de identidade e acesso) (Park, 2020:1458). Proteção de dados refere-se a um conjunto extensivo de procedimentos e estratégias para garantir que dados pessoais sejam acessados e utilizados de maneira adequada para atingir os objetivos incutidos em regras de privacidade e proteção, ao mesmo tempo que possibilite o desenvolvimento econômico e tecnológico. Neste ponto, há uma observação importante: leis de proteção de dados e da privacidade não são proibitivas com relação ao processo de coleta, armazenamento, processamento e compartilhamento de dados. Leis de proteção de dados criam desenhos institucionais regulatórios para impedir abusos e violações da privacidade dos cidadãos, associando a esses desenhos regulatórios estruturas de direitos de liberdade que fundamentam instrumentos de proteção (Blanke, Hiller, 2019).

Os mecanismos de proteção e governança de dados, justificados no direito fundamental de privacidade, respondem aos mecanismos de vigilância que emergem em governos e corporações, implicando, por um lado, uma lógica de direitos emergentes que surgem com o avanço de tecnologias disruptivas; por outro lado, a criação de uma arquitetura institucional que solidifica normas, cria regras e define estratégias para o tratamento de dados e a gestão dos riscos emergentes (Blanke, Hiller, 2019). A vigilância emergente no mundo contemporâneo é exercida por governos e corporações coletando dados em tempo real, traçando perfis de cidadãos e produzindo ações a partir das preferências, opiniões e perspectivas captados em dados diversos (Brayne, 2017). O mundo contemporâneo rotiniza a presença de artefatos de vigilância, os quais integram sistemas discretos a amplos conjuntos de dados, convergindo dispositivos, plataformas, algoritmos e bancos de dados para possibilitar um monitoramento mais sistêmico e abrangente da sociedade (Haggerty, Ericson, 2000).

A governança de dados especifica uma estrutura para o gerenciamento de dados como um ativo estratégico tanto de empresas quanto de governos. Pode-se afirmar que os dados passaram a ser entendidos como recursos de uso comum (*common-pool resources*), usando o conceito popularizado por Elinor Ostrom (Ostrom, 1990). O sentido de entender os dados de tal forma possibilita torná-los legítimos alvos de uma política pública, e não apenas como meros insumos para a formulação de políticas públicas diversas (tal como saúde, educação, previdência, etc.). Ao fazer isso, a estrutura de governança dispõe sobre direitos e responsabilidades para a tomada de decisão de uma organização sobre os dados. Além disso, a governança de dados formaliza políticas, padrões e procedimentos, e monitora a conformidade.

A inovação institucional com a LGPD no Brasil

Neste artigo, o foco essencial está na aplicação de tecnologias digitais em governos. A última década no Brasil representou um conjunto amplo de esforços no sentido de desenvolver a governança digital nas três esferas da federação. Governança digital é entendida como uma mudança estrutural de governos, os quais inovam processos de serviços públicos e desenhos de políticas públicas com o apoio de tecnologias disruptivas apoiadas em dados (Margetts, Dunleavy, 2013).

A política brasileira para inovação em governos é embasada na Estratégia Brasileira de Transformação Digital (EGD), iniciada em 2016 e revisada em 2020, conforme o Decreto 10.332/2020. A EGD prevê a plataformização

da administração pública, por meio da plataforma Gov.Br, associada à expansão do compartilhamento de dados na administração, regulada pelo Decreto 10.046/2020. A EGD também é regulada pela Lei 13.460/2017, que trata da proteção de direitos dos usuários do serviço público, e pela Lei do Governo Digital (Lei 14.129/2021). Associada à EGD, temos a Estratégia Brasileira de Inteligência Artificial, que difunde a estados e municípios os requisitos e práticas para o uso de inteligência artificial na administração pública, instituída pela Portaria 4979/2021, do Ministério de Ciência, Tecnologia e Inovação (MCTI). Por fim, a EGD é apoiada também no Plano Nacional de Internet das Coisas, instituído pelo Decreto 9854/2019, bem como a diversificação de tecnologias de *blockchain* para mercados, especialmente no Banco Central.

O desenho dessas políticas foi apoiado em diversos documentos da Organização para Cooperação e Desenvolvimento Econômico (OCDE), a qual difundiu práticas, *benchmarks* e princípios para o desenvolvimento tecnológico em governos (OCDE, 2014). Em especial, a OCDE formulou recomendações que apoiam o desenvolvimento de aplicações digitais com especial enfoque na plataformização do serviço público e no aprimoramento e aprofundamento da coleta, armazenamento, processamento e compartilhamento de dados para formular e implementar políticas públicas (Filgueiras, Palotti e Nascimento, 2022). Além do processo de difusão por parte da OCDE, o Banco Mundial difundiu uma perspectiva de governança de dados por meio do seu último relatório de desenvolvimento mundial (World Bank, 2021).

O Brasil tem avançado essa estratégia de inovação institucional em governos, difundindo entre estados e municípios, com apoio de organizações internacionais, a plataformização e os processos de coleta, armazenamento, processamento e compartilhamento de dados para apoiar a formulação de políticas públicas. O objetivo é criar novas dinâmicas de governo na gestão do serviço público e na formulação de políticas públicas baseadas em dados, seguindo a orientação da OCDE de um setor público digital pelo desenho (*digital by design*), dirigido por dados (*data-driven public sector*), com foco no usuário (*user driven*).

Nesse contexto – em que os objetivos da política de dados são facilitar a coleta, armazenamento, processamento e compartilhamento, incluindo as organizações públicas e privadas – o Congresso Nacional aprovou a Lei Geral de Proteção de Dados. A LGPD ampliou as possibilidades de privacidade e proteção de dados pessoais, além de criar procedimentos

relacionados à gestão de dados. A LGPD representou um momento crítico que exigiu que os formuladores de políticas passassem por todo um processo de calibração de instrumentos e ajuste dos objetivos e práticas da política de dados.

A LGPD teve um longo processo de agenda e formulação, iniciando no Projeto de Lei 4060/2012 da Câmara dos Deputados. Naquele momento, em 2012, a LGPD surgia como uma resposta a diferentes ordens de problemas do mundo digital, especialmente os escândalos de espionagem contra a Presidência da República e diversos abusos praticados em redes sociais e crimes virtuais. A Lei Carolina Dieckmann (Lei 12.737/2012) disciplinou os crimes virtuais, mas o consenso era o de que havia a necessidade de uma lei que disciplinasse a proteção de dados e a privacidade dos cidadãos[2]. O processo decisório avançou quando veio a público o escândalo Cambridge Analytica, que ressoou no processo eleitoral brasileiro com denúncias de manipulação indevida de dados obtidos em redes sociais.

A LGPD avançou em quatro aspectos centrais. Primeiro, ela regulamentou normas constitucionais, criando uma estrutura de direitos dos cidadãos em relação à sua titularidade de dados e autodeterminação informativa. A LGPD criou e inovou em direitos de cidadania, cobrindo diferentes aspectos do mundo digital. Segundo, a LGPD definiu claramente princípios para o tratamento e proteção de dados e da privacidade, os quais estabelecem uma ordem de valores públicos que orienta o trabalho com dados, cobrindo a coleta, armazenamento, processamento e compartilhamento. Terceiro, a LGPD definiu uma estrutura de governança de dados, estabelecendo atores e responsabilidades regulatórias. A LGPD criou a figura do controlador de dados e do encarregado de dados, cobrindo o setor público e o setor privado. A LGPD definiu também a autoridade regulatória por meio da Autoridade Nacional de Proteção de Dados, e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, assegurando representação da sociedade civil e estruturas representativas para aconselhamento e difusão de boas práticas. Quarto, a LGPD definiu regras para tratamento de dados, cobrindo procedimentos, permissões e proibições, assim como padrões de segurança de dados, processos de comunicação e transferência internacional de dados. O Quadro 1, a seguir, sintetiza os avanços da LGPD.

Quadro 1
Síntese das Inovações da LGPD

Elementos	Atributos	Definição normativa
Princípios	Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades
	Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento
	Necessidade	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados
	Livre acesso	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais
	Qualidade dos dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
	Transparência	Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial
	Segurança	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão
	Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais
	Não discriminação	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos
	Accountability	Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas

Quadro 1
Síntese das Inovações da LGPD (cont.)

Elementos	Atributos	Definição normativa
Governança	Definição da titularidade de dados	Definição dos titulares de dados como pessoas naturais a quem se referem os dados pessoais que são objeto de tratamento.
	Definição do controlador de dados e encarregado de dados	Definição de atribuições institucionais e responsabilidades em relação a conjuntos de dados sob seu controle.
	Conselho Nacional de Proteção de Dados Pessoais e da Privacidade	Constituição de conselho com a atribuição de promover boas práticas de proteção de dados, diretrizes estratégicas, elaborar estudos e propor ações para a Autoridade Nacional de Proteção de Dados (ANPD)
	Autoridade Nacional de Proteção de Dados	Constituição de autoridade regulatória, com poder fiscalizatório sobre proteção de dados e promoção da privacidade.
Direitos	Privacidade	Definição como direito fundamental de liberdade.
	Autodeterminação informativa	Garantia de titularidade dos dados e poder para consentir ou revogar consentimento com relação ao tratamento de dados.
	Liberdade de expressão, de informação, de comunicação e de opinião	Reconhecimento do uso de dados para a liberdade de expressão, de informação, de comunicação e opinião.
	Inviolabilidade da intimidade, da honra, da imagem	Reconhecimento da intimidade honra e imagem como direitos invioláveis por parte de controladores de dados.
	Desenvolvimento econômico e tecnológico	Possibilidades de uso de dados em políticas públicas e formas de uso de dados para o desenvolvimento econômico.
	Livre iniciativa, livre concorrência, defesa do consumidor	Regras para estabelecer liberdade econômica para coleta, armazenamento, processamento e compartilhamento de dados respeitados os requisitos da LGPD
	Direitos humanos	Reconhecimento dos direitos humanos como elemento central da proteção de dados e da privacidade.

Quadro 1
Síntese das Inovações da LGPD (cont.)

Elementos	Atributos	Definição normativa
Regras de proteção de dados	Definição de requisitos para tratamento de dados pessoais	Requisitos de consentimento de titulares de dados, obrigações regulatórias pelo controlador de dados, permissões para cumprimento de obrigações legais ou para a administração pública desenhar políticas públicas.
	Definição de requisitos para tratamento de dados pessoais sensíveis	Requisitos para tratamento de dados sensíveis, proibições com relação a dados de saúde, regras para tratamento de dados de crianças e adolescentes,
	Transferência internacional de dados	Definição de regras e instrumentos regulatórios para o compartilhamento de dados além do território nacional.
	Segurança e sigilo de dados	Regras para a segurança da informação e definição de sigilo.
	Anonimização	Definição dos requisitos de anonimização de dados pessoais, incidindo no processamento sem identificação pessoal.
	Comunicação de incidentes de dados	Regras de comunicação entre os responsáveis pela proteção de dados em casos de incidentes como vazamentos ou tratamento inadequado de dados.
	Término do tratamento de dados	Regras para eliminação de dados após o término do tratamento de dados em função do alcance da finalidade, fim do período de tratamento, revogação do consentimento com relação ao tratamento por parte do titular, ou determinação de autoridade nacional.

Fonte: Elaboração própria

Como resultado, cabe destacar que a partir da LGPD, a Emenda Constitucional 115/2022 constitucionalizou a proteção de dados como direito fundamental, incluindo no Art. 5º da Constituição Federal o inciso LXXIX, onde se lê que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais". A Emenda 115 acrescentou, também, o inciso XXVI no Art. 21 da Constituição Federal, dando competência para a União organizar e fiscalizar a proteção e tratamento de dados pessoais. Por fim, acrescentou o inciso XXX ao Art. 22 da Constituição Federal, dando competência exclusiva para a União legislar sobre a matéria. A Emenda 115/2022 estabeleceu a proteção de dados como direito

fundamental, definiu competência da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais, e deu competência legislativa para a União para legislar sobre proteção e tratamento de dados pessoais.

Embora a LGPD seja bastante ampla com relação às definições técnicas e jurídicas da proteção de dados, ela estabeleceu exceções com relação à necessidade de proteção. Conforme o Art. 4º da LGPD, nos casos em que o tratamento de dados pessoais seja feito por pessoa natural para fins exclusivamente privados, jornalístico ou artístico, acadêmico, ou para fins de segurança pública, defesa nacional, segurança do Estado e atividade de repressão e investigação penal, os termos da Lei não se aplicam.

Diante dessas inovações institucionais, o surgimento da LGPD criou uma situação que obriga as organizações públicas – incluindo a administração direta, indireta, fundacional e empresas públicas – a redesenharem suas políticas de dados. No Brasil, dada a estrutura federativa trina, a LGPD não se estende apenas à União, mas também aos entes subnacionais – estados e municípios. Conforme já referenciado, já existem estudos que observam de que forma o desenho da governança de dados se desenvolveu no Brasil nos últimos anos, em especial após o advento da LGPD (Filgueiras, Fernandes, Palotti, 2019; Filgueiras, Lui, 2023). Contudo, ainda há uma carência de estudos que observem o desenho institucional adotado pelos entes subnacionais. A presente pesquisa visa contribuir com uma dimensão desse processo, enfatizando os estados da federação.

Os governos estaduais necessitam de dados precisos, relevantes e oportunos para tomada de decisão e construção de políticas públicas, ao mesmo tempo que crie uma infraestrutura de dados protegida e que respeite aos direitos fundamentais da cidadania. A forma como cada estado regulamenta a LGPD e estabelece suas próprias regras de governança de dados revela quais estratégias são utilizadas para a construção do respectivo enquadramento. Tradicionalmente, estados possuem pouca autonomia legislativa para inovar em relação às regras impostas pela União (Couto, Absher-Bellon, 2018). No caso da proteção de dados e da privacidade, essa competência é privativa da União, nos termos da Emenda Constitucional 115/2022.

No que tange à LGPD, não se espera que os governos estaduais inovem no sentido de propor uma nova lei de proteção de dados, mas que traduzam as diretrizes da lei em estratégias práticas para orientar seus próprios processos de coleta, armazenamento, uso e compartilhamento de dados, assim como assegurar mecanismos de proteção e cumprimento

de direitos fundamentais. O que se espera, a partir da regulamentação da LGPD, é que os estados tracem suas próprias diretrizes estratégicas para a coleta, compartilhamento e uso de dados (Carroll *et al.*, 2019). Nesse sentido, o presente artigo busca compreender tais estratégias contidas nos enunciados institucionais a partir da ferramenta analítica e metodológica conhecida como *Institutional Grammar Tool*.

Estratégia analítica e metodológica

Do ponto de vista da construção de uma política de dados pelos estados brasileiros, com vistas a regulamentar a forma como o próprio ator estatal efetiva a LGPD, a abordagem conhecida como desenho de políticas públicas, ou *policy design*, pode ser de grande valor analítico. Entendido de forma geral, o governo visa implementar metas de forma eficaz e eficiente e, na fase de formulação, os formuladores de políticas definem os instrumentos para atingir seus objetivos (Capano, Howlett, 2020). O conceito de desenho de políticas analisa de que forma as estruturas formais de uma política pública são criadas e interagem entre si, produzindo efeitos e implicações na relação entre os cidadãos e o Estado (Lima, Aguiar, Lui, 2021). A perspectiva do desenho confere atenção especial aos instrumentos de política, que são definidos como a caixa de ferramentas a partir da qual os governos devem escolher na construção ou criação de políticas públicas (Capano, Howlett, 2020). Assim, a seleção de instrumentos de política ocorre dentro de um contexto mais amplo que contém instituições, atores e práticas e que afetam o processo de formulação.

Nesse sentido, voltando à definição de governança de dados, ou seja, o exercício da autoridade e controle sobre a gestão dos dados, questiona-se como os governos estaduais no Brasil construíram a sua própria estratégia de governança após o advento da LGPD. Mais especificamente, questiona-se de que forma é designado, a nível estadual, o amplo leque de responsabilidades e competências sobre a governança de dados, procedimentos para proteção e efetivação de direitos fundamentais, qual é o papel que cabe aos cidadãos nesse processo e qual tipo de constrangimentos institucionais foram dispostos em forma de regulamento.

Para isso, usaremos a lente analítica conhecida como *Institutional Grammar Tool* (IGT), ou ferramenta de gramática institucional, para compreender o desenho da política de governança de dados nos governos estaduais brasileiros. Crawford e Ostrom (1995) propuseram uma

ferramenta analítica voltada ao estudo da gramatica institucional que pudesse servir para examinar instituições, definidas como regras, normas e estratégias, como parte do *Institutional Analysis and Development Framework* (IAD). A proposta das autoras contribuiu para compreender como as instituições criam regularidades referentes à ação humana e como a gramática institucional permite conhecer a respeito das estratégias adotadas pelos atores em relação a cada instituição.

No quadro teórico proposto por Crawford e Ostrom (1995), a estrutura gramatical de normas, regras e estratégias ocupam um ponto central de análise institucional. Nesse sentido, as autoras ofereceram uma abordagem prática para analisar as instituições e criar as categorias para a posterior discussão. O desenvolvimento seguinte do framework desenvolvido pelas autoras é conhecido como *Institucional Grammar Tool,* ou pela sua sigla IGT.

Instituições estão embutidas em estruturas linguísticas que são interpretadas e cristalizadas pelos atores a partir dos enunciados prescritos. Os enunciados institucionais são definidos por Crawford e Ostrom (1995:583) como a restrição ou oportunidade linguística compartilhada que prescreve, permite ou aconselha ações ou resultados para os atores (individuais ou coletivos). Segundo as autoras, os enunciados institucionais (*institucional statements*) são falados, escritos ou tacitamente compreendidos de uma forma inteligível para os atores em um cenário empírico.

Nos últimos anos, muitos estudos contribuíram para avançar no trabalho de Crawford e Ostrom e a gramática institucional foi transformada em uma ferramenta analítica de maior potência (Basurto *et al.*, 2010; Dunlop *et al.*, 2021; Siddiki *et al.*, 2011; 2012; 2022; Watkins, Westphal, 2016). Uma parte da aplicação dessa teoria foi usada para analisar políticas regulatórias (Siddiki *et al.*, 2012) e outras para investigar políticas ambientais (Watkins, Westphal, 2016). Como argumentam Siddiki *et al.* (2012), o desafio de pesquisa envolve desenvolver uma desconstrução sistemática dos elementos escritos (por exemplo, populações-alvo, requisitos, sanções, condições) dentro de normas, regras e estratégias. De acordo com os autores, os componentes regulatórios podem ser extensos, multifacetados e interativos, compreendendo dezenas de enunciados que proíbem, permitem e requerem ações específicas de populações alvo em determinadas situações.

Siddiki *et al.* (2022) observaram, no entanto, que o quadro proposto por Ostrom e Crawford continha algumas fragilidades em termos de instruções específicas para colocar em prática a gramática institucional. Por isso, segundo eles, o IGT foi deixado de lado no debate principal da análise institucional por quase uma década. Por esse motivo, Basurto *et al.* (2010) propuseram alguns ajustes no framework. O IGT criou uma abordagem para dividir os componentes das instituições formais. Como Basurto *et al.* (2010) observaram, um dos principais desafios na aplicação de teorias institucionais aos ambientes políticos é traduzir conceitos-chave em estratégias confiáveis para observação, e o IGT permite que os pesquisadores superem essa barreira. Como descrito por Siddiki *et al.* (2012), os enunciados institucionais são compostos por sentenças únicas dentro das instituições e correspondem às diretrizes individuais que indicam uma gama de componentes como: um ator, uma ação específica, o sentido temporal, os limites da atividade. (Siddiki *et al.*, 2012).

Após a identificação dos enunciados institucionais dentro de uma determinada regra, as declarações são descritas em seis componentes: (i) atributo (*attribute*), ou os agentes(s) encarregados de realizar a ação específica; (ii) objeto (*object)*, a parte animada ou inanimada do enunciado que é o receptor de uma ação; (iii) operador deôntico (*deontic*), o operador prescritivo que especifica se uma ação é necessária, permitida ou proibida; (iv) alvo (*aim*), ou a ação em si; (v) condições (*conditions*), que especificam os limites espaciais, temporais e/ou processuais nos quais a ação em questão deve ser realizada; e (vi) consequência (*or else*), as sanções punitivas associadas à não realização de uma ação conforme prescrito (Dunlop *et al.*, 2021; Siddiki *et al.*, 2012; 2022; Watkins, Westphal, 2016). A sigla para a referida taxonomia é ADICO. É importante registrar que Siddiki *et al.* (2011) adicionaram um componente de sintaxe ao ADICO. O "objeto" permite aos pesquisadores discernir ainda mais entre quem conduz o enunciado institucional e quem ele afeta, permitindo a aplicação do IAD em uma ampla gama de objetos empíricos de pesquisa. A desconstrução dos enunciados institucionais diversos dentro de uma norma, regra ou estratégia compartilhada pode ser resumida conforme o Quadro 2 a seguir:

Quadro 2
Elementos Sintáticos da Gramática Institucional

Elementos de sintaxe	Conceito
Atributo (*Attribute*)	O componente Atributo captura o ator responsável por um determinado enunciado institucional, seja de forma explícita ou implícita. Além disso, em alguns enunciados, um Atributo e suas propriedades podem ser apresentados juntos. Por exemplo, um enunciado pode se referir a "agricultores" ou a "agricultores certificados" ou a "agricultores certificados e em conformidade". Nesses exemplos, o substantivo "agricultores" retransmite o ator geral ao qual a declaração se aplica, e "conformidade" e "certificado" são propriedades desse ator.
Operador deôntico (*Deontic*)	O componente operador deôntico baseia-se nas operações modais usadas na lógica deôntica para distinguir enunciados prescritivos de não prescritivos. O conjunto completo de operadores deônticos, D, consiste em P permitido, O obrigatório, e F. proibido.
Alvo (*Aim*)	O alvo é a descrição específica de uma parte ativa em uma situação de ação à qual se refere um enunciado institucional. Ou seja, qual ação é obrigatória, permitida ou requerida do atributo?
Objeto (*Object*)	O componente Objeto é definido como o receptor de uma ação (descrita pelo Objetivo) e executada pelo ator (descrita pelo Atributo). Objetos podem ser entidades animadas e inanimadas em enunciados institucionais, e cada enunciado pode conter vários objetos.
Condição (*Condition*)	Condições indicam o conjunto de variáveis que definem quando e onde um enunciado institucional se aplica. Por exemplo, as condições para um enunciado institucional podem indicar quando ele se aplica, como durante certas condições meteorológicas, em um horário definido ou em uma etapa específica de algum processo.
Consequência (*Or else*)	O componente final de nossa sintaxe institucional é a consequência que um enunciado institucional atribui ao descumprimento detectado com os outros componentes desse enunciado. Em alguns casos, a consequência especifica uma série de punições possíveis se uma regra não for seguida.

Fonte: Siddiki *et al.,* 2011.

Um ponto importante dessa estratégia analítica é a distinção que Crawford e Ostrom fazem a respeito dos tipos de instituições. Instituições são definidas como normas, regras e estratégias que moldam a ação humana (Crawford, Ostrom, 1995). A diferença entre estes três tipos diz respeito ao tipo de enunciado institucional. O enunciado institucional referente a normas prescreve ações aos atores em um nível constitucional, mais

orientado para a estrutura de valores e direitos que informam a ação. O enunciado institucional referido a regras define as escolhas coletivas de políticas. Necessariamente as regras apresentam todos os elementos da sintaxe institucional, em termos de sua completude gramatical. Por fim, as estratégias estão em um nível operacional, que reconhece os valores embutidos em normas e as escolhas coletivas definidas em regras para efetivamente moldar a ação dos atores (Ostrom, 2005:177).

O método de análise institucional proposto pelo IGT tem limitações. Essencialmente, ele é descritivo da arquitetura institucional, permitindo analisar o desenho de uma determinada política pública, cobrindo suas estratégias, regras e normas. O IGT não é um *framework* analítico centrado nos atores e nas dinâmicas de design que constroem as instituições. Embora a o IAD seja centrado nos atores, o IGT é uma estratégia para analisar o desenho institucional em si, tendo limitações quanto às escolhas sociais e uma epistemologia ou ontologia das instituições. Embora existam essas limitações, a análise do desenho institucional da proteção de dados e da privacidade pode ser potencializada com o IGT.

Para entender os elementos das regulamentações estaduais da LGPD, este artigo utiliza a ferramenta de gramática institucional (IGT) para desconstruir os decretos de regulamentação em enunciados institucionais. Regulamentações de lei definem uma estratégia operacional, como destacado anteriormente. Entende-se que a regulamentação estadual da LGPD constitui um interessante corpus de investigação dado que, a partir de sua análise, é possível entender o *framework* organizacional referente à governança de dados nos estados e os termos em que os atores estaduais reconhecem e cumprem direitos fundamentais de proteção de dados e privacidade.

Assim, foram coletados os decretos estaduais que regulamentam a LGPD em 15 estados da federação e o do Distrito Federal. Estes decretos foram decompostos em diferentes enunciados institucionais, os quais foram classificados, categorizados e analisados constituindo uma base de dados em termos do IGT. A coleta de dados se deu entre os meses de março e abril de 2022.

A desconstrução dos enunciados institucionais implicou em separar cada artigo no texto de cada decreto regulamentador da LGPD dos estados. Cada artigo foi classificado a partir dos componentes que constituem o IGT, descritos acima. O Quadro 3, a seguir, especifica a classificação proposta, de forma a descrever os enunciados institucionais.

Quadro 3
Classificação dos Enunciados Institucionais das Regulamentações Estaduais da LGPD

Componentes	Categorias
Atributo	• Cidadãos e usuários • Empresas • Encarregado de dados • Controlador de dados • Operador de dados • Governos municipais • Governos estaduais • Governo federal • Organizações da sociedade civil • Agência reguladora • Conselhos, comissões ou organizações equivalentes • Organizações internacionais
Operador deôntico	• Permissão • Obrigação • Proibição • Revogação/anulação
Alvo	• Competência • Coleta e processamento de dados • Compartilhamento de dados • Certificação e conformidade • Autorização • Monitoramento • Padronização • Direitos
Objeto	• Governança • Gestão e processos • Produto • Serviço • Recursos naturais
Condição	• Prazos e condições determinados • Prazos e condições indeterminados
Consequência	• Multas • Suspensão de atividade • Cassação

Fonte: Elaboração própria.

O componente atributo especifica a quem um determinado enunciado institucional é aplicado. Dito isso, definimos tipos de atores a quem uma determinada ação pode ser atribuída. Neste primeiro componente, enten-

demos que as ações de proteção de dados e da privacidade nos estados podem ser atribuídas aos tipos de atores elencados no Quadro 3. O operador deôntico especifica o conector lógico do enunciado institucional, podendo ser uma permissão, obrigação ou proibição. Conhecendo a estrutura dos decretos analisados, incluímos nesse componente a categoria revogação/anulação, quando um determinado enunciado institucional revogar outros atos normativos. O terceiro componente diz respeito ao alvo, ou seja, à ação requerida dos atores a quem foi atribuído um enunciado institucional. Nesse componente, classificamos ações típicas requeridas dos atores atribuídos e da governança de dados, tais como competências institucionais, coleta e processamento de dados, compartilhamento de dados, certificação e conformidade dos atores, autorizações para tratamento de dados que são expedidas, monitoramento da política de dados, ações de padronização de processos e de dados, questões relativas a direitos.

O componente objeto refere-se àquilo que recebe a ação descrita no alvo. Classificamos os enunciados institucionais nesse componente compreendendo o que recebe a ação descrita, sendo a governança em si, na definição de seus princípios e práticas, a gestão e processos que criam procedimentos relativos a quem, quando, onde e como coleta, armazena, processa e compartilha dados. Ainda nesse componente, classificamos questões relativas a produtos, serviços e questões que envolvam recursos naturais como categorias que podem estar envolvidas na governança dos dados. Condição é o componente que descreve quando e onde o enunciado institucional deve ser cumprido. Como se trata de decretos regulamentadores, classificamos este componente a partir do momento que eles especifiquem ou não prazos e condições para que os atores cumpram com o enunciado. Por fim, classificamos o componente consequência a partir das categorias multas, suspensão de atividade e cassação. Este último componente especifica as consequências caso os atores atribuídos ao enunciado institucional não cumpram com o alvo pretendido.

Compreendendo esses componentes do IGT, analisamos os decretos regulamentadores da LGPD nos estados como estratégias para realizar um empreendimento coletivo das administrações públicas. De acordo com Ostrom (2005), estratégias são ideias compartilhadas que orientam a ação coletiva, envolvendo atores para realizar e instrumentalizar um empreendimento comum. Partimos da premissa que os decretos regulamentadores especificam estratégias das administrações públicas

estaduais para regulamentar e lidar com os problemas que emergem com a LGPD. Assim, o resultado da análise aqui realizada não pretende tipificar a estratégia, mas produzir conclusões empíricas que indiquem o estado da arte da regulamentação da LGPD nos estados da federação.

O exame de cada decreto regulamentador da LGPD foi feito qualitativamente, desconstruindo cada artigo de cada decreto coletado. Cada artigo foi desconstruído nos componentes do IGT e cada componente identificado foi classificado nas categorias elencadas no Quadro 3. Foi feita uma primeira rodada de classificação e depois a conferência e validação externa realizada por membros do CONACI – Conselho Nacional de Controle Interno –, o qual é uma rede das Controladorias-Gerais dos estados. Os resultados obtidos estão apresentados na próxima seção.

Resultado

Identifica-se, na Tabela 1, que o número de enunciados institucionais dos decretos estaduais que regulamentam LGPD variam de estado para estado. Em alguns estados, como Santa Catarina e Piauí, vê-se uma regulamentação extremamente simplificada e curta. Enquanto isso, outros estados apresentam documentos robustos, ricos no sentido de possuírem definições e estabelecerem as regras e procedimentos para a proteção de dados.

Outro ponto importante é que apenas 16 estados brasileiros regulamentaram a LGPD até o primeiro semestre de 2022, época da coleta de dados da pesquisa. Há, nesse sentido, uma grande diferença regional. Enquanto os estados da Região Sul e Sudeste regulamentaram a LGPD, em outros estados a configuração é mais heterogênea. Na Região Norte, apenas Rondônia e Amapá regulamentaram a LGPD, enquanto os decretos dos estados do Acre, Amazonas, Pará, Roraima e Tocantins não foram encontrados nos sites oficiais. Na Região Centro-Oeste, apenas o estado do Mato Grosso não apresenta regulamentação da LGPD, enquanto os demais apresentam. Na Região Nordeste, identifica-se que Bahia, Alagoas, Rio Grande do Norte, Ceará e Maranhão não regulamentaram a LGPD. Contudo, foram encontrados documentos nos estados do Piauí, Pernambuco, Paraíba e Sergipe.

Tabela 1
Número de Enunciados Institucionais nos Documentos Estaduais de Regulamentação da LGPD, por Estado, 2022.

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	AP	51	10,3	10,3	10,3
	DF	33	6,7	6,7	17,0
	ES	44	8,9	8,9	25,9
	GO	22	4,5	4,5	30,4
	MG	31	6,3	6,3	36,6
	MS	21	4,3	4,3	40,9
	PB	19	3,8	3,8	44,7
	PE	30	6,1	6,1	50,8
	PI	5	1,0	1,0	51,8
	PR	51	10,3	10,3	62,1
	RJ	28	5,7	5,7	67,8
	RO	38	7,7	7,7	75,5
	RS	37	7,5	7,5	83,0
	SC	12	2,4	2,4	85,4
	SE	46	9,3	9,3	94,7
	SP	26	5,3	5,3	100,0
	Total	494	100,0	100,0	

Fonte: Elaboração dos autores.

Passaremos, a seguir, para a análise dos dados conforme o instrumento analítico ADICO, proposto pelo IGT.

Atributo

Em relação ao atributo, ou seja, o ator a quem um enunciado institucional atribui permissões, proibições ou requerimento de ação, verifica-se que a administração pública estadual ocupa o lugar central quando se analisam todos os documentos estaduais presentes no *corpus* de pesquisa. Ou seja, 44,1% dos enunciados institucionais atribuem para a administração pública estadual permissões, proibições ou requerimentos de ação. Em segundo lugar, verifica-se a existência de conselhos, comissões ou organizações equivalentes, responsáveis por conduzir a estratégia de governança de dados estaduais, perfazendo 19,4% dos enunciados

institucionais. Na esteira, seguem as figuras previstas pela LGPD por instrumentalizar a governança de dados – o controlador, o encarregado e o operador de dados. Verifica-se, por outro lado, um papel diminuto reservado aos cidadãos e às empresas privadas. Esse dado mostra que a estrutura de proteção de dados nos governos estaduais brasileiros é eminentemente endógena, ou seja, valoriza muito os próprios atores estatais, instalados na burocracia governamental e reserva pouco espaço para cidadãos e empresas.

Tabela 2
Frequência da Categoria Atributo, por Tipo, nos Documentos Estaduais de Regulamentação da LGPD, 2022

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	Administração pública estadual	218	44,1	44,1	44,1
	Cidadãos e usuários	30	6,1	6,1	50,2
	Conselho, comissões ou organizações equivalentes	96	19,4	19,4	69,6
	Controlador de dados	20	4,0	4,0	73,7
	Empresas	29	5,9	5,9	79,6
	Encarregado de dados	70	14,2	14,2	93,7
	Governo Federal	3	,6	,6	94,3
	Operador de dados	28	5,7	5,7	100,0
	Total	494	100,0	100,0	

Fonte: Elaboração dos autores

De forma ilustrativa, podemos citar o caso do Decreto Nº 47.826 de 11/11/2021, do Governo do Estado do Rio de Janeiro. No Decreto, lê-se que

> Os órgãos e as entidades da Administração Pública do Poder Executivo podem efetuar o uso compartilhado de dados pessoais com outros órgãos e entidades públicas para atender a finalidades específicas de execução de políticas públicas, no âmbito de suas atribuições legais, observados os princípios de proteção de dados pessoais elencados no art. 6º da Lei Federal nº 13.709, de 2018.

Nesse caso, verifica-se que o atributo do enunciado institucional dispõe sobre a forma como a própria administração pública irá operar a política.

Operador deôntico

O operador deôntico se refere à lógica das normas, no sentido de identificar o que é obrigatório, permitido ou proibido. Adicionamos também a categoria revogação e anulação, dado que ambas produzem os mesmos efeitos dos operadores deônticos clássicos. Nesse caso, não foi encontrado nenhum enunciado institucional que revogue ou anule outros dispositivos normativos. Verifica-se que o maior percentual de operadores deônticos usados referem-se ao sentido de obrigação, requerendo ações por parte dos atores a quem foi atribuído um enunciado institucional. Em segundo lugar aparece o operador ligado à permissão e, apenas em terceiro, proibição. Depreende-se desse dado que toda a estrutura institucional dos governos estaduais brasileiros no que tange à construção de estratégias de proteção de dados e implementação da LGPD estão, basicamente, restritas à obrigação.

Associado com o que foi identificado na Tabela 2, onde os governos estaduais figuram entre os principais atores no processo, pode-se dizer que o arranjo institucional estadual envolve a lógica de distribuição de obrigações aos próprios governos estaduais, novamente, reforçando o caráter endógeno da estratégia, pouco aberta à presença de atores não estatais e ao disciplinamento de suas respectivas atividades. As estratégias adotadas pelos documentos analisados não revelam uma preocupação maior em estabelecer proibições e pouco se referem a direitos dos cidadãos, reproduzindo mais uma lógica de controle sobre a ação das administrações públicas estaduais com relação a dados.

A contagem de operadores ligados à ideia de revogação e anulação demonstra um baixo número de casos, considerando que a regulamentação da LGPD é recente.

Tabela 3
Frequência da Categoria Operador Deôntico, por Tipo, nos Documentos Estaduais de Regulamentação da LGPD, 2022

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	Obrigação	412	83,4	83,4	83,4
	Permissão	65	13,2	13,2	96,6
	Proibição	17	3,4	3,4	100,0
	Total	494	100,0	100,0	

Fonte: Elaboração dos autores.

De forma elucidatória, podemos citar o caso do Decreto nº 55.987 de 7/07/2021, do Governo do Estado do Rio Grande do Sul, em que lê-se:

> O Grupo de Trabalho sobre a Implementação da LGPD no Poder Executivo Estadual poderá detalhar as diretrizes de que trata este artigo, por meio de esclarecimentos compartilhados com a Rede de Encarregados em Caderno de Orientações disponibilizados em plataforma digital.

Nesse sentido, verifica-se que o enunciado institucional cria a possibilidade de criação de um material informativo e orientativo acerca da LGPD em âmbito da administração pública. Novamente, reitera-se o caráter endógeno da política.

Em sentido oposto, lê-se no Decreto nº 48.237 de 22/07/2021, editado pelo Governo do Estado de Minas Gerais, que "É vedado aos órgãos e às entidades da Administração Pública do Poder Executivo transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto (...)". Nesse caso, identifica-se um enunciado institucional no sentido proibitivo.

Tabela 4
Tabulação Cruzada da Categoria Atributo com o Operador Deôntico

		Operador deôntico			Total
		Obrigação	Permissão	Proibição	
Atributo	Administração pública estadual	189	20	9	218
	Cidadãos e usuários	21	9	0	30
	Conselho, comissões ou organizações equivalentes	82	10	4	96
	Controlador de dados	19	1	0	20
	Empresas	18	11	0	29
	Encarregado de dados	64	2	4	70
	Governo Federal	2	1	0	3
	Operador de dados	17	11	0	28
Total		412	65	17	494

Fonte: Elaboração própria

Alvo

O alvo refere-se na ação ao ponto que a norma pretende regular, ou seja, o que se pretende regular. Verifica-se que os alvos dos enunciados institucionais estão, em sua maioria, voltados à ideia de certificação e conformidade. Em segundo plano, está preocupado em distribuir competências. De forma menor, o alvo se volta à questão de compartilhamento de dados, coleta e processamento de dados, autorização, direitos e monitoramento. Essa característica deve-se pelo fato de que a própria LGPD é uma lei que, eminentemente, dispõe sobre processos e conformidade, e não necessariamente em relação à entrega de um produto/serviço à população.

Outro ponto que merece destaque refere-se ao fato de que as estratégias de proteção de dados nos governos estaduais brasileiros estão fortemente voltadas às questões procedimentais, dado que majoritariamente se preocupam com certificação e conformidade e estão menos preocupadas com a questão do uso dos dados para a construção de políticas públicas e soluções para problemas de gestão pública. A afirmação decorre devido ao fato de que os enunciados que apresentam alvos voltados às atividades típicas de uso de dados para a gestão pública (compartilhamento de dados,

autorização, coleta e processamento) aparecem de forma muito tímida nos documentos analisados. A categoria "não categorizado" significa que alguns enunciados institucionais (16) não têm um alvo definido.

Tabela 5
Frequência da Categoria Alvo, por Tipo, nos Documentos Estaduais de Regulamentação da LGPD, 2022

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	Não categorizado (*missing*)	16	3,2	3,2	3,2
	Autorização	5	1,0	1,0	4,3
	Certificação e conformidade	273	55,3	55,3	59,5
	Coleta e processamento de dados	31	6,3	6,3	65,8
	Compartilhamento de dados	39	7,9	7,9	73,7
	Competência	105	21,3	21,3	94,9
	Direitos	3	,6	,6	95,5
	Monitoramento	2	,4	,4	96,0
	Padronização	20	4,0	4,0	100,0
	Total	494	100,0	100,0	

Fonte: Elaboração própria

Um exemplo de uso da categoria alvo nos decretos estaduais pode ser observado no Decreto 40.006 de 5 de outubro de 2021 do Estado de Sergipe. Nele, averígua-se:

> Os órgãos e entidades do Poder Executivo Estadual, de que trata o art. 1º deste Decreto, deverão providenciar a adequação de suas páginas e plataformas tecnológicas para atender ao disposto na LGPD, em prazo a ser definido pelo CGPEPDP (Conselho de Governança da Política Estadual de Proteção de Dados Pessoais).

Nesse sentido, o alvo refere-se à ideia de padronizar e adequar, atrelado à ideia de certificação e conformidade.

Em outro caso, no Decreto 55.987 de 7/07/2021, editado pelo Governo do Estado do Rio Grande do Sul, verifica-se que o alvo é o próprio compartilhamento de dados. Lê-se, no respectivo decreto, que

> Os dados deverão 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.

Tabela 6
Tabulação Cruzada da Categoria Atributo com o Alvo

		Alvo									
		Não categorizado	Autorização	Certificação e conformidade	Coleta e processamento de dados	Compartilhamento de dados	Competência	Direitos	Monitoramento	Padronização	Total
Atributo	Administração pública estadual	5	4	119	6	23	42	0	2	17	218
	Cidadãos e usuários	6	0	12	4	5	0	3	0	0	30
	Conselho, comissões ou organizações equivalentes	2	1	61	0	1	31	0	0	0	96
	Controlador de dados	1	0	10	1	0	7	0	0	1	20
	Empresas	2	0	13	6	5	3	0	0	0	29
	Encarregado de dados	0	0	47	0	5	17	0	0	1	70
	Governo Federal	0	0	2	0	0	0	0	0	1	3
	Operador de dados	0	0	9	14	0	5	0	0	0	28
	Total	16	5	273	31	39	105	3	2	20	494

Fonte: Elaboração própria

Objeto

O objeto é o receptor de uma ação e executada pelo ator, descrito no atributo. A análise do objeto reforça a tese do que foi apontado anteriormente, visto que a maioria dos enunciados institucionais estão voltados à gestão de processos e governança, e os que denotariam um uso estratégico pela gestão pública estadual para a construção de soluções baseadas em dados (produto e serviço) aparecem de forma diminuta, conforme se identifica na Tabela 7. A categoria "não categorizado" significa que 15 enunciados institucionais não têm um objeto definido, representando sentenças incompletas.

Tabela 7
Frequência da Categoria Objeto, por Tipo, nos Documentos Estaduais de Regulamentação da LGPD, 2022

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	Não categorizado	15	3,0	3,0	3,0
	Gestão e processos	206	41,7	41,7	44,7
	Governança	256	51,8	51,8	96,6
	Produto	2	,4	,4	97,0
	Serviço	15	3,0	3,0	100,0
	Total	494	100,0	100,0	

Fonte: Elaboração própria.

No que tange ao objeto, verifica-se que o Decreto 49.265, de 6 de agosto de 2020 do Estado do Pernambuco, apresenta o seguinte enunciado institucional:

> Os órgãos e as entidades da Administração Pública Estadual direta, autárquica e fundacional deverão estabelecer suas respectivas Políticas de Proteção de Dados Pessoais Locais – PPDPL a serem aprovadas pelo dirigente máximo.

Nesse caso, o objeto refere-se ao receptor da ação e, no caso da regra em específico, trata de um objeto ligado à noção de governança.

No caso do Estado de Goiás, a Resolução SEDI N.1 de 22/04/2021 dispõe o seguinte:

> O Encarregado pelo Tratamento dos Dados Pessoais indicado: I - deverá possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, os relativos aos temas de: privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público (...).

Nesse caso, identifica-se que o objeto refere-se aos conhecimentos que o encarregado de dados deve possuir para o desempenho de suas funções.

Tabela 8
Tabulação Cruzada da Categoria Atributo com o Objeto

		Objeto					Total
		Não categorizado	Gestão e processos	Governança	Produto	Serviço	
Atributo	Administração pública estadual	1	75	141	0	1	218
	Cidadãos e usuários	2	20	5	0	3	30
	Conselho, comissões ou organizações equivalentes	2	48	46	0	0	96
	Controlador de dados	0	7	13	0	0	20
	Empresas	1	10	9	0	9	29
	Encarregado de dados	3	31	35	0	1	70
	Governo Federal	0	0	3	0	0	3
	Operador de dados	6	15	4	2	1	28

Fonte: Elaboração própria.

Condição

Dada a característica da LGPD, voltada a regular processos e estipular protocolos de ação sobre a proteção de dados, não se identifica no *corpus* de pesquisa selecionado uma preocupação em estipular condições para a governança de dados a nível estadual. Os poucos elementos identificados mostram que as condições estão voltadas à estipulação de prazos para a criação de comitês de gestão de dados e seu respectivo funcionamento. A categoria "não categorizado" significa que 451 enunciados institucionais não especificam condições de tempo e espaço para a realização do alvo prescrito.

Tabela 9
Frequência da Categoria Condição, por Tipo, nos Documentos Estaduais de Regulamentação da LGPD, 2022

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	Não categorizado	451	91,3	91,3	91,3
	Prazos e condições determinados	34	6,9	6,9	98,2
	Prazos e condições indeterminados	9	1,8	1,8	100,0
	Total	494	100,0	100,0	

Fonte: Elaboração própria.

Sobre o tópico, averígua-se, na Resolução SEDI N.1 de 22/04/2021 do Estado de Goiás, que "A indicação do Encarregado pelo Tratamento dos Dados Pessoais deverá ocorrer em até trinta dias corridos contados da publicação desta Resolução". Nesse caso, observa-se que as condições estão basicamente relacionadas a elementos temporais de procedimentos administrativos e não dizem respeito sobre questões concernentes à governança de dados em si, uso desses dados por agentes privados, usuários, terceiro setor etc.

Quanto à questão das consequências (*or else*) prescritas nas regulamentações estaduais da LGPD, não foram encontrados enunciados com as consequências prescritas. Isso ocorre porque a LGPD remete as consequências de seus enunciados institucionais à estrutura normativa de responsabilização administrativa (no caso do setor público) e civil (no caso do setor privado), não sendo necessário fixar penalidades.

Discussão

Conforme apontam Capano e Howlett (2020), a perspectiva que aborda o desenho das políticas públicas (*policy design*) propõe a análise dos aspectos substantivos das políticas, isto é, dos elementos que formam seu conteúdo, os quais traçam sua estrutura e dinâmica. Embora no exterior essa abordagem voltada ao *policy process* esteja presente, no Brasil sua discussão ainda é incipiente. Conforme indicam Lima *et al.* (2021), entende-se que as formas empíricas das políticas públicas (leis, estatutos, regras administrativas, por exemplo) contêm elementos comuns, que correspondem à sua estrutura lógica, são eles: problemas e objetivos, instrumentos de implementação, beneficiários e regras de inclusão/exclusão, sistema de governança, racionalidades e construções sociais. O presente estudo se propôs a contribuir com o avanço desse campo de estudo, tomando como objeto empírico o desenho institucional da proteção de dados nos estados brasileiros. A pesquisa se baseou em análise documental e utilizou o ferramental analítico proposto inicialmente por Crawford e Ostrom (1995), posteriormente aprimorado por Basurto *et al.* (2010) e Siddiki *et al.* (2011; 2022), relativo à análise da gramática institucional. A partir desse enfoque teórico e metodológico foi possível compreender o desenho das políticas estaduais de governança de dados.

O corolário da pesquisa possibilita identificar quatro ordens de questões com relação aos decretos de regulamentação da LGPD nos estados. O desenho institucional da LGPD estabeleceu uma ordem de princípios, reconhecendo a importância da privacidade no mundo contemporâneo e definindo uma ordem de valores públicos que orientam o tratamento de dados pessoais. O desenho institucional também definiu mecanismos de governança dos dados e responsabilidades organizacionais, reconheceu e definiu estruturas de direitos para os cidadãos frente aos complexos de vigilância que emergem com o desenvolvimento tecnológico e criou regras para a proteção em diferentes aspectos que cercam a coleta, armazenamento, processamento e compartilhamento de dados. A regulamentação da LGPD nos estados representa estratégias compartilhadas para a gestão dos dados e o cumprimento dos requisitos institucionais dirigidos para a administração pública estadual. Nesse sentido, a análise dos decretos de regulamentação da LGPD permite entender qual estratégia as administrações estaduais estão adotando para estabelecer conformidade com as escolhas coletivas expressas na lei federal.

O primeiro ponto a ser examinado e discutido é o dos princípios. Em geral, as regulamentações estaduais emulam os princípios da LGPD, sem necessariamente adicionar algum ou especificar como eles serão estabelecidos em procedimentos regulamentares específicos. Os princípios da LGPD são vistos como valores públicos orientativos, não compondo a ação estratégica dos estados para alcançar os objetivos, isto é, sem compor enunciados institucionais completos. Um detalhe importante da pesquisa é que os princípios, quando emulados nos decretos estaduais, não compunham um enunciado institucional, sendo apresentados de forma aberta e referida como valores. No estudo empírico aqui apresentado, os princípios não foram tratados como enunciado institucional, uma vez que eles não apresentam proposições completas e diretrizes de ação claras aos atores. Esse achado vai ao encontro da proposição de Couto e Absher-Bellon (2018), que apontaram a baixa capacidade dos estados da federação em criar leis próprias, optando por emular os princípios já dispostos pela Constituição Federal.

O segundo ponto diz respeito à estrutura de governança. Conforme os dados apresentados nas tabelas anteriores, as regulamentações estaduais atribuem para os próprios órgãos da administração pública um conjunto de obrigações relacionadas aos procedimentos requeridos na LGPD, havendo uma maior preocupação com certificações e produção de *compliance*, ou definição de competências administrativas. O objeto desses decretos regulamentadores está na definição de gestão e processos, ou mecanismos de governança, sem necessariamente incidir na definição de procedimentos para a proteção de dados pessoais.

O terceiro aspecto refere-se à estrutura de direitos dos cidadãos na LGPD. As regulamentações estaduais referem-se pouco a direitos e quais estratégias que os estados adotarão para efetivá-los. Por fim, com relação ao quarto aspecto, relacionado a regras específicas de proteção de dados, os decretos regulamentadores prescrevem enunciados institucionais quase lacônicos com relação a procedimentos para coleta, armazenamento, processamento e compartilhamento de dados.

De uma forma geral, os decretos regulamentadores da LGPD nos estados revelam mais uma estratégia de controle burocrático, prescrevendo procedimentos de conformidade e competências de gestão, do que propriamente uma estratégia de governança para a proteção de dados pessoais, reconhecimento de princípios que incidam na prática do desenvolvimento tecnológico em governos e em direitos fundamentais hoje, inclusive, consagrados

na Constituição, e com reduzida participação da sociedade civil. Ou seja, a arquitetura institucional da proteção de dados no Brasil, tal como construída nos estados, pressupõe mais uma estratégia de controle e *compliance* com a LGPD do que propriamente uma estratégia que elenque instrumentos voltados para a ampliação da segurança de dados, uso de dados em políticas públicas, qualificação de dados, construções de ontologias, procedimentos para coleta, armazenamento e processamento, assim como procedimentos para o compartilhamento de dados. Além disso, os decretos regulamentadores envolvem pouco a participação da sociedade civil, como requerido na LGPD, bem como de diversos *stakeholders* da política.

Isso decorre, empiricamente, na forma como a própria administração pública atribui a si as ações requeridas nos *frameworks* de governança de dados. Associado a isso, os decretos regulamentadores atribuem a controladores e encarregados de dados (agentes da própria administração) boa parte das obrigações requeridas (vide Tabela 2). Os operadores deônticos voltam-se especificamente para obrigações atribuídas para produzir *compliance*, com especial foco em processos de certificação e conformidade, ou definição de competências dentro da administração (Tabela 5). O alvo desses decretos diz pouco sobre procedimentos para coleta, armazenamento, processamento e compartilhamento de dados (coração da governança de dados) e mais sobre competências voltadas para uma conformidade genericamente definida. Da mesma forma, os decretos não definem prazos ou condições para que as ações sejam executadas. Por fim, os decretos não definem consequências, uma vez que, estando em um nível estratégico, eles remetem a outras legislações, em particular referidas a responsabilidades administrativas.

Utilizando-se analiticamente de prisma institucional, identifica-se uma dissociação, no sentido atribuído por Boxenbaum e Jonsson (2017), entre as regras formais postas e as demandas inscritas na LGPD no que tange ao processo de proteção de dados pessoais. Observa-se, portanto, a existência de lacunas entre as políticas oficiais e as estratégias compartilhadas entre os estados da federação. Essa dissociação, ou *decoupling*, pode comprometer o desenvolvimento de soluções tecnológicas, plataformas de governo e de produtos e serviços baseados em dados em nível subnacional.

Em todos os estados os decretos regulamentadores contaram com profunda participação das controladorias estaduais, reproduzindo uma concepção burocrática da LGPD como uma instituição de controle e não propriamente de direitos. Essa concepção de controle ofuscou a natureza primeira da Lei

como um instrumento regulador e relacionado a novos direitos da cidadania, os quais deveriam moldar a prática do desenvolvimento de tecnologias digitais disruptivas aplicadas a governos. O desenho institucional da proteção de dados nos estados projeta uma arquitetura voltada para o controle e *compliance* e não para a garantia de direitos e efetivação de princípios que orientem o desenvolvimento tecnológico em governos.

No Brasil, já existe uma extensa literatura que versa sobre o papel dos órgãos de controle na administração pública (Loureiro *et al.* 2012; Cruz *et al.* 2016; Schabbach, Garcia, 2021), contudo, ainda não se identifica esforços na compreensão da relação entre os órgãos de controle com a implementação da LGPD nas burocracias estatais. Essa nova agenda de pesquisa tem o potencial de identificar quais recursos de poder e estratégias de ação os diversos atores sociais mobilizam para fazer valer seus interesses nesse campo. Embora a LGPD tenha inserido procedimentos e regras específicos para as áreas de tecnologias dos governos, como a definição de controlador e encarregados de dados (Carturan *et al.*, 2022), essas áreas pouco participam da construção institucional nos estados, tendo as controladorias e planejamento assumido essa tarefa de regulamentar a proteção de dados por uma semântica de controle burocrático, pouco referindo-se a direitos e ações requeridas pelos controladores e encarregados de dados.

A abordagem do desenho das políticas públicas envolve a tentativa propositada dos governos de ligar os instrumentos ou ferramentas de políticas aos objetivos que gostariam de realizar (Capano, Howlett, 2020). A partir da análise realizada, argumenta-se que a concepção burocrática da proteção de dados como controle inviabiliza a ação estratégica das administrações públicas para alcançar os objetivos formulados na LGPD, fazendo com que os instrumentos sejam meros mecanismos de *compliance* e não propriamente uma política que produza proteção de dados pessoais e da privacidade dos cidadãos, acione claramente as organizações com responsabilidade atribuída pela Lei e produza resultados em termos de desenvolvimento tecnológico e de direitos.

Conclusão

Este artigo desconstruiu os enunciados institucionais presentes nos decretos regulamentadores da LGPD de forma a proporcionar uma gramática da proteção de dados e da privacidade no Brasil, com especial foco nos governos estaduais. Este artigo contribui com uma literatura emergente

em Ciências Sociais no Brasil sobre a regulação do desenvolvimento tecnológico, especialmente das tecnologias digitais disruptivas. A contribuição aqui apresentada é empírica, de forma a descortinar uma estratégia burocrática das administrações públicas estaduais em torno da proteção de dados e da privacidade como controle e não como direitos.

Embora a Lei Geral de Proteção de Dados estabeleça uma série de princípios e regras que produzem mudanças nas políticas de dados e visam a fortalecer direitos dos cidadãos, os decretos regulamentadores nos estados produzem uma dissociação institucional. Essa dissociação institucional refere-se à forma como os decretos produzem mecanismos entrópicos de controle e *compliance* que pouco afetam procedimentos e estratégias relativos aos elementos essenciais da governança de dados: procedimentos e regras que organizem e estabeleçam mecanismos de decisão sobre a coleta, armazenamento, processamento e compartilhamento de dados. Essa dissociação institucional está refletida na forma como a estratégia dos estados para regulamentar a LGPD busca pela constituição de mecanismos de certificação e conformidade e menos por uma estrutura procedimental comum que instrumentalize ações, procedimentos e *accountability*.

No caso do Brasil, a institucionalização da proteção de dados e da privacidade requer um conjunto de análises complementares. Em vários aspectos, a LGPD tem sido utilizada pelos governos como instrumento de opacidade e mudança do entendimento da Lei de Acesso à Informação (LAI) – Lei 12527, de 18 de novembro de 2011. A LAI foi elemento importante de desenvolvimento institucional no Brasil, colocando a transparência como regra e o sigilo como exceção. Após a sanção da LGPD, ela tem sido utilizada como mecanismos para vetar requerimentos de acesso à informação, alegando que dados pessoais são protegidos em função da privacidade. A LGPD não contraria procedimentos e regras presentes na LAI, uma vez que ela quer reforçar mecanismos de governança e transparência sobre quais dados foram tratados para quais finalidades em governos. O estudo da relação entre a LGPD e a LAI é uma pesquisa futura em função de um problema público construído a partir da sanção da LGPD.

O artigo fez uso de uma estratégia teórico e metodológica extremamente valorizada no campo acadêmico internacional para análise de políticas públicas, principalmente quando se procura compreender as dimensões institucionais das mesmas. Nesse sentido, o presente artigo inovou ao aplicar o IGT em uma investigação empírica no Brasil. Entende-se que a

lente analítica proposta permitiu a observação e análise do objeto empírico em tela. Espera-se que o arcabouço teórico e metodológico proposto por Crawford e Ostrom (1995) e reformulado nos anos recentes por Siddiki *et al.* (2022) e outros autores inspire uma nova agenda de pesquisas no Brasil voltada à análise dos arranjos institucionais, com foco nos enunciados institucionais e na sua relação com o desenho das políticas públicas.

Esta pesquisa inicia uma agenda futura de investigação dos desenhos institucionais de proteção de dados e da privacidade, assim como dos desenhos institucionais relativos à regulação de tecnologias emergentes. Em investigações futuras, a análise empírica da gramática institucional pode fortalecer estudos comparativos e para análise de impacto em termos de desenvolvimento tecnológico e adoção de tecnologias disruptivas. O cenário posto no Brasil é profícuo para avançar essa agenda de pesquisa, de modo a fortalecer os mecanismos institucionais de proteção de dados e efetivação de novos direitos para o mundo digital.

(Recebido para publicação em 26 de setembro de 2022)
(Reapresentado em 30 de janeiro de 2023)
(Aprovado para publicação em 16 de março de 2023)

Notas

1. Tradução nossa.

2. A Lei Carolina Dieckmann alterou o Código Penal Brasileiro incluindo os crimes virtuais e delitos informáticos. A Lei recebeu o nome da atriz Carolina Dieckmann em função do vazamento de 36 fotos pessoais de cunho íntimo após a invasão de um hacker ao seu computador pessoal. A fotos da atriz foram publicadas na internet após a recusa dela em pagar R$10.000,00 ao hacker para resgatar as fotos. A Lei Carolina Dieckmann disciplina os crimes virtuais e foi um marco para iniciar a proteção de dados no Brasil.

Referências

Abraham, Rene; Schneider, Johannes; vom Brocke, Jan. (2019), "Data Governance: A Conceptual Framework, Structured Review, and Research Agenda". *International Journal of Information Management*, v. 49, pp. 424-438. Disponível em: https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Almeida, Virgilio; Filgueiras, Fernando; Mendonça, Ricardo Fabrino. (2022), "Algorithms and Institutions. How Social Science Can Contribute to Governance of Algorithms". *IEEE Internet Computing*, v. 26, n. 2, pp. 42-46. Disponível em: https://doi.org/10.1109/MIC.2022.3147923

Amoore, Louise. (2014), "Security and the Incalculable". *Security Dialogue*, v. 45, n. 5, pp. 423-439. Disponível em: http://dx.doi.org/10.1177/0967010614539719

Basurto, Xavier; Kingsley, Gordon; McQueen, Kelly; Smith, Mshadoni; Weible, Christopher M. (2010), "A Systematic Approach to Institutional Analysis: Applying Crawford and Ostrom's Grammar". *Political Research Quarterly*, v. 63, n. 3, pp. 523-537. Disponível em: https://doi.org/10.1177/1065912909334430

Benjamin, Ruha. (2019), "Assessing Risk, Automating Racism". *Science*, v. 366, n. 6464, pp. 421-422, 2019. Disponível em: https://www.science.org/doi/abs/10.1126/science.aaz3873

Blanke, Jordan; Hiller, Janine. (2019), "Predictability for Privacy in Data-Driven Government". *Minnesota Journal of Law, Science & Technology,* v. 20, n. 1, pp. 32-76. Disponível em: https://scholarship.law.umn.edu/mjlst/vol20/iss1/3

Boxebaum, Eva; Jonsson, Stefan. (2017), "Isomorphism, Diffusion and Decoupling: Concept Evolution and Theoretical Challenges". In: *The Sage Handbook of Organizational Institutionalism*, v. 2, pp. 79-104.

Brayne, Sarah. (2017), "Big Data Surveillance". *American Sociological Review,* v. 82, n. 5, pp. 977-1008. Disponível em: https://doi.org/10.1177/0003122417725865

Capano, Giliberto; Howlett, Michael P. (2020), "The Knowns and Unknowns of Policy Instrument Analysis: Policy Tools and the Current Research Agenda on Policy Mixes". *SAGE Open*, v. 10, n. 1, 1-20. Disponível em: https://doi.org/10.1177/2158244019900568

Carroll, Stephanie R.; Rodriguez-Lonebear, Desi; Martinez, Andrew. (2019), "Indigenous Data Governance: Strategies from United States Native Nations". *Data Science Journal*, v. 18, p. 31. Disponível em: https://doi.org/10.5334/dsj-2019-031

Carturan, Sara B. O. G.; Matsui, Beatriz M. A.; Goya, Denise H. (2022). "LGPD Framework: Na Implementation and Compliance Guide for Technology Areas". *Anais do Seminário Integrado de Software e Hardware (SEMISH), Sociedade Brasileira de Computação*, Niterói, pp. 176-187. Disponível em: https://doi.org/10.5753/semish.2022.223289

Couldry, Nick; Mejias, Ulises. (2019), "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject". *Television & New Media*, v. 20, n. 4, pp. 336-349. Disponível em: https://doi.org/10.1177/1527476418796632

Couto, Claudio G.; Absher-Bellon, Gabriel L. (2018), "Imitação ou Coerção? Constituições Estaduais e Centralização Federativa no Brasil". *Revista de Administração Pública*, v. 52, n. 2, pp. 321-344. Disponível em: https://doi.org/10.1590/0034-761220170061

Crawford, Kate. (2021), *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Heaven, Yale University Press.

Crawford, Sue E. S.; Ostrom, Elinor. (1995), "A Grammar of Institutions". *The American Political Science Review*, v. 89, n. 3, pp. 582-600. Disponível em: https://doi.org/10.2307/2082975

Cruz, Maria do Carmo Meirelles Toledo; Silva, Thomaz Anderson Barbosa; Spinelli, Mario Vinícius. (2016), "O Papel das Controladorias Locais no Cumprimento da Lei de Acesso à Informação pelos Municípios Brasileiros". *Cadernos EBAPE*, v. 14, n. 3, pp. 721-743. Disponível em: http://dx.doi.org/10.1590/1679-395131556

Culpepper, Pepper D.; Thelen, Kathleen. (2021), "Are we all Amazon Primed? Consumers and the Politics of Platform Power". *Comparative Political Studies,* v. 53, n. 2, pp. 288-318. Disponível em: https://doi.org/10.1177/0010414019852687

Dunlop, Claire A.; Kamkhaji, Jhonatan C.; Radaelli, Claudio M.; Taffoni, Giulia. (2021), "The Institutional Grammar Tool Meets the Narrative Policy Framework: Narrating Institutional Statements in Consultation". *European Policy Analysis*, v. 7, n. S2, pp. 365-385. Disponível em: https://doi.org/10.1002/epa2.1126

Eubanks, Virginia. (2018), *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*. New York, St. Martin's Press.

Filgueiras, Fernando. (2022), "The Politics of AI: Democracy and Authoritharianism in Developing Countries". *Journal of Information Technology & Politics*, v. 19, n. 4, pp. 449-464. Disponível em: https://doi.org/10.1080/19331681.2021.2016543

Filgueiras, Fernando; Lui, Lizandro. (2023), "Designing Data Governance in Brazil: An Institutional Analysis". *Policy Design and Practice*, v. 6, n. 1, pp. 41-56. Disponível em: https://doi.org/10.1080/25741292.2022.2065065

Filgueiras, Fernando; Palotti, Pedro Lucas de Moura; Nascimento, Maricilene Isaira Baia. (2022), "Policy Design e Uso de Evidências: O Caso da Plataforma Gov.br", in Koga, Natália Massaco; Palotti, Pedro Lucas de Moura; Mello, Janine; Pinheiro, Maurício Mota Saboya (orgs.), *Políticas Públicas e Uso de Evidências no Brasil: Conceitos, Métodos, Contextos e Práticas.* Brasília, IPEA.

Filgueiras, Fernando; Fernandes, Flávio C.; Palotti, Pedro. (2019), "Digital Transformation and Public Service Delivery in Brazil". *Latin American Policy*, v. 10, n. 2, pp. 195-219. Disponível em: https://doi.org/10.1111/lamp.12169

Frischmann, Bert; Selinger, Evan. (2018), *Re-Engineering Humanity*. Cambridge, Cambridge University Press.

Gitelman, Lisa; Jackson, Virginia. (2013), "Introduction". In: Lisa Gitelman (Ed.). *Raw Data is an Oxymoron*. Cambridge, MIT Press.

Gunduz, Muhammed Z.; Das, Resul. (2020), "Cyber-Security on Smart Grid: Threats and Potential Solutions". *Computer Networks*, v. 169, 107094. Disponível em: https://doi.org/10.1016/j.comnet.2019.107094

Haggerty, Kevin D.; Ericson, Richard V. (2000). "The Surveillant Assemblage". *British Journal of Sociology*, v. 51, n. 4, pp. 605-622. Disponível em: https://doi.org/10.1080/00071310020015280

Hallinan, Dara; Friedewald, Michael; McCarthy, Paul. (2012). "Citizens' Perceptions of Data Protection and Privacy in Europe". *Computer Law & Security Review*, v. 28, n. 3, pp. 263-272. Disponível em: https://doi.org/10.1016/j.clsr.2012.03.005

Hartzog, Woodrow. (2021), "What is Privacy? That's the Wrong Question". *University of Chicago Law Review*, v. 88, pp. 1677-1688. Disponível em: https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/08_ESSAY_HARTZOG.pdf

Joyce, Kelly; Smith-Doerr, Lauren; Alegria, Sharla; Bell, Susan; Cruz, Taylor; Hoffman, Steve G., Noble, Safia U.; Shestakofsky, Ben. (2021), "Toward a Sociology of Artificial Intelligence: A Call for Research on Inequalities and Structural Change". *Socius: Sociological Research for a Dynamic World*, v. 7, pp. 1-11. Disponível em: https://doi.org/10.1177/2378023121999581

Kendall-Taylor, Andrea; Frantz, Erica; Wright Joseph. (2020), "The Digital Dictators: How Technology Strengthens Autocracy". *Foreign Affairs*, v. 99, n. 2, pp. 103-115.

Kitchin, Robin. (2013), "Big Data and Human Geography: Opportunities, Challenges, and Risks". *Dialogues in Human Geography*, v. 3, n. 3, pp. 262-267. Disponível em: https://www.doi.org/10.1177/2043820613513388

Lima, Luciana L.; Aguiar, Rafael B. de; Lui, Lizandro. (2021), "Conectando Problemas, Soluções e Expectativas: Mapeando a Literatura sobre Análise do Desenho de Políticas Públicas". *Revista Brasileira de Ciência Política*, v. 36, e246779. Disponível em: https://doi.org/10.1590/0103-3352.2021.36.246779

Loureiro, Maria Rita; Abrucio, Fernando L.; Olivieri, Cecília; Teixeira, Marco Antônio C. (2012), "Do Controle Interno ao Controle Social: A Múltipla Atuação da CGU na Democracia Brasileira". *Cadernos Gestão Pública e Cidadania*, v. 17, n. 60, pp. 54-67. Disponível em: https://doi.org/10.12660/cgpc.v17n60.3980

Manheim, Karl; Kaplan, Lyric. (2019), "Artificial Intelligence: Risks to Privacy and Democracy". Yale Journal of Law & Technology, v. 21, pp. 106-188.

Margetts, Helen; Dunleavy, Patrick. (2013), "The Second Wave of Digital-Era Governance: A Quasi-Paradigm for Government on the Web". *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, v. 371, n. 1987, pp. 1-17. Disponível em: https://doi.org/10.1098/rsta.2012.0382

Mayer-Schönberger, Viktor; Cukier, Kenneth. (2013), *Big Data: A Revolution that Will Transform How We Live, Work and Think*. London, John Murray.

Noble, Safia U. (2018), *Algorithms of Oppression. How Search Engines Reinforce Racism*. New York, New York University Press.

O'Neil, Cath. (2016), *The Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*. New York, Crown.

OCDE. (2014). *Council Recommendation on Digital Governance Strategies*. Paris, OECD Publishing. Disponível em: https://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm

Ostrom, Elinor (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge, Cambridge University Press.

Ostrom, Elinor (2005), *Understanding Institutional Diversity*. Princeton, Princeton University Press.

Park, Grace. (2020). "The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act". *UC Irvine Law Review*, v. 10, n. 4, pp. 1455-1489. Disponível em: https://scholarship.law.uci.edu/ucilr/vol10/iss4/11/

Rosenberg, Daniel. (2013), "Data Before the Fact", in: Gitelman, Lisa (ed.). *Raw Data is a Oxymoron.* Cambridge, MIT Press.

Russell, Stuart J. (2019), *Human Compatible. Artificial Intelligence and the Problem of Control*. New York, Viking.

Schabbach, Letícia Maria; Garcia, Karin Comandulli (2021), "Novos Atores nas Políticas Educacionais: o Ministério Público e o Tribunal de Contas". *Civitas-Revista de Ciências Sociais*, v. 21, n. 1, pp. 130-143. Disponível em: https://doi.org/10.15448/1984-7289.2021.1.34752

Siddiki, Saba; Basurto, Xavier; Weible, Christopher M. (2012), "Using the Institutional Grammar Tool to Understand Regulatory Compliance: The Case of Colorado Aquaculture". *Regulation & Governance*, v. 6, n. 2, pp. 167-188. Disponível em: https://doi.org/10.1111/j.1748-5991.2012.01132.x

Siddiki, Saba; Heikkila, Tania; Weible, Christopher M.; Pacheco-Vega, Raul; Carter, David; Curley, Cali; Deslatte, Aron; Bennett, Abby. (2022). "Institutional Analysis with the Institutional Grammar". *Policy Studies Journal*, v. 50, n. 2, pp. 315-339. Disponível em: https://doi.org/10.1111/psj.12361

Siddiki, Saba; Weible, Christopher M.; Basurto, Xavier; Calanni, J. (2011). "Dissecting Policy Designs: An Application of the Institutional Grammar Tool". *Policy Studies Journal*, v. 39, n. 1, pp. 79-103. Disponível em: https://doi.org/10.1111/j.1541-0072.2010.00397.x

Solove, Daniel J. (2008), *Understanding Privacy*. Cambridge, Harvard University Press.

Watkins, Cristy; Westphal, Lynne M. (2016), "People Don't Talk in Institutional Statements: A Methodological Case Study of the Institutional Analysis and Development Framework". *Policy Studies Journal*, v. 44, n. S1, pp. 98-122. Disponível em: https://doi.org/10.1111/psj.12139

Whitford, Andrew; Yates, Jeff. (2022), "Surveillance and Privacy as Coevolving Disruptions: Reflections on 'Notice and Choice'". *Policy Design and Practice*, early view, pp. 1-13. Disponível em: https://doi.org/10.1080/25741292.2022.2086667

World Bank (2021). *Dados Para uma Vida Melhor. Relatório de Desenvolvimento Mundial*. Washington: World Bank. Disponível em: https://openknowledge.worldbank.org/bitstream/handle/10986/35218/211600ovPT.pdf

Zhuravskaya, Ekaterina; Petrova, Maria; Enikolopov, Ruben. (2020), "Political Effects of the Internet and Social Media". *Annual Review of Economics*, v. 12, pp. 415-438. Disponível em: https://doi.org/10.1146/annurev-economics-081919-050239

Zuboff, Shoshana. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, Public Affairs.