Revista de Direito Mercantil

industrial, econômico e financeiro

Vol. nº 188, ago. 2024/dez. 2024

EXPERT
EDITORA DIGITAL

rdm
revista de direito mercantil

RDM 188

Artigos e Atualidades:

1. Disciplinando a Economia da Informação - Análise do Data Act da UE como uma Estratégia Brasileira para o Desenvolvimento da Internet das Coisas (Carlos Portugal Gouvêa, Michelle Baruhm Diegues).

2. Qual Bem-Estar do Consumidor? Um Objetivo sem Significado (Rodrigo Fialho Borges, Gustavo Manicardi Schneider).

3. A Recuperação Judicial é um Processo Coletivo Estrutural? (Luis Miguel Roa Florentin, Adriano Camargo Gomes).

4. A Guinada Verde do Direito Societário (Maria Eduarda Lessa).

5. Natureza Jurídica do Evento Material Adverso: Alocação de Riscos como Critério para Extinção do Contrato (Pedro Sergio Liberato Souza).

6. Direito Concorrencial em Plataformas Digitais: Ressignificando o Debate entre Fake News e o Antitruste (Stella Maria Margarita La Regina).

7. Personalidade Jurídica: Uma Dimensão Esquecida da Disciplina Jurídica dos Mercados? (Luiz Guilherme Ros, Arthur Sadami).

8. Aplicação da Affectio Societatis na Dissolução em Sentido Amplo nas Sociedades Limitadas e Anônimas: Análise Teórica e Jurisprudencial (Thales Solis Farha).

9. A Sociedade de Propósito Específico e seu Patrimônio de Afetação na Recuperação Judicial (Giulia Ottani Gonçalves).

10. Processo Administrativo Sancionador nos Órgãos Supervisores do Sistema Financeiro Nacional Brasileiro (Thiago da Cunha Brito).

11. A Dualidade dos Interesses Sociais das Estatais e os Limites na Persecução dos Interesses Públicos pelo Estado (Levi Custódio Santos).

ISBN 978-65-6006-166-8

9 786560 061668 >

IDGLOBAL Instituto de Direito Global

rdm revista de direito mercantil

EXPERT EDITORA DIGITAL

Revista de Direito Mercantil

industrial, econômico e financeiro

REVISTA DE DIREITO MERCANTIL

industrial, econômico e financeiro

188

Publicação do Instituto Brasileiro de Direito Comercial Comparado e Biblioteca Tullio Ascarelli do Departamento de Direito Comercial da Faculdade de Direito da Universidade de São Paulo

Ano LXIII (Nova Série)

Agosto 2024/Dezembro 2024

REVISTA DE DIREITO MERCANTIL
Industrial, econômico e financeiro
Nova Série – Ano LXIII – n. 188 – ago. 2024/dez. 2024

REVISTA DE DIREITO MERCANTIL
Publicação semestral da Editora Expert LTDA
Rua Carlos Pinto Coelho, CEP 30664790 Minas Gerais, BH – Brasil
Diretores: Luciana de Castro Bastos, Daniel Carvalho

Direção Executiva: Luciana de Castro Bastos
Direção Editorial: Daniel Carvalho
Diagramação e Capa: Editora Expert
Revisão: Do Autor
A regra ortográfica usada foi prerrogativa do autor.

AUTORES: Adriano Camargo Gomes, Arthur Sadami, Carlos Portugal Gouvêa, Giulia Ottani Gonçalves, Gustavo Manicardi Schneider, Levi Custódio Santos, Luis Miguel Roa Florentin, Luiz Guilherme Ros, Maria Eduarda Lessa, Michelle Baruhm Diegues, Pedro Sergio Liberato Souza, Rodrigo Fialho Borges, Stella Maria Margarita La Regina, Thales Solis Farha, Thiago da Cunha Brito.

ISBN: 978-65-6006-166-8

Publicado Pela Editora Expert, Belo Horizonte, Abril de 2025

A Revista de Direito Mercantil agradece ao Instituto de Direito Global pelo fomento à publicação deste volume.

Pedidos dessa obra:

experteditora.com.br
contato@editoraexpert.com.br

EXPERT
EDITORA DIGITAL

ÍNDICE E CV DOS AUTORES

Carlos Portugal Gouvêa

Livre-Docente em Direito Comercial pela Faculdade de Direito da USP (2022). Professor Associado de Direito Comercial da Universidade de São Paulo (USP) e sócio fundador do PGLaw. Doutor em Direito pela Universidade de Harvard (S.J.D., 2008). Bacharel pela Universidade de São Paulo (USP). Lecionou como professor visitante na Harvard Law School e foi pesquisador visitante na Yale Law School e na Wharton Business School da University of Pennsylvania. É credenciado pela Ordem dos Advogados do Brasil e pela New York State Bar Association. É membro vice-presidente da Comissão de Mercado de Capitais e Governança Corporativa da OAB-SP e membro do conselho da Comissão Fulbright do Brasil. Foi membro do Conselho de Recursos do Sistema Financeiro Nacional.

Michelle Baruhm Diegues

Doutoranda em Direito Comercial e bacharel pela Faculdade de Direito da Universidade de São Paulo. Coordenadora do Grupo Direito e Pobreza. Editora da Revista de Direito Mercantil, Industrial, Econômico e Financeiro. Advogada com experiência nas áreas de Direito Societário e Governança Corporativa.

Rodrigo Fialho Borges

Professor da Graduação e do Mestrado Profissional na FGV Direito SP. Doutor em Direito Comercial e bacharel pela Faculdade de Direito da Universidade de São Paulo. Pesquisador visitante na University of Pennsylvania Law School (2018-2019). Coordenador do Grupo de Estudos em Fusões e Aquisições (GEM&A) da FGV Direito SP. Sócio no PGLaw.

Gustavo Manicardi Schneider

Mestrando em Direito Comercial e bacharel pela Faculdade de Direito da Universidade de São Paulo. LL.M. Candidate na Harvard Law School (2024-2025).

Luis Miguel Roa Florentin

Mestre em Direito pela Universidade Federal do Paraná (UFPR). Doutorando em Direito Comercial pela USP. Membro do grupo de pesquisa CNPq/Lattes Processo Civil Comparado (UFPR). Advogado em Curitiba e São Paulo. luis@asantosadvogados.adv.br

Adriano Camargo Gomes

Mestre em Direito pela Universidade de Oxford. Doutor em Direito Processual pela USP. Pós-Doutorando em Direito Processual Civil pela UFPR. Membro do grupo de pesquisa CNPq/Lattes Processo Civil Comparado (UFPR). Advogado em Curitiba e São Paulo. adriano@camargoegomes.com

Maria Eduarda Lessa

Bacharel em Direito na Universidade de São Paulo e pesquisadora no Centro de Governança Corporativa.

Pedro Sergio Liberato Souza

Graduado em Direito pela Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo (FDRP-USP), Laurea Magistrale pela Scuola de Giurisprudenza della Università di Camerino (UNICAM), e é doutorando pela Faculdade de Direito do Largo São Francisco (FD-USP).

Stella Maria Margarita La Regina

Advogada. Bacharel em Direito pela FGV Direito São Paulo.

Luiz Guilherme Ros

Mestre e doutorando pela Universidade de Brasília, sócio em Silva Matos Advogados.

Arthur Sadami

Mestre pela Universidade de São Paulo, pesquisador na Fundação Getúlio Vargas e na Universidade de São Paulo.

Thales Solis Farha

Graduado em Direito pela FGV Direito São Paulo – Escola de Direito de São Paulo. E-mail:thalesfarha@outlook.com.

Giulia Ottani Gonçalves

Advogada, graduada em Direito e pós-graduada em Direito Processual Civil pela Universidade Presbiteriana Mackenzie, pós-graduada em Direito Empresarial pela Pontifícia Universidade Católica de São Paulo e membra da comissão de mediação empresarial da Ordem dos Advogados do Brasil Seção São Paulo (OAB/SP).

Thiago da Cunha Brito

Auditor Federal de Controle Externo do Tribunal de Contas da União. Mestrando em Direito Econômico e Desenvolvimento, pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), Brasília, Brasil. Pós-graduado LLM Direito Penal Econômico (IDP). Graduado em Direito (IDP). Licenciado em Engenharia Informática, pelo Instituto Superior de Engenharia do Porto (ISEP), Portugal. Pós-graduado em Marketing e Gestão Estratégica, pela Universidade do Minho (UMinho), Braga, Portugal.

Levi Custódio Santos

Graduado em direito pela Faculdade de Direito da Universidade de São Paulo e certificado em governança corporativa, riscos e compliance pela Saint Paul Escola de Negócios. Foi pesquisador vinculado à Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP). Atua como Advogado em Mercado de Capitais e Governança Corporativa no Veirano Advogados.

SUMÁRIO

DISCIPLINANDO A ECONOMIA DA INFORMAÇÃO: ANÁLISE DO DATA ACT DA UNIÃO EUROPEIA COMO UMA ESTRATÉGIA BRASILEIRA PARA O DESENVOLVIMENTO DA INTERNET DAS COISAS

Carlos Portugal Gouvêa[1] *(USP, São Paulo)*
Michelle Baruhm Diegues[2] *(USP, São Paulo)*

RESUMO:

Em fevereiro de 2020, a Comissão Europeia apresentou uma ambiciosa estratégia conjunta dos Estados-Membros para absorver os benefícios da economia de dados, especialmente em razão do desenvolvimento de produtos relacionados à Internet das Coisas. Esse planejamento, altamente focado em aspectos regulatórios, envolvia, particularmente, a promulgação de dois novos instrumentos normativos considerados centrais para a efetividade das medidas propostas: o *Data Governance Act* (DGA) e o *Data Act* (DA). O Brasil, por sua vez, vivenciou um significativo aumento nos debates sobre a proteção de dados com a promulgação da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), mas a agenda regulatória brasileira não parece ter avançado desde então. Este artigo, portanto, parte da hipótese de que a implementação da estratégia de dados brasileira é insuficiente para garantir a competitividade do mercado nacional diante de novas tecnologias relacionadas à Internet das Coisas. A análise do arcabouço regulatório em vigor no Brasil a respeito da proteção de dados sugere a ausência de medidas específicas voltadas a estimular o desenvolvimento tecnológico e o fluxo de informações entre os agentes do mercado.

1 Professor Associado do Departamento de Direito Comercial da Faculdade de Direito da Universidade de São Paulo. Professor Visitante da Harvard Law School. E-mail: carlosgouvea@usp.br.

2 Doutoranda em Direito Comercial na Faculdade de Direito da Universidade de São Paulo. E-mail: michellebaruhm@usp.br.

ABSTRACT:

In February 2020, the European Commission unveiled its ambitious joint strategy of Member States to harness the benefits of the data economy, particularly in relation to the development of Internet of Things-related products. This strategy, heavily focused on regulatory aspects, notably included the enactment of two pivotal regulatory instruments aimed at enhancing the effectiveness of proposed measures: the Data Governance Act (DGA) and the Data Act (DA). Meanwhile, Brazil experienced a significant surge in discussions on data protection following the enactment of Law No. 13,709, of August 14, 2018 (General Data Protection Law – LGPD). Yet, the country's regulatory agenda appears to have stagnated since. This article posits that Brazil's data strategy is insufficient to ensure national market competitiveness amidst emerging Internet of Things technologies. The analysis of the regulatory framework in Brazil regarding data protection suggests the absence of specific measures to stimulate technological development and the flow of information among market agents.

Palavras-chave: proteção de dados; economia da informação; regulação; Internet das Coisas; tecnologia.

1. INTRODUÇÃO

A emergência dos debates sobre a governança de dados, especialmente diante do rápido avanço da economia da informação, expôs aos responsáveis pela formulação de políticas públicas de diversas jurisdições a necessidade de dispor de uma moldura normativa adequada para promover o desenvolvimento tecnológico. O pioneirismo regulatório europeu, em particular, mostrou-se especialmente relevante após a divulgação da estratégia europeia para os dados, que apresentou diretrizes sofisticadas para tratar de temas de vanguarda, como o compartilhamento de informações geradas por dispositivos conectados. Existe aqui um avanço importante

por parte dos legisladores europeus. Não se trata mais apenas de proteger a privacidade de indivíduos, mas de efetivamente regular a monopolização de bancos de dados para induzir a concorrência nos mercados.

Mais do que um mero conjunto de normas, as práticas utilizadas pelo regulador europeu para a proteção de dados constituem um verdadeiro ecossistema, responsável pela extração de valor das informações geradas no interior do continente. Nesse contexto, a recente promulgação do *Data Act* tem o potencial de estimular o avanço do mercado europeu especialmente em relação à Internet das Coisas, cujos dispositivos conectados podem ampliar significativamente o fluxo de informações.

Apesar da influência global que as práticas regulatórias europeias exercem nas demais jurisdições, a estratégia de governança de dados do bloco econômico não parece ter sido incorporada pelo legislador brasileiro no que tange a este aspecto central, que é o próprio compartilhamento de dados por concorrentes. Na verdade, o planejamento nacional a respeito da economia de dados aparenta ter estagnado após a promulgação da Lei nº 13.709, de 14 de agosto de 2018, que instituiu a Lei Geral de Proteção de Dados Pessoais (LGPD). Nesse sentido, este artigo parte da hipótese de que a implementação da estratégia de dados brasileira é insuficiente para garantir a competitividade do mercado nacional diante de novas tecnologias relacionadas à Internet das Coisas, mas também para criar alguma possibilidade de competitividade e de desenvolvimento de uma indústria nacional de produtos tecnológicos. Caso o Brasil siga sua lógica formalista de apenas proteger direitos individuais, será apenas mais um exemplo do que se poderia chamar de a "vanguarda do atraso", ou o mal costume do legislador brasileiro de ser o primeiro a regular novas tecnologias com leis que, sistematicamente, são superficiais demais e promovem a consolidação dos mercados em setores de tecnologia por companhias estrangeiras.

Para testar essa proposição, este artigo divide-se em duas partes. A primeira descreve as normativas a respeito da governança

e proteção de dados estabelecidas pela União Europeia, como forma de analisar o estado da arte das práticas de regulação sobre o tema, e depois os seus efeitos extraterritoriais diretos e indiretos em países que não fazem parte do continente europeu. A segunda, por sua vez, apresenta a estrutura atualmente vigente de proteção de dados no Brasil, além de analisar sua inserção no planejamento do Governo Federal para a transformação digital, a fim de verificar se o país adotou ou não práticas semelhantes às europeias para estimular o progresso tecnológico e a concorrência da indústria nacional.

Nesse sentido, espera-se que esta análise possa propor uma visão crítica a respeito das técnicas utilizadas pelo legislador nacional para a adaptação às demandas da economia da informação. Considerando a lacuna entre a agenda regulatória europeia e a atual abordagem brasileira, é imperativo que o país implemente normativas robustas para criar um ambiente favorável à inovação e ao desenvolvimento tecnológico. A colaboração internacional e a harmonização de padrões podem ser essenciais para fortalecer a competitividade do mercado brasileiro, especialmente em setores emergentes como a Internet das Coisas, onde a conectividade e o uso de dados são cruciais para o progresso econômico e social.

2. O ECOSSISTEMA DE PROTEÇÃO DE DADOS EUROPEU

Em 2016, o Parlamento Europeu promulgou o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR), um dos primeiros e principais instrumentos normativos a regular o tratamento de dados pessoais. A estrutura e os mecanismos regulatórios do GDPR inspiraram diretamente diversas outras jurisdições fora do continente europeu, instigando debates sobre as melhores práticas para proteção de dados diante do rápido avanço tecnológico.

O GDPR, todavia, não era uma regulação isolada. Sua publicação tornou-se parte de uma diretriz maior do bloco europeu que envolvia a

formação de um verdadeiro planejamento multissetorial para garantir o pioneirismo dos Estados-Membros na economia de dados. Foi esse ponto que parece ter passado desapercebido ao legislador brasileiro, o de que a legislação de proteção de dados é apenas o primeiro passo para uma efetiva regulação de dados que tenha como objetivo não apenas conceder direitos formais, mas sim estimular uma indústria de tecnologia que possa trazer desenvolvimento econômico e direitos reais. Com o Data Act, que será analisado aqui, ficou evidente que uma política de dados deve ser, acima de tudo, uma política industrial e, neste sentido, temos a aprender com o que os legisladores europeus fizeram e com o que o legislador brasileiro deixou de fazer. Diante de seu potencial de geração de valor, o regulador europeu preocupou-se em assegurar que os dados gerados no interior do continente seriam utilizados em benefício de companhias europeias, e não de indústrias multinacionais. Assim, não se estava apenas defendendo direitos individuais dos cidadãos europeus, mas o direito coletivo ao emprego, à renda e a todos os benefícios de um desenvolvimento econômico efetivo.

Nesse sentido, a estratégia europeia se desdobrou em uma série de políticas públicas complementares, com o objetivo de estimular o desenvolvimento tecnológico e a competitividade da indústria dos países compõem o bloco. Assim, para compreender a dimensão dessas novidades regulatórias sobre governança dos dados, é necessário, em primeiro lugar, analisar os instrumentos normativos que integram essa abordagem para, depois, examinar sua influência no arcabouço regulatório global.

2.1 UMA ESTRATÉGIA EUROPEIA PARA A REGULAÇÃO DE DADOS

Em fevereiro de 2020, a Comissão Europeia apresentou, pela primeira vez, uma estratégia unificada para promover e capturar os benefícios da economia de dados. A proposta buscava enfrentar problemas como a interoperabilidade e qualidade dos dados, sua

governança e o desequilíbrio de poder de mercado no acesso a esse material por meio de uma série de políticas públicas voltadas para a regulação digital.

O desenvolvimento da proposta europeia, no entanto, é anterior a essa sistematização. Em 2016, os Estados-Membros decidiram pela adoção da GDPR, cujos esforços de regulação sobre organizações fora da União Europeia induziram efeitos adaptativos globais[3]. Por exemplo, o artigo 20 da GDPR já dispunha sobre o direito de portabilidade dos dados, segundo o qual o titular deve receber os dados que tenha transmitido e poder difundi-los a outros responsáveis pelo tratamento[4]. Esperava-se que o artigo 20 do GDPR fosse capaz de promover o fluxo de informações e incentivar a competitividade do mercado europeu. A aplicação do dispositivo, no entanto, encontrou diversas limitações práticas[5]. Ou seja, não é possível imaginar que apenas os consumidores com recurso à chamada "portabilidade" consigam efetivamente

3 Goddard, Michelle. *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*. International Journal of Market Research, v. 59, n. 6, p. 703-705, 2017, p. 704.

4 GDPR, artigo 20, *in verbis*: "Direito de portabilidade dos dados. 1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: a) O tratamento se basear no consentimento dado nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a), ou num contrato referido no artigo 6.o, n.o 1, alínea b); e b) O tratamento for realizado por meios automatizados. 2 Ao exercer o seu direito de portabilidade dos dados nos termos do n.o 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível. 3. O exercício do direito a que se refere o n.o 1 do presente artigo aplica-se sem prejuízo do artigo 17.o. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. 4. O direito a que se refere o n.o 1 não prejudica os direitos e as liberdades de terceiros." Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016R0679-20160504>. Acesso em: 14 abr. 2024.

5 European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data*. 2020. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>. Acesso em: 14 abr. 2024.

estimular a competitividade em um mercado no qual o domínio sobre os dados dá uma vantagem brutal para determinados competidores. Era uma crença ingênua desde a largada e o pensamento crítico está na capacidade de responder a institutos jurídicos que não atingem seus objetivos. O objetivo de qualquer legislação é atingir objetivos, e não existir de forma plácida e falha sem gerar efeitos na sociedade. Uma lei que não atinge seus objetivos é uma ideia fracassada e nada mais. Diante do fracasso, o que se deve fazer é mudar até que o objetivo da regulação tenha sido atingido.

Diante do desenvolvimento de novas tecnologias baseadas na geração de dados por consumidores, especialmente as relacionadas à Internet das Coisas, ampliam-se as possibilidades de práticas anticompetitivas, discriminatórias e de efeitos de *vendor lock-in*. Afinal, dado que a maior parte dos sistemas de Internet das Coisas apenas permite acesso a dispositivos de fabricantes específicos, a interoperabilidade entre os produtos é significativamente reduzida, o que pode aumentar os custos de migração para equipamentos de outras marcas[6].

Nesse cenário, a estratégia europeia surge com o objetivo de fornecer aos indivíduos ferramentas e mecanismos para decidir detalhadamente como seus dados são utilizados. A proposta é baseada em quatro pilares: (i) estruturas de governança intersetoriais para acesso e uso de dados; (ii) investimento na capacidade europeia de processamento, interoperabilidade e uso de dados; (iii) empoderamento dos indivíduos e investimentos em pequenas e médias empresas; e (iv) estratégias comuns dos Estados-Membros em setores estratégicos e domínios de interesse público[7]. Com isso, a União Europeia visa

6 Zeeuw, Alex van Der; Van Deursen, Alexander Jam; Jansen, Giedo. *The Orchestrated Digital Inequalities of the IoT: How Vendor Lock-In Hinders and Playfulness Creates IoT Benefits in Every Life*. New Media & Society, [S.L.], p. 1-19, 23 nov. 2022. p. 4.

7 European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data*. 2020. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>. Acesso em: 14 abr. 2024

a garantir seu papel de liderança em uma sociedade cada vez mais baseada no fluxo de informações e com amplo potencial de geração de riqueza.

A nova regulação, na verdade, advém da identificação da tendência de crescimento da economia de dados, capaz de gerar cerca de 270 bilhões de euros em PIB adicional para o território europeu até 2028, bem como economias significativas em setores como saúde, transporte, indústria e no mercado imobiliário[8]. A estratégia atual, portanto, diverge da adotada até a implementação do GDPR na medida em que não apenas busca proteger as informações de pessoas naturais, mas, principalmente, explorar o potencial econômico dos dados e das tecnologias orientadas por eles[9].

No entanto, para além dos objetivos econômicos, a reformulação da proposta europeia para o tratamento de dados pode advir, também, de motivações políticas. Dado que companhias sediadas nos Estados Unidos fornecem cerca de 70% dos serviços de armazenamento em nuvem utilizados no continente europeu, a preocupação do regulador com a ausência de provedores de processamento de dados estabelecidos na Europa também favoreceu a percepção de que os Estados-Membros deveriam se beneficiar dos dados gerados por seus cidadãos[10].

Para atingir esses objetivos, a estratégia europeia propunha a criação de um quadro regulatório centralizado em dois instrumentos: o *Data Governance Act* (DGA) e o *Data Act* (DA). O primeiro, inicialmente apresentado pela Comissão Europeia em novembro de 2020, visava a facilitar o compartilhamento voluntário de informações entre setores da indústria e Estados-Membros por meio da regulação dos

8 European Commission. *Data Act – Factsheet*. Download the factsheet to find out more about the Data Act. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet>. Acesso em: 14 abr. 2024.

9 Metzger, Axel; Schweitzer, Heike. *Shaping Markets: A Critical Evaluation of the Draft Data Act*. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4222376>. Acesso em: 14 abr. 2024.

10 CSIS. Center for Strategic & International Studies. *The EU Data Act: The Long Arm of European Tech Regulation Continues*. Disponível em: <https://www.csis.org/analysis/eu-data-act-long-arm-european-tech-regulation-continues>. Acesso em: 14 abr. 2024.

intermediários de dados. Esses agentes, que podem ser tanto entidades públicas quanto privadas, tem como principal função aumentar a confiança entre titulares de dados e seus respectivos utilizadores, como forma de eliminar assimetrias de poder[11].

Nesse sentido, os intermediários de dados, como os *marketplaces*, devem se apresentar de maneira neutra, sem utilizar os dados trocados para qualquer outro fim que não a conexão entre detentores e usuários[12]. Ainda, para aumentar o fluxo de informações no mercado europeu, o DGA introduz mecanismos de altruísmo de dados[13], que permitem que organizações interessadas em coletar e disponibilizar dados com objetivos de interesse público cadastrem-se como tal na União Europeia, como forma de ampliar a confiança sobre os materiais oferecidos, nos termos do Capítulo IV do DGA. Com isso, espera-se contribuir para a criação de repositórios de dados que podem ser utilizados para projetos de *machine learning* e de apoio a pesquisas científicas[14]. Como se vê, não estamos mais na fase da

11 Carovano, Gabriele; Finck, Michèle. Regulating Data Intermediaries: The Impact of The Data Governance Act on the EU's Data Economy. *Computer Law & Security Review*, [S.L.], v. 50, p. 105830, set. 2023.

12 Gellert, Raphaël; Graef, Inge. *The European Commission's proposed Data Governance Act: Some initial reflections on the increasing complex EU regulatory puzzle of stimulating data sharing*. TILEC Discussion Paper 2021-006. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3814721>. Acesso em: 17 abr. 2024.

13 O conceito é definido como "a partilha voluntária de dados, com base no consentimento dos titulares dos dados para o tratamento dos respetivos dados pessoais ou na autorização, por parte de outros detentores dos dados, da utilização dos seus dados não pessoais, sem que esses titulares ou detentores procurem ou recebam uma gratificação que vá além de uma compensação pelos custos em que incorrem ao disponibilizarem os seus dados, para fins de interesse geral, previstos no direito nacional, se aplicável, tais como os cuidados de saúde, a luta contra as alterações climáticas, a melhoria da mobilidade, a facilitação do desenvolvimento, produção e divulgação de estatísticas oficiais, a melhoria da prestação dos serviços públicos, a elaboração de políticas públicas ou a investigação científica de interesse geral". Ver União Europeia. *Regulamento (EU) 2022/868*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32022R0868>. Acesso em: 17 abr. 2024.

14 Regulamento (EU) 2022/868, Considerando 45, *in verbis*: "[...] O presente regulamento deverá visar contribuir para que surjam agrupamentos de dados disponibilizados com base no altruísmo de dados com dimensão suficiente para permitir a análise de dados e a aprendizagem automática, inclusive a nível da União. Para alcançar esse objetivo, os Estados-Membros deverão poder dispor de mecanismos organizacionais ou

proteção de dados, mas sim na fase da regulação de dados. Mais do que proteger a privacidade de alguns indivíduos, o modelo agora tem o objetivo de estimular o acesso aos dados e a competitividade como uma resposta à monopolização de novos mercados por plataformas da internet. O risco é real, pois com a Internet das Coisas, as plataformas que dominarem os dados dos consumidores poderiam dominar não um mercado específico, mas todos os mercados.

Por fim, o DGA estabelece, ainda, as condições para a reutilização de dados detidos por organizações do setor público para fins diferentes dos de interesse público para os quais tais informações tenham sido coletadas. Trata-se, portanto, de um mecanismo que permite que dados protegidos por motivos de confidencialidade comercial ou estatística, proteção de direitos de propriedade intelectual de terceiros ou proteção de dados pessoais, desde que em conformidade com o GDPR, sejam concedidos para pessoas físicas jurídicas com fins comerciais ou não[15]. O artigo 4º proíbe, por fim, a execução de acordos de exclusividade sobre os dados que recaiam nas categorias descritas acima, e que tenham como efeito limitar a disponibilidade da reutilização por terceiros[16].

técnicos, ou ambos, que facilitem o altruísmo de dados". União Europeia. *Regulamento (EU) 2022/868*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32022R0868>. Acesso em: 17 abr. 2024.

15 Regulamento (EU) 2022/868, Artigo 3º(1), *in verbis*: "1. O presente capítulo aplica-se aos dados detidos por organismos do setor público e protegidos por motivos de: a) Confidencialidade comercial, nomeadamente segredos comerciais, profissionais e empresariais; b) Confidencialidade estatística; c) Proteção dos direitos de propriedade intelectual de terceiros; ou d) Proteção dos dados pessoais, na medida em que os dados em causa não sejam abrangidos pelo âmbito de aplicação da Diretiva (UE) 2019/1024." União Europeia. *Regulamento (EU) 2022/868*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32022R0868>. Acesso em: 17 abr. 2024. Ver Ruohonen, Jukka; Mickelsson, Sini. Reflections on the Data Governance Act. *Digital Society*, [S.L.], v. 2, n. 1, p. 2-10, 29 mar. 2023. p. 3.

16 Regulamento (EU) 2022/868, Artigo 4º(1), *in verbis*: "1. São proibidos os acordos ou outras práticas que digam respeito à reutilização de dados detidos por organismos do setor público que incluam categorias de dados referidas no artigo 3.o , n.o 1, e que concedam direitos exclusivos ou tenham por objeto ou efeito conceder direitos exclusivos ou restringir a disponibilidade dos dados para reutilização por entidades que não sejam partes nesses acordos ou outras práticas". União Europeia. *Regulamento (EU) 2022/868*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32022R0868>. Acesso em: 17 abr. 2024.

A partir desses mecanismos, o DGA buscou ampliar tanto o influxo de informações no mercado europeu quanto a confiança nos dados já disponíveis. Com essas medidas, esperava-se, também, estimular o potencial de desenvolvimento da economia de dados. O estudo de impacto conduzido pela Comissão Europeia em 2020 indicou que o setor poderia crescer para um valor estimado de 533,5 bilhões de euros até 2028, que poderia ser ampliado para 540,7 a 544,4 bilhões de euros caso o regulamento fosse adotado[17].

A mera ampliação do volume de dados disponíveis, no entanto, não era suficiente para implementar o projeto de regulação abrangente da União Europeia. Nesse sentido, em fevereiro de 2022, a Comissão Europeia disponibilizou a primeira minuta do *Data Act*, mecanismo central da estratégia europeia para os dados que se dispunha a complementar tanto o GDPR, por abranger dados pessoais e não-pessoais,[18] quanto o DGA, esclarecendo quais agentes poderiam criar valor a partir dos dados disponibilizados e sob quais condições[19]. Assim, enquanto o DGA estabelecia mecanismos regulatórios que pudessem facilitar o compartilhamento de dados entre os Estados-Membros, o DA propõe direitos horizontais de acesso para usuários de produtos que geram dados, ao mesmo tempo em que estabelece disposições obrigatórias em contratos celebrados entre detentores de dados, seus usuários e terceiros. Trata-se, portanto, da garantia de um

17 European Commission. *Impact Assessment Report Accompanying the Document 'Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)'*. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-study-accompanying-proposal-regulation-data-governance>. Acesso em: 17 abr. 2024.

18 O DA define "dados" como "qualquer representação digital de atos, fatos ou informações e qualquer compilação desses atos, fatos ou informações, incluindo sob a forma de gravação sonora, visual ou audiovisual". Como o *Data Act* abrange todos os dados, e não apenas os pessoais, deve ser lido em conjunto com o GDPR da União Europeia. CSIS. Center for Strategic & International Studies. *The EU Data Act: The Long Arm of European Tech Regulation Continues*. Disponível em: <https://www.csis.org/analysis/eu-data-act-long-arm-european-tech-regulation-continues>. Acesso em: 24 abr. 2023.

19 European Commission. *Data Act – Factsheet.* Disponível em: <https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet>. Acesso em: 26 abr. 2024.

direito amplo de acesso aos dados gerados pelos próprios *stakeholders* durante a utilização de um produto[20].

O DA, dessa forma, busca limitar os impactos que possíveis monopólios e oligopólios que trabalhem com processamento e tratamento de dados possam causar no mercado europeu[21]. A preocupação se origina do rápido avanço das tecnologias de Internet das Coisas[22], como carros conectados, geladeiras inteligentes e demais equipamentos domésticos capazes de gerar grande volume de dados sobre seus utilizadores. Embora a maior parte das informações produzidas por esses dispositivos seja protegida pela GDPR, os fabricantes podem empregar *designs* técnicos em seus produtos que impedem o acesso dos consumidores aos dados gerados. Nessa situação, os produtores de equipamentos relacionados à Internet das Coisas tornavam-se detentores exclusivos das informações advindas dos dispositivos, o que poderia trazer efeitos negativos para a competitividade do mercado[23].

Dentre as preocupações concorrenciais, a baixa interoperabilidade entre os ecossistemas de Internet das Coisas gera altos custos de transição caso o usuário decida migrar de um produto para outro. Isto é, um consumidor que compra um dispositivo de determinada marca provavelmente terá grandes dificuldades de integrá-lo com outros produtos inteligentes comercializados por um fabricante diverso. Ainda, as informações produzidas em uma das plataformas usualmente não conseguem ser transferidas em sua

20 Metzger, Axel; Schweitzer, Heike. *Shaping Markets: A Critical Evaluation of the Draft Data Act*. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4222376>. Acesso em: 26 abr. 2024.

21 Portugal Gouvêa, Carlos; Baruhm, Michelle. *Data Act da União Europeia: Um Modelo de Regulação de Dados?* Portal Jota. 12 mar. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/data-act-da-uniao-europeia-um-modelo-de-regulacao-de-dados-12032024>. Acesso em: 26 abr. 2024.

22 European Commission. *Data Act*. Shaping Europe's digital future. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/data-act>. Acesso em: 28 abr. 2024.

23 Kerber, Wolfgang. EU Data Act: Will New User Access and Sharing Rights on IoT Data Help Competition and Innovation?. *Journal Of Antitrust Enforcement*, [S.L.], v. 0, n. 00, p. 1-7, 13 abr. 2024.

totalidade para um ecossistema concorrente, o que gera dispêndios adicionais com a migração dos dados[24]. Esses obstáculos podem levar os utilizadores a um efeito de *vendor lock-in*, em que os consumidores se veem impedidos de mudar de fornecedor em razão de custos financeiros ou de aprendizado para adaptar os dispositivos à nova plataforma[25].

Para mitigar esses eventuais efeitos negativos, o DA exige, inicialmente, que os fabricantes produzam os dispositivos conectados de modo a tornar as informações neles contidas acessíveis aos utilizadores[26]. Além disso, o regulamento impõe uma série de direitos e obrigações dos usuários e dos detentores de dados quanto ao acesso e utilização das informações geradas pelos equipamentos. O artigo 4(1) estabelece, nesse sentido, que, caso o consumidor não possa acessar diretamente os dados por ele produzidos, os fabricantes devem disponibilizá-los prontamente, assim como os metadados necessários para sua interpretação[27]. O acesso a essas informações somente pode

24 Basaure, Arturo; Vesselkov, Alexandr; Töyli, Juuso. Internet of Things (IoT) Platform Competition: Consumer Switching versus Provider Multihoming. *Technovation*, v. 90-91, p. 102101, fev. 2020. p. 4.

25 Ver Amit, Raphael; Zott, Christoph. Value creation in E-business. *Strategic Management Journal*, [S.L.], v. 22, n. 6-7, p. 493-520, jun. 2001; Zeeuw, Alex van Der; Van Deursen, Alexander Jam; Jansen, Giedo. The orchestrated digital inequalities of the IoT: How vendor lock-in hinders and playfulness creates IoT benefits in every life. *New Media & Society*, [S.L.], p. 1-19, 23 nov. 2022. p. 2.

26 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 3(1), *in verbis*: "1. Os produtos conectados devem ser concebidos e fabricados, e os serviços conexos concebidos e prestados, de modo a que os dados relativos a um produto e os dados relativos a um serviço conexo, incluindo os metadados pertinentes necessários para interpretar e utilizar os dados, sejam acessíveis ao utilizador por defeito de forma fácil, segura e gratuita e num formato abrangente, estruturado, de uso corrente e de leitura automática e, quando pertinente e tecnicamente viável, de forma direta." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

27 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 4(1), *in verbis*: "1. Caso o utilizador não possa aceder diretamente aos dados a partir do produto conectado ou do serviço conexo, os detentores dos dados devem tornar acessíveis ao utilizador os dados prontamente disponíveis, bem como os metadados necessários para interpretar e utilizar esses dados, sem demora injustificada, com uma qualidade idêntica à que está disponível para o detentor dos dados, de forma fácil, segura e gratuita, num formato abrangente, estruturado, de uso corrente e de leitura

ser limitado em situações específicas em que o compartilhamento possa causar malefícios à saúde, proteção ou segurança dos usuários[28].

No entanto, para além da garantia de acesso aos consumidores, o DA também estabelece, em seu artigo 5º, as condições sob as quais as informações pré-processadas devem ser compartilhadas com terceiros. Da mesma forma como estipulado para os usuários diretos, os dados devem ser prontamente disponibilizados ao terceiro após a solicitação, mas somente podem ser tratados para os fins e condições previamente acordados com o utilizador, como forma de evitar violações de dados pessoais[29].

O regulamento prevê, ainda, que até mesmo os segredos industriais podem ser compartilhados com os usuários e com terceiros, desde que a divulgação seja necessária para as finalidades indicadas

automática, e, se pertinente e tecnicamente viável, de forma contínua e em tempo real. Esta disponibilização é feita com base num simples pedido por via eletrónica, caso tal seja tecnicamente viável." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

28 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 4(2), *in verbis*: "2. Os utilizadores e os detentores dos dados podem limitar ou proibir contratualmente o acesso, a utilização ou a partilha posterior dos dados, sempre que tal tratamento seja suscetível de comprometer os requisitos de segurança do produto conectado, previstos no direito da União ou no direito nacional, causando efeitos negativos graves na saúde, proteção ou segurança das pessoas singulares. As autoridades setoriais podem facultar aos utilizadores e aos detentores dos dados conhecimentos técnicos especializados nesse contexto. Caso o detentor dos dados se recuse a partilhar dados nos termos do presente artigo, deve notificar a autoridade competente designada nos termos do artigo 37º." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

29 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 6(1), *in verbis*: "1. Um terceiro deve tratar os dados que lhe foram disponibilizados nos termos do artigo 5.o unicamente para as finalidades e nas condições acordadas com o utilizador e sujeito ao direito da União e ao direito nacional sobre a proteção de dados pessoais, incluindo os direitos do titular dos dados no que se refere aos dados pessoais. O terceiro deve apagar os dados quando já não sejam necessários para a finalidade acordada, salvo acordo em contrário com o utilizador relativamente aos dados não pessoais." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

e que os envolvidos tomem todas as medidas para preservar sua confidencialidade, nos termos dos artigos 4(6)[30] e 5(9)[31]. Para muitos, o compartilhamento de segredos industriais poderia representar o máximo sacrilégio a uma ordem antiga das coisas, na qual os segredos industriais eram a base de indústrias relevantes, como a indústria militar. Mas para estabelecer um mínimo de competitividade nos mercados de plataformas que capturam uma quantidade colossal de dados de seus consumidores, tal prática é absolutamente essencial. Com essa abordagem, o DA tenta balancear os interesses gerais da comunidade europeia de ter livre acesso a todos os tipos de dados e os da indústria, ao assegurar que os segredos comerciais não devem perder seu caráter de confidencialidade[32].

Por fim, o DA também inova ao enfrentar diretamente o problema dos custos de transição entre plataformas. O artigo 29 do

30 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 4(6), *in verbis*: "6. Os segredos comerciais devem ser preservados e só podem ser divulgados se o detentor dos dados e o utilizador tomarem, antes da divulgação, todas as medidas necessárias para preservar a sua confidencialidade, em especial no que diz respeito a terceiros. O detentor dos dados ou, caso não sejam a mesma pessoa, o titular dos segredos comerciais deve identificar os dados protegidos como segredos comerciais, incluindo nos metadados pertinentes, e acordar com o utilizador as medidas técnicas e organizativas proporcionadas necessárias para preservar a confidencialidade dos dados partilhados, em especial em relação a terceiros, tais como modelos de cláusulas contratuais, acordos de confidencialidade, protocolos de acesso rigorosos, normas técnicas e a aplicação de códigos de conduta." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

31 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 5(9), *in verbis*: "Os segredos comerciais são preservados e só podem ser divulgados a terceiros na medida em que tal divulgação seja estritamente necessária para cumprir a finalidade acordada entre o utilizador e o terceiro. O detentor dos dados ou, caso não sejam a mesma pessoa, o titular dos segredos comerciais, identifica os dados protegidos como segredos comerciais, incluindo nos metadados pertinentes, e acorda com o terceiro todas as medidas técnicas e organizativas proporcionadas necessárias para preservar a confidencialidade dos dados partilhados, como os modelos de cláusulas contratuais, os acordos de confidencialidade, os protocolos de acesso rigorosos, as normas técnicas e a aplicação de códigos de conduta." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

32 Metzger, Axel; Schweitzer, Heike. *Shaping Markets: A Critical Evaluation of the Draft Data Act*. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4222376>. Acesso em: 26 abr. 2024.

novo regulamento europeu dispõe que os encargos de mudança cobrados por prestadores de serviços de tratamento de dados devem ser paulatinamente reduzidos após a data de publicação da normativa e completamente abolidos após três anos de sua entrada em vigor[33]. Por meio dessa supressão parcial, a União Europeia espera incentivar a concorrência e ampliar as possibilidades de mudança de fornecedores entre os usuários, a fim de impedir efeitos de *lock-in*.

Apesar de críticas pontuais ao texto final do DA[34], com esse ambiente regulatório, a Comissão Europeia tem como objetivo estimular a inovação e estabelecer relações justas na alocação do valor derivado dos dados entre os agentes econômicos que atuam no continente. A autoridade europeia menciona explicitamente a preocupação de assegurar que as indústrias dos Estados-Membros estejam em condições de competir e criar valor a partir dos dados gerados por seus cidadãos[35]. Esse entendimento, que parte da finalidade de reduzir a dependência da União Europeia das empresas de tecnologia estadunidenses, impacta não apenas o mercado

33 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 29(1)(2), *in verbis*: "1. A partir de 12 de janeiro de 2027, os prestadores de serviços de tratamento de dados não podem impor ao cliente, pelo processo de mudança, quaisquer encargos decorrentes da mudança. 2. A partir de 11 de janeiro de 2024 até 12 de janeiro de 2027, os prestadores de serviços de tratamento de dados podem impor ao cliente, pelo processo de mudança, encargos decorrentes da mudança reduzidos." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

34 Ver Kerber, Wolfgang. EU Data Act: Will New User Access and Sharing Rights on IoT Data Help Competition and Innovation?. *Journal Of Antitrust Enforcement*, [S.L.], v. 0, n. 00, p. 1-7, 13 abr. 2024 (que argumenta que o DA é pouco claro e impõe tantas restrições aos utilizadores e receptores dos dados que não se pode esperar um aumento tão significativo no volume de informações compartilhadas); Eckardt, Martina; Kerber, Wolfgang. Property rights theory, bundles of rights on IoT data, and the EU Data Act. *European Journal Of Law And Economics*, [S.L.], p. 1-31, 19 jan. 2024 (em que os autores alegam se que o DA se baseia excessivamente no conceito de exclusividade do controle sobre as informações geradas a partir de dispositivos conectados à Internet das Coisas, seja ele pelos detentores dos dados ou pelos direitos exclusivos outorgados aos usuários, sem que haja abertura para as demais partes interessadas).

35 European Commission. *Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act)*. Explanatory Memorandum. 23 fev. 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068>. Acesso em: 28 abr. 2024.

europeu, mas também os processos globais de compartilhamento de dados, como se passa a analisar a seguir.

2.2 A INFLUÊNCIA EUROPEIA NO ARCABOUÇO REGULATÓRIO GLOBAL

Muito antes da entrada em vigor do GDPR, diversas jurisdições já sentiam a influência da legislação europeia em suas próprias normativas nacionais sobre proteção de dados[36]. Esse fenômeno, comumente chamado de "efeito Bruxelas", indica a tendência de externalização das regras vigentes no mercado interno europeu para países geograficamente distantes dos Estados-Membros, mas que mantêm com eles uma estreita relação comercial. A abrangência dos efeitos extraterritoriais estaria relacionada a cinco fatores que, de acordo com Anu Bradford, estariam presentes no mercado europeu: tamanho do mercado, capacidade regulatória, padrões rigorosos, alvos inelásticos e indivisibilidade[37] – ou seja, as companhias não devem conseguir diferenciar o nível de *compliance* necessário para cada jurisdição.

A emergência das empresas multinacionais e dos mercados globalizados faz com que as companhias tenham incentivos a adotar um padrão único de produção, como forma de facilitar os fluxos comerciais com diferentes nações (efeito Bruxelas *de facto*). Essa padronização a partir do modelo europeu, por conseguinte, torna-se um incentivo para que os Estados de origem das multinacionais também considerem implementá-lo, o que confere às características práticas do efeito Bruxelas um espectro jurídico (efeito Bruxelas *de jure*)[38].

36 Greenleaf, Graham. *Global Data Privacy Laws: 89 Countries and Accelerating*. 6 fev. 2012. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034>. Acesso em: 28 abr. 2024.

37 Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press, 2020, p. 46.

38 Bradford, Anu. Exporting standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics*, Amsterdam, v. 42, p.

Trata-se, portanto, de uma globalização regulatória que adota o modelo europeu como referencial e paradigma. Essa expansão normativa, todavia, não parece ser uma escolha consciente da União Europeia ou parte de sua política externa, mas sim um efeito inesperado da persecução de seus próprios objetivos para o desenvolvimento de seu mercado interno[39]. Tal entendimento fica reforçado pelo fato de que não se identifica um esforço financeiro e pedagógico dos reguladores europeus em serem copiados internacionalmente. Tal efeito tem sido identificado de forma orgânica, pois muitos outros mercados estão em uma situação semelhante ao mercado europeu, qual seja, o de necessitar criar estímulos ao mercado interno por meio de competição no setor de tecnologia. Por outro lado, é verdade que a não adaptação às regras europeias poderia representar significativos custos de oportunidade para as empresas estrangeiras, tendo em vista o tamanho do mercado europeu e sua capacidade regulatória de efetivamente fazer cumprir as normativas estabelecidas[40]. Assim, por mais que o regulador europeu não faça um esforço "evangelizador", inexoravelmente as normas europeias passam a ser estudadas em todo o mundo e a gerar debates de direito comparado.

Em matéria de dados, diversas jurisdições fora do continente europeu tomaram o GDPR como inspiração para a produção de seus próprios regulamentos sobre a proteção de dados pessoais. O *Consumer Privacy Act*, da California (CCPA), faz referência expressa à regulação europeia nos documentos de seu processo legislativo[41]. De maneira similar, conforme analisado na Parte 3, abaixo, a LGPD, também apresenta clara inspiração nos mecanismos desenvolvidos pelo regulador europeu para a proteção de dados. O sucesso do GDPR

158–173, 2015.

39 Bradford, Anu. Exporting standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics*, Amsterdam, v. 42, p. 158–173, 2015.

40 Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press, 2020, p. 25-26.

41 Gunst, Simon; De Ville, Ferdi. The Brussels Effect: How the GDPR Conquered Silicon Valley. *European Foreign Affairs Review*, v. 26, n. 3, p. 437-458, 2021. p. 452.

como padrão global parece derivar não apenas do apelo do acesso ao mercado interno da União Europeia, mas também da credibilidade do regulador europeu e da sincronia dessas medidas com as necessidades mundiais por políticas sobre o tema[42].

Nesse sentido, a implementação da estratégia europeia para os dados, como descrita no tópico anterior, tinha o potencial de influenciar significativamente o comércio internacional que dependesse do fluxo de informações. O DA, em particular, já apresenta diversos dispositivos voltados especificamente para a regulação de aspectos transnacionais dos serviços digitais, como o artigo 28, que estabelece obrigações de transparência contratual para o acesso e transferências internacionais de dados[43]. Da mesma forma, o artigo 32(1) também estabelece obrigações positivas aos prestadores de serviços de tratamento de dados para impedir que governos internacionais tenham acesso ou transfiram dados não pessoais armazenados na União Europeia em caso de potenciais conflitos com o direito europeu[44]. Isto é, além de

42 Cervi, Giulio Vittorio. Why and How Does the EU Rule Global Digital Policy: An Empirical Analysis of EU Regulatory Influence in Data Protection Laws. *Digital Society*, [S.L.], v. 1, n. 2, p. 1-24, set. 2022.

43 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 28, *in verbis*: "1. Os prestadores de serviços de tratamento de dados devem facultar e manter atualizadas nos seus sítios Web as seguintes informações: a) A jurisdição a que está sujeita a infraestrutura informática implantada para o tratamento de dados de cada um dos seus serviços; b) Uma descrição geral das medidas técnicas, organizativas e contratuais adotadas pelo prestador de serviços de tratamento de dados a fim de impedir o acesso governamental internacional a dados não pessoais detidos na União ou a sua transferência, caso esse acesso ou transferência seja suscetível de criar um conflito com o direito da União ou o direito nacional do Estado-Membro pertinente. 2. Os sítios Web a que se refere o n.o 1 devem ser elencados nos contratos relativos a todos os serviços de tratamento de dados oferecidos pelos prestadores de serviços de tratamento de dados." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

44 Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, artigo 32(1), *in verbis*: "1. Sem prejuízo do disposto nos n.os 2 ou 3, os prestadores de serviços de tratamento de dados devem tomar todas as medidas técnicas, organizativas e legais adequadas, incluindo contratos, a fim de impedir que entidades governamentais internacionais ou de países terceiros acedam a dados não pessoais detidos na União ou os transfiram, caso esse acesso ou essa transferência seja suscetível de criar um conflito com o direito da União ou o direito nacional do Estado-Membro pertinente." União Europeia. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível

regular o fluxo de dados dentro do continente, o DA também exige que as companhias tomem medidas para impedir que países ou organizações com um nível de proteção de direitos fundamentais inferior ao europeu acessem essas informações.

Diante desse contexto, as reações iniciais à implementação do DA refletem a preocupação da comunidade internacional com o aumento de seus gastos operacionais para acessar o mercado europeu. Os requisitos regulatórios adicionais para transferências de dados para fora da União Europeia, como o do artigo 32(1), foram tidos como potencialmente discriminatórios em relação às companhias estrangeiras, que teriam seu fluxo de informação global reduzido ou excessivamente mais caro, a ponto de impossibilitar a atuação em determinados setores[45].

Não apenas as multinacionais, mas também as empresas europeias que fornecem serviços digitais para a União seriam afetadas. Parte da doutrina discute, ainda, que as empresas europeias já apresentam gastos com *compliance* regulatório maiores do que suas concorrentes, de modo que a inclusão de despesas adicionais poderia prejudicar sua competitividade em relação às companhias sediadas fora do continente[46].

De todo modo, a estratégia europeia para os dados avança sua agenda regulatória ao reconhecer que a efetividade da proteção dos direitos fundamentais a que se voltam o DGA e o DA depende não apenas de mecanismos internos ao continente europeu, mas principalmente da regulação extraterritorial dos principais agentes globais no tema. Ou seja, existe uma questão de justiça isonômica, pois é importante que os maiores custos estejam nos grandes monopolistas do setor, e

em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

45 CSIS. Center for Strategic & International Studies. *The EU Data Act: The Long Arm of European Tech Regulation Continues*. Disponível em: <https://www.csis.org/analysis/eu-data-act-long-arm-european-tech-regulation-continues>. Acesso em: 19 maio 2024.

46 CSIS. Center for Strategic & International Studies. *The EU Data Act: The Long Arm of European Tech Regulation Continues*. Disponível em: <https://www.csis.org/analysis/eu-data-act-long-arm-european-tech-regulation-continues>. Acesso em: 19 maio 2024.

não nas *start-ups* que tem o potencial de estimular a competitividade e serem o motor do desenvolvimento econômico local. Dado que, na nova economia da informação, o controle sobre os dados determina de forma fundamental o exercício de poder no sistema econômico e político[47], o esforço europeu em descentralizar o debate e estimular novas companhias que queiram participar em mercados de tecnologia ou contestar agentes já estabelecidos pode ter efeitos muito benéficos[48]. Não se trata, pois, de uma imposição de custos pelo regulador, mas de uma distribuição dos custos do monopólio na sociedade, tirando tal custo dos consumidores e concorrentes e colocando tal custo de volta no monopolista.

É necessário analisar, dessa forma, se tais estratégias europeias sofisticadas para os dados também foram capazes de influenciar o ambiente regulatório brasileiro. Após a promulgação da LGPD, o debate sobre a proteção de dados tornou-se uma pauta constante entre acadêmicos e reguladores nacionais, mas a tradução de tais padrões em medidas efetivas para promover a competitividade do mercado brasileiro diante da transformação tecnológica introduzida pela Internet das Coisas exige um exame mais aprofundado das medidas adotadas para esse fim.

3. TRANSFORMAÇÃO DIGITAL E REGULAÇÃO DE DADOS NO BRASIL

Diante do rápido desenvolvimento da economia digital e de seu potencial de impacto nos mercados globais, legisladores de diversas jurisdições apoiaram-se em instrumentos normativos para direcionar o progresso tecnológico de modo a conter seus efeitos negativos e potencializar suas externalidades positivas. A União Europeia, como analisado na seção anterior, adotou uma estratégia de planejamento

47 Portugal Gouvêa, Carlos. *A Estrutura da Governança Corporativa*. São Paulo: Quartier Latin, 2022, p. 567-568.

48 Portugal Gouvêa, Carlos; Baruhm, Michelle. *Data Act da União Europeia: Um Modelo de Regulação de Dados?* Portal Jota. 12 mar. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/data-act-da-uniao-europeia-um-modelo-de-regulacao-de-dados-12032024>. Acesso em: 19 maio 2024.

regulatório voltada a extrair valor do tráfego de dados, sem, contudo, negligenciar a proteção de direitos fundamentais a eles relacionados.

No caso brasileiro, a influência da implementação da GDPR foi sentida, particularmente, com a ampliação dos debates envolvendo a proteção de dados pessoais e, depois, com a promulgação da Lei Geral de Proteção de Dados, que inaugurou um marco teórico sobre o tratamento de dados pessoais no Brasil. No entanto, a União Europeia já havia sinalizado que a GDPR seria apenas um dos pilares de uma estratégia maior voltada não só à proteção, mas também à governança da nova economia de dados. Cumpre analisar, portanto, se o legislador brasileiro também se atentou a essas preocupações, a partir da descrição dos instrumentos normativos em vigor no país, e em que medida a estrutura regulatória nacional comporta o desenvolvimento tecnológico dos produtos relacionados à Internet das Coisas.

3.1 A REGULAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL

A promulgação da Lei Geral de Proteção de Dados, em agosto de 2018, representou a consolidação de uma série de debates sobre a emergência da economia digital no Brasil[49]. Apesar da possibilidade de conhecimento e eventual modificação ou correção de dados pessoais por meio do *habeas data*, assegurado pela Constituição da República em seu artigo 5º, LXXII[50], e regulamentado pela Lei nº 9.507, de 12 de novembro de 1997, a legislação setorial tinha caráter esparso e disposições voltadas apenas para segmentos específicos. Não era suficiente, portanto, para que o país fosse considerado alinhado com as melhores práticas internacionais sobre a governança de dados, como

49 Bioni, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019, p. 187-188.

50 Constituição da República, art. 5º, LXXII, *in verbis*: "LXXII - conceder-se-á 'habeas-data': a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo."

as diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[51].

Dentre os instrumentos normativos já existentes,[52] a primeira legislação a abordar o tratamento de dados pessoais no Brasil foi a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor – CDC). Em seu artigo 43, o CDC dispõe sobre o direito de acesso do consumidor "*às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes*"[53]. O dispositivo, assim, regulamenta a criação e manutenção de bancos de dados a respeito de consumidores, de modo a garantir não apenas a transparência das informações coletadas, como também o controle do titular dos dados a respeito de sua exatidão[54] e uma limitação temporal de cinco anos para o armazenamento de informações negativas[55].

Nesse sentido, o CDC institui os mesmos parâmetros de proteção de dados que seriam, posteriormente, utilizados como eixos

51 OCDE. *Recommendation of the Council OECD Legal Instruments concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OCDE, 2014.

52 A Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos Públicos) e a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) também são citadas por parte da doutrina como predecessoras da proteção de dados pessoais no Brasil, ainda que regulem aspectos mais amplos sobre o acesso à informação em geral. Ver Oliveira, Marco Aurélio Bellizze; Lopes, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2020, p. 61-65.

53 Lei nº 8.078, de 11 de setembro de 1990, art. 43, *caput*, *in verbis*: "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes."

54 Lei nº 8.078, de 11 de setembro de 1990, art. 43, §3º, *in verbis*: "§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas."

55 Lei nº 8.078, de 11 de setembro de 1990, art. 43, §1º, *in verbis*: "§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos."

normativos da LGPD – isto é, o fortalecimento da autonomia e do poder dos indivíduos de controlar o fluxo de suas informações pessoais. No entanto, dado seu caráter setorial, a legislação consumerista não teria competência para regular os demais tipos de relações que se baseiam no tráfego de dados.

Depois, a Lei nº 9.214, de 9 de junho de 2011 (Lei do Cadastro Positivo) regulamentou o acesso e a formação de bancos de dados no setor de crédito. Nesse sentido, o apelido de "*cadastro positivo*" advém da característica da legislação de permitir que a condição financeira dos solicitantes de crédito seja analisada não apenas a partir de seu histórico de inadimplementos, como também das informações a respeito de suas dívidas já pagas[56]. O banco de dados do indivíduo também não pode conter informações excessivas, ou seja, que não estejam relacionadas à análise de risco de crédito, e sensíveis, classificadas como "*aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas*"[57]. A legislação estabelece, ainda, que o histórico de crédito formado a partir dessas anotações somente pode ser disponibilizado a um consulente após autorização específica, com o objetivo de capacitar o titular de dados a administrar o fluxo de suas informações[58].

Por fim, o Marco Civil da Internet (MCI), instituído pela Lei nº 12.965, de 23 de abril de 2014, tem como princípio a proteção da privacidade e de dados pessoais[59]. Nesse sentido, seu artigo 7º

56 Bioni, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019, p. 185.

57 Lei nº 9.214, de 9 de junho de 2011, art. 3º, §3º, *in verbis*: "§ 3º Ficam proibidas as anotações de: I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas."

58 Lei nº 9.214, de 9 de junho de 2011, art. 4º, IV, 'b', *in verbis*: "Art. 4º O gestor está autorizado, nas condições estabelecidas nesta Lei, a: IV - disponibilizar a consulentes: [...] b) o histórico de crédito, mediante prévia autorização específica do cadastrado."

59 Lei nº 12.965, de 23 de abril de 2014, art. 3º, II e III, *in verbis*: "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II - proteção da privacidade;

assegura ao usuário da internet o direito de não fornecer a terceiros seus dados pessoais, da divulgação de informações claras a respeito da coleta, uso, armazenamento e proteção de seus dados e de solicitar a exclusão definitiva de quaisquer informações que tenha fornecido a uma determinada aplicação após o término da relação[60].

O MCI também dispõe que a disponibilização de registros referentes a dados pessoais deve obedecer à proteção da intimidade, da vida privada, da honra e da imagem dos envolvidos, além de exigir a apresentação de ordem judicial para a transferência das informações a terceiros[61]. A legislação, portanto, apresenta um amplo escopo de proteção às informações veiculadas em ambientes digitais, e tem como objetivo capacitar os indivíduos a exercerem seu consentimento a respeito da coleta e tratamento de seus dados por aplicações de internet.

Não havia, no entanto, um instrumento normativo capaz de regular de maneira generalista a proteção de dados pessoais, sem que sua aplicação fosse limitada a setores específicos da economia. Nesse

III - proteção dos dados pessoais, na forma da lei."

60 Lei nº 12.965, de 23 de abril de 2014, art. 7º, VII, VIII e X, *in verbis*: "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; [...] X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais."

61 Lei nº 12.965, de 23 de abril de 2014, art. 10, *caput* e §1º, *in verbis*: "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º."

sentido, a LGPD foi responsável por consolidar a estrutura regulatória sobre o tratamento de dados no Brasil, estabelecendo diretrizes abrangentes e sistematizadas a respeito da coleta, processamento e utilização de informações de caráter pessoal, aplicáveis tanto no setor público quanto privado[62].

A nova legislação foi aprovada por unanimidade no Congresso Nacional, poucos meses após a entrada em vigor da GDPR[63]. As similaridades entre os textos normativos europeu e brasileiro foram destacadas tanto na sistemática de organização dos capítulos quanto nos conceitos previstos em diversos dispositivos da legislação nacional. A definição de "dado pessoal" trazida pela LGPD, por exemplo, apresenta grande correspondência com a prevista na legislação europeia, assim como a forma de categorização dos responsáveis pelo tratamento dos dados em controladores e operadores[64]. Em análise comparativa, a semelhança dos textos de lei[65] e de processos legislativos similares[66] seria um indicativo até mesmo da existência de um transplante jurídico do modelo europeu para o Brasil.

Dessa forma, assim como sua predecessora europeia, a LGPD também institui uma série de princípios e direitos do titular de dados, ao lado de obrigações dos operadores e hipóteses de responsabilização. A transparência, por exemplo, tanto no momento da coleta das informações quanto ao longo de todo o processo de tratamento

62 Mendes, Laura Schertel; Doneda, Danilo. Reflexões Iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, v. 120. ano 27, p. 469-483, nov./dez. 2018. p. 472.

63 Doneda, Danilo. *Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados*. São Paulo: Thomson Reuters, 2020, p. viii.

64 Portugal Gouvêa, Carlos; Fucci, Eduardo; Forti, Gabriela. *A Nova Lei Geral de Proteção de Dados Brasileira*. Bluepaper PGLaw. Ago. 2018. Disponível em: <https://www.academia.edu/117646375/A_Nova_Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_brasileira_Bluepaper_PGLaw_24_ago_2018>. Acesso em: 09 jul. 2024.

65 Derbli, Ludimila Santos. O Transplante Jurídico do Regulamento Geral de Proteção de Dados da União Europeia ("GDPR") para o Direito Brasileiro. *E-legis*, Brasília, v. 30, p. 181-193, set./dez. 2019. p. 191.

66 Abreu, Matheus Chebli de. O processo legislativo e a identificação dos transplantes jurídicos: Uma proposta de análise da elaboração legislativa da Lei Geral de Proteção de Dados. *Revista de Direito Mercantil, Industrial, Econômico e Financeiro*, v. 184-185, p. 291-369, ago. 2022/jul. 2023. p. 349.

dos dados, destaca-se como um dos princípios mais presentes na LGPD[67]. Assim, para o tratamento de dados pessoais, a legislação brasileira adota como pressuposto a necessidade da existência de uma base normativa que autorize as operações[68]. Ou seja, somente serão considerados legítimos os tratamentos que se enquadram nas hipóteses previstas no artigo 7º ou 23 do diploma legal, que constituem hipóteses autorizativas para a continuidade de quaisquer processos envolvendo os dados coletados.

A LGPD, portanto, exigiu das companhias nacionais certas adaptações que tinham como objetivo resguardar o direito à privacidade e, em particular, proporcionar aos indivíduos *autodeterminação informativa*[69] – ou seja, o exercício de controle sobre suas informações pessoais. Assim, o consentimento livre e informado do titular de dados – ou seja, com sua efetiva participação no processo de tomada de decisão – também é citado em diversos dispositivos como uma exigência para o fluxo de tratamento das informações de caráter pessoal[70].

A lei brasileira também estabelece sanções administrativas a serem aplicadas em caso de infrações aos seus dispositivos, como advertências, multas, publicização da infração, bloqueio e eliminação dos dados pessoais referentes ao ato ilícito[71]. As sanções, no entanto,

67 Oliveira, Marco Aurélio Bellizze; Lopes, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2020, p. 75-76.

68 Mendes, Laura Schertel; Doneda, Danilo. Reflexões Iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, v. 120. ano 27, p. 469-483, nov./dez. 2018. p. 472.

69 Lei nº 13.709, de 14 de agosto de 2018, art. 2º, II, *in verbis*: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] II - a autodeterminação informativa."

70 Monteiro, Renato Leite; Bioni, Bruno; Gomes, Maria Cecília Oliveira. *GDPR matchup: Brazil's General Data Protection Law*. International Association of Privacy Professionals (IAPP). 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em: 09 jul. 2024.

71 Lei nº 13.709, de 14 de agosto de 2018, art. 52, *in verbis*: "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta

deveriam ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), pensada originalmente como uma autarquia em regime especial. Essa estrutura, todavia, foi vetada pela Presidência da República, que entendeu que um ente público seria mais adequado para garantir a efetividade da LGPD[72].

Em 27 de dezembro de 2018, a Presidência publicou a Medida Provisória nº 869, posteriormente convertida na Lei nº 13.853, de 8 de julho de 2019, por meio da qual instituiu uma série de mudanças na legislação sobre proteção de dados promulgada em agosto, além de delinear a nova estrutura da ANPD. Nos termos do artigo 55-A, a ANPD seria um órgão da administração pública federal, vinculado à Presidência da República, com natureza jurídica transitória. Ou seja, a autoridade nacional poderia ser transformada em entidade da administração pública federal indireta, submetida à regime autárquico especial, no prazo de dois anos a contar da entrada em vigor dessa nova estrutura regimental[73]. Depois, a Lei nº 14.460, de 26 de outubro de 2022, revogou esses dispositivos e instituiu a ANPD como

Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - (VETADO); VIII - (VETADO); IX - (VETADO); X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados."

72 Doneda, Danilo. *Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados*. São Paulo: Thomson Reuters, 2020, p. 233.

73 Lei nº 13.853, de 8 de julho de 2019, art. 55-A, §§ 1º e 2º, *in verbis*: "Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. § 2º A avaliação quanto à

uma autarquia de natureza especial, dotada de autonomia técnica e decisória e de um patrimônio próprio[74].

Diante de tais idas e vindas regulatórias, a ANPD teve sua atuação altamente esvaziada nos primeiros anos de sua existência. A autarquia aplicou sua primeira sanção administrativa por descumprimento à LGPD em 5 de julho de 2023, a respeito de um processo administrativo sancionador iniciado em 2022 contra a microempresa Telekall Infoservice, acusada de fornecer listas de contatos telefônicos para disseminação de material eleitoral durante a eleição municipal de Ubatuba em 2020[75]. A Coordenação-Geral de Fiscalização da ANPD (CGF/ANPD) verificou que os dados tratados pela Telekall não dispunham de base normativa que autorizasse a operação, o que configurou infração ao artigo 7º da LGPD e ao artigo 5º do Regulamento de Fiscalização da ANPD, com a consequente aplicação de multa no valor total de R$ 14.400,00[76].

Desde a entrada em vigor da LGPD, a CGF/ANPD instaurou nove processos administrativos sancionadores, todos a partir de 2022[77]. Diante da ausência de uma norma que estabelecesse os parâmetros da dosimetria da pena aplicada, todos os processos foram sobrestados até a publicação da Resolução CD/ANPD nº 4/2023, que trata do

transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD."

74 Lei nº 14.460, de 26 de outubro de 2022, art. 1º, *in verbis*: "Art. 1º Fica a Autoridade Nacional de Proteção de Dados (ANPD) transformada em autarquia de natureza especial, mantidas a estrutura organizacional e as competências e observados os demais dispositivos da Lei nº 13.709, de 14 de agosto de 2018."

75 Brasil. *ANPD aplica a primeira multa por descumprimento à LGPD*. 07 jul. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd>. Acesso em: 10 jul. 2024.

76 ANPD. *Relatório de Instrução nº 1/2023/CGF/ANPD*. Processo SEI/ANPD nº 00261.000489/2022-62. Autuado: Telekall Infoservice. 5 jul. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf>. Acesso em: 10 jul. 2024.

77 ANPD. *Processos Administrativos Sancionadores*. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-administrativos-sancionadores>. Acesso em: 13 jul. 2024.

Regulamento de Dosimetria e Aplicação de Sanções Administrativas[78]. Entre os agentes autuados, apenas a Telekall Infoservice, mencionada acima, é uma entidade privada. Os demais processos dizem respeito a órgãos da administração pública direta e indireta, incluindo secretarias, institutos de pesquisa e o Ministério da Saúde.

Tabela 1: Lista de processos administrativos sancionadores instaurados pela CGF/ANPD.

Nº do processo	Agente de Tratamento	Motivo da Instauração	Artigos da LGPD violados	Decisão Final	Multa Aplicada
00261.000456/2022-12	Ministério da Saúde	Falta de comprovação de indicação do encarregado, ausência de envio do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), falta de comunicação de incidente de segurança à ANPD e aos titulares e por deixar de atender requisições da ANPD.	N/A	N/A	N/A
00261.000489/2022-62	Telekall Infoservices	Não atendimento a determinação da ANPD.	Art. 7º e 41	Aplicação de advertência e multa simples.	R $ 14.400,00
00261.000574/2022-21	Instituto de Pesquisa Jardim Botânico do Rio de Janeiro	Falta de comunicação de incidente de segurança à ANPD e aos titulares e por deixar de atender requisições da ANPD.	Art. 48	Arquivamento	N/A

78 ANPD. *Relatório de Ciclo de Monitoramento – 1º Semestre de 2023*. Brasília, 2023. p. 28. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf>. Acesso em: 13 jul. 2024.

Nº do processo	Agente de Tratamento	Motivo da Instauração	Artigos da LGPD violados	Decisão Final	Multa Aplicada
00261.001192/2022-14	Secretaria de Educação do Distrito Federal	Falta de comunicação de incidente aos titulares, ausência de comprovação que os sistemas utilizados atendem aos requisitos de segurança, padrões de boas práticas e governança, ausência de comprovação da manutenção de registros das operações de tratamento de dados pessoais, não apresentação de RIPD e por deixar de atender requisições da ANPD.	Art. 37, 38 e 48	Aplicação de advertência	N/A
00261.001882/2022-73	Ministério da Saúde	Ausência de comunicação a titulares de incidente de segurança; ausência de medidas de segurança.	N/A	N/A	N/A
00261.001886/2022-51	Secretaria de Estado da Saúde de Santa Catarina	Ausência de comunicação a titulares de incidente de segurança; ausência de medidas de segurança; não atendimento a determinações da ANPD.	Art. 38, 48 e 49	Aplicação de advertência e de medidas corretivas envolvendo a comunicação de incidente de segurança a titulares de dados.	N/A

Nº do processo	Agente de Tratamento	Motivo da Instauração	Artigos da LGPD violados	Decisão Final	Multa Aplicada
00261.001969/2022-41	Instituto de Assistência ao Servidor Público Estadual de São Paulo – IAMSPE	Ausência de comunicação a titulares de incidente de segurança; ausência de medidas de segurança.	Art. 48 e 49.	Aplicação de advertência e de medidas corretivas envolvendo a comunicação de incidente de segurança a titulares de dados.	N/A
00261.001963/2022-73	Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS)-PE	Ausência de comunicação a titulares de incidente de segurança; ausência de medidas de segurança.	Art. 48 e 49	Aplicação de advertência e de medidas corretivas envolvendo a comunicação de incidente de segurança a titulares de dados, além de comprovação de medidas técnicas envolvendo a prevenção de novos incidentes de segurança.	N/A

Nº do processo	Agente de Tratamento	Motivo da Instauração	Artigos da LGPD violados	Decisão Final	Multa Aplicada
00261.001888/2023-21	Instituto Nacional do Seguro Social - INSS	Ausência de comunicação de incidente de segurança aos titulares e não atendimento de medida preventiva adotada pela ANPD.	N/A	N/A	N/A

Fonte: ANPD[79].

Nos processos administrativos sancionadores em que a ANPD ainda não apresentou decisão final, o inteiro teor dos autos encontra-se com acesso restrito, de modo que não foi possível acessar as razões de decidir da autarquia. Esse é o caso de ambos os processos movidos contra o Ministério da Saúde e o Instituto Nacional do Seguro Social – INSS. Nos demais, ou seja, considerando apenas os seis processos administrativos passíveis de acesso, a ANPD optou por advertências em 83,33% dos casos e pela aplicação de multa somente para a Telekall, conforme descrito acima. Em 50% dos processos cujos documentos foram disponibilizados ao público, a autarquia se utilizou de medidas corretivas para complementar as advertências, como a comunicação aos titulares de dados da ocorrência de incidentes de segurança e a comprovação de que medidas técnicas foram adotadas, após certo prazo, para prevenir novos incidentes.

Os artigos 48 e 49 da LGPD são os mais citados pela ANPD nos processos administrativos sancionadores. O primeiro diz respeito à obrigação do controlador de comunicar a autarquia e os titulares de dados da ocorrência de incidentes de segurança que possam acarretar riscos ou danos relevantes aos titulares[80]. O artigo 49, por sua vez,

79 ANPD. *Processos Administrativos Sancionadores*. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-administrativos-sancionadores>. Acesso em: 13 jul. 2024.

80 Lei nº 13.709, de 14 de agosto de 2018, art. 48, *in verbis*: "Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá

exige que os sistemas utilizados para o tratamento de dados pessoais atendam aos requisitos de segurança, aos padrões de boas práticas e de governança, além dos princípios previstos na LGPD e nos demais regulamentos aplicáveis[81].

A segurança do tratamento de dados, dessa forma, é um dos principais focos de preocupação da autoridade nacional. A maior atenção à conformidade dos sistemas utilizados parece fazer sentido para uma autarquia que inicia suas atividades após a promulgação de uma lei que instituiu diversas novas obrigações aos agentes públicos e privados. Durante o período de adaptação à nova norma, a ANPD aparenta, portanto, assumir o papel de nivelar os mecanismos utilizados pelos agentes que estão sob sua esfera de regulação.

Para cumprir com esse objetivo, a autoridade nacional promove, além de processos administrativos sancionadores, ações de monitoramento, orientação e prevenção. A Resolução CD/ANPD nº 1/2021, que dispõe sobre o regulamento dos processos de fiscalização e das atividades repressivas por meio da aplicação de sanções, permite que a ANPD levante dados e informações para assegurar o bom funcionamento do ambiente regulado, promova a orientação e a conscientização dos agentes acerca do tratamento de dados pessoais e atue de maneira conjunta com os regulados para construir soluções

---

mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los."

81 Lei nº 13.709, de 14 de agosto de 2018, art. 49, *in verbis*: "Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares."

que levem os agentes investigados de volta à conformidade com a LGPD[82]. As ações repressivas, portanto, somente são instauradas quando já existem indícios probatórios de infração[83].

Essa atuação parecer ser, hoje, o principal foco das atividades da ANPD. A autoridade nacional conta com quatro processos de monitoramento e quinze de fiscalização em andamento. Nessas ações preventivas, o perfil observado nos processos administrativos sancionadores se inverte: cerca de 73,68% dos processos de monitoramento e fiscalização foram movidos contra agentes privados, e apenas 26,32% contra entidades públicas[84]. Dentre os vinte processos de fiscalização concluídos, 75% dos agentes de tratamento autuados eram entes públicos, 20% eram entidades privadas e um dos agentes não pôde ser identificado[85].

Nesse sentido, a atuação da ANPD como autoridade reguladora no âmbito da proteção de dados pessoais ainda é relativamente

82 Resolução CD/ANPD nº 1/2021, art. 15, *in verbis*: "Art. 15. A ANPD adotará atividades de monitoramento, de orientação e de prevenção no processo de fiscalização e poderá iniciar a atividade repressiva. § 1º A atividade de monitoramento destina-se ao levantamento de informações e dados relevantes para subsidiar a tomada de decisões pela ANPD com o fim de assegurar o regular funcionamento do ambiente regulado. § 2º A atividade de orientação caracteriza-se pela atuação baseada na economicidade e na utilização de métodos e ferramentas que almejam a promover a orientação, a conscientização e a educação dos agentes de tratamento e dos titulares de dados pessoais. § 3º A atividade preventiva consiste em uma atuação baseada, preferencialmente, na construção conjunta e dialogada de soluções e medidas que visam a reconduzir o agente de tratamento à plena conformidade ou a evitar ou remediar situações que possam acarretar risco ou dano aos titulares de dados pessoais e a outros agentes de tratamento. § 4º A atividade repressiva caracteriza-se pela atuação coercitiva da ANPD, voltada à interrupção de situações de dano ou risco, à recondução à plena conformidade e à punição dos responsáveis mediante a aplicação das sanções previstas no artigo 52 da LGPD, por meio de processo administrativo sancionador."

83 Resolução CD/ANPD nº 1/2021, art. 4º, II, *in verbis*: "Art. 4º As seguintes definições são adotadas neste Regulamento: [...] II - autuado: agente regulado que, uma vez identificados indícios suficientes de conduta infrativa, tem instaurado processo administrativo sancionador contra si, por meio de auto de infração."

84 ANPD. *Processos de Fiscalização em Andamento*. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao>. Acesso em: 13 jul. 2024.

85 ANPD. *Processos de Fiscalização Concluídos*. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao-concluidos>. Acesso em: 13 jul. 2024.

incipiente. Suas atividades repressivas somente puderam ser propriamente estruturadas em 2022, cerca de quatro anos após a promulgação da LGPD e dois anos após sua entrada em vigor. Dessa forma, a ausência de mecanismos sancionadores atuantes pode ter prejudicado a efetividade da lei em seus primeiros anos de vigência, o que impede a efetiva construção de um ambiente seguro para o compartilhamento de dados pessoais.

Outro traço que começa a se consolidar é o presente em diversos tipos de regulação setorial. As companhias monopolistas ou oligopolistas têm muitos mais recursos para adaptarem-se às regras do chamado *compliance* setorial e, de tal forma, são muito menos sujeitas aos efeitos do processo sancionador administrativo. Além disso, o custo de *compliance* dos monopolistas é proporcionalmente muito inferior ao custo suportado proporcionalmente por companhias pequenas que queiram desafiar os monopolistas. Os monopolistas, de tal forma, beneficiam-se do fato de terem atingido a posição monopolista antes da existência da regulação e, após a sua instauração, tal regulação torna-se uma dádiva ao monopolista, ao tornar-se uma barreira à entrada de novos competidores. É um "custo da desigualdade" inerente a qualquer mercado regulado que tenha como objetivo simplesmente impactar condutas e não ter um impacto estratégico no setor aumentando sua competitividade[86].

No entanto, diante das crescentes transformações tecnológicas, somente a proteção aos dados pessoais é insuficiente para promover a competitividade dos mercados e extrair valor da economia de dados, como buscou fazer o regulador europeu. A ausência de instrumentos normativos nacionais que permitam a regulação completa do ambiente digital pode significar um empecilho para o futuro desenvolvimento da indústria tecnológica brasileira. Necessário, portanto, examinar como a LGPD se insere em uma estratégia nacional maior de promoção da economia digital e se existem projetos em andamento capazes

86 Para uma análise mais detalhada do conceito de "Custos da Desigualdade", ver Portugal Gouvêa, Carlos. *Análise dos Custos da Desigualdade: Efeitos Institucionais do Círculo Vicioso de Desigualdade e Corrupção*. São Paulo: Quartier Latin, 2021.

de direcionar os andamentos das novas tecnologias, especialmente aquelas relacionadas à Internet das Coisas.

3.2 ESTRATÉGIAS PARA O FUTURO E (DES)ESTÍMULO AO DESENVOLVIMENTO TECNOLÓGICO

Em 2018, o Governo Federal anunciou a Estratégia Brasileira para a Transformação Digital, denominada como E-Digital. O documento reconhece que a rápida transformação da economia, impulsionada pelo desenvolvimento de novas tecnologias, demanda mudanças e adaptações à forma de atuação do governo. A estratégia nacional indica a Administração Pública como o conjunto de entidades responsável por capitanear e facilitar a transformação digital dos setores produtivos, além de garantir os direitos fundamentais da população diante da nova forma de estruturação das relações econômicas[87].

O relatório tem como objetivo elaborar um plano de longo prazo para direcionar a transformação digital do mercado brasileiro, por meio da propositura de uma série de iniciativas relacionadas aos diferentes setores da economia e à adoção de novas tecnologias pelos entes públicos, como forma de promover o exercício da cidadania e a prestação eficiente de serviços. A E-Digital, nesse sentido, guia-se pelo incentivo à pesquisa e inovação, atração de investimentos e pela consolidação da confiança no ambiente digital, especialmente por meio da proteção de direitos e da privacidade.

A governança da nova economia de dados é indicada como o eixo temático central das estratégias a serem implementadas. A Internet das Coisas, em particular, serviria como a base do processo de digitalização, em razão de seu potencial de geração de dados e de sua relevância para garantir a competitividade de diversos setores

87 Ministério da Ciência, Tecnologia e Inovação. *Estratégia Brasileira para a Transformação Digital – E-Digital*. Brasília, 2018. Disponível em: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>. Acesso em: 13 jul. 2024.

produtivos[88]. Nesse contexto, o Decreto nº 9.854, de 25 de junho de 2019, instituiu o Plano Nacional de Internet das Coisas, com o objetivo de incentivar o desenvolvimento de produtos conectados no Brasil e a livre circulação de dados[89].

O plano, no entanto, somente institui seus objetivos, que incluem, por exemplo, capacitação profissional e fomento à produtividade e competitividade das empresas brasileiras[90], e designa a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas (Câmara IoT) para o acompanhamento de sua execução[91].

A Câmara IoT elaborou uma lista contendo sessenta ações estratégicas para a expansão da Internet das Coisas[92]. Nenhuma delas,

88 Ministério da Ciência, Tecnologia e Inovação. *Estratégia Brasileira para a Transformação Digital – E-Digital*. Brasília, 2018. p. 67. Disponível em: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>. Acesso em: 13 jul. 2024.

89 Brasil. *Plano Nacional de Internet das Coisas*. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/plano-nacional-de-internet-das-coisas>. Acesso em: 13 jul. 2024.

90 Decreto nº 9.854, de 25 de junho de 2019, art. 3º, *in verbis*: "Art. 3º São objetivos do Plano Nacional de Internet das Coisas: I - melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT; II - promover a capacitação profissional relacionada ao desenvolvimento de aplicações de IoT e a geração de empregos na economia digital; III - incrementar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT, por meio da promoção de um ecossistema de inovação neste setor; IV - buscar parcerias com os setores público e privado para a implementação da IoT; e V - aumentar a integração do País no cenário internacional, por meio da participação em fóruns de padronização, da cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de IoT desenvolvidas no País."

91 Decreto nº 9.854, de 25 de junho de 2019, art. 7º, *in verbis*: "Art. 7º A Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas - Câmara IoT é órgão de assessoramento destinado a acompanhar a implementação do Plano Nacional de Internet das Coisas, a quem compete: I - monitorar e avaliar as iniciativas de implementação do Plano Nacional de Internet das Coisas; II - promover e fomentar parcerias entre entidades públicas e privadas para o alcance dos objetivos do Plano Nacional de Internet das Coisas; III - discutir com os órgãos e entidades públicas os temas do plano de ação de que trata o art. 5º; IV - apoiar e propor projetos mobilizadores; e V - atuar conjuntamente com órgãos e entidades públicas para estimular o uso e o desenvolvimento de soluções de IoT."

92 Ministério da Ciência, Tecnologia e Inovação. *Internet das Coisas – Ações Estratégicas*. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/

no entanto, envolve a promulgação de instrumentos normativos e regulatórios abrangentes a respeito da governança de dados. A ação nº 42, por exemplo, envolve a revisão do quadro regulatório de telecomunicações para viabilizar o investimento na ampliação de rede no país, e ação nº 46 diz respeito à estruturação de governança multissetorial para coordenar atividades baseadas em segurança da informação. Apesar de relevantes, as estratégias são incapazes de incentivar o aumento do fluxo de dados entre os diversos setores produtivos e de promover a competitividade da indústria brasileira diante de um mercado internacional cada vez mais baseado na extração de valor das informações.

As medidas categorizadas pela Câmara IoT como relacionadas a aspectos regulatórios, de segurança e privacidade compõem apenas cerca de 16,67% do Plano Nacional de Internet das Coisas. A maioria delas, na verdade, trata da segurança da informação, sem trazer disposições a respeito da ampliação de acesso aos dados gerados. Nesse sentido, a estratégia brasileira parece ainda estar demasiadamente apegada à privacidade e proteção dos dados pessoais, sem se atentar ao fato de que um ambiente econômico dinâmico depende da regulação ampla também dos dados não-pessoais que circulam entre os agentes econômicos.

Dessa forma, o regulador brasileiro parece ter optado por uma via diversa do europeu. Como analisado na seção 2.1, acima, a União Europeia apresentou o DGA e o DA como instrumentos regulatórios complementares, com o objetivo de garantir que os dados gerados dentro do continente europeu poderiam ser amplamente acessados pelos agentes econômicos que atuassem dentro do bloco – sem, contudo, desconsiderar a proteção à privacidade e aspectos concorrenciais controvertidos relacionados às informações extraídas pelos produtos conectados, como a possibilidade de *vendor lock-in*. A estratégia brasileira, por outro lado, não traz qualquer preocupação

transformacaodigital/nternet-das-coisas-acoes>. Acesso em: 13 jul. 2024.

com os impactos da potencial formação de monopólios e oligopólios decorrentes da concentração de informações.

No mesmo sentido, a E-Digital também traz apenas disposições genéricas a respeito da regulação que deve ser desenvolvida para amparar a transformação digital. O relatório indica que os instrumentos normativos devem incentivar a inovação e promover um ambiente concorrencial equilibrado, mas, diferentemente da estratégia europeia para os dados, não estabelece os contornos concretos das medidas necessárias para chegar a esse fim.

Diante desse cenário e da necessidade de constante monitoramento dos resultados da E-Digital, o Centro de Gestão e Estudos Estratégicos (CGEE), organização social supervisionada pelo Ministério da Ciência, Tecnologia e Inovação (MCTI), promoveu a atualização da estratégia em 2021. O relatório apresenta o diagnóstico da transformação digital ocorrida no Brasil e os efeitos das ações estratégicas promovidas no âmbito da E-Digital. No âmbito regulatório, o CGEE destaca, em particular, que "*as leis voltadas para o ambiente digital ainda carecem da desenvoltura de investigação e técnicas de proteção para tornarem-se garantias de direito*"[93].

A partir do estudo realizado pelo CGEE, o MCTI publicou a atualização da E-Digital para o ciclo de 2022-2026[94]. No entanto, apesar de reconhecer a centralidade da Internet das Coisas e dos dispositivos conectados para o desenvolvimento econômico, a nova E-Digital também não traz propostas regulatórias abrangentes relacionadas ao fluxo de informações.

A ausência de aplicabilidade da E-Digital levou o Tribunal de Contas da União (TCU) a declarar, no Acordão nº 870/2024, "*ser necessário que as estruturas de governança da E-Digital sejam mais efetivas, a fim de*

93 CGEE. *Diagnóstico da E-Digital – Atualização da Estratégia Brasileira para a Transformação Digital*. Brasília, 2021. p. 97. Disponível em: <https://www.cgee.org.br/documents/10195/734063/Diagnostico+E-digital.pdf>. Acesso em: 13 jul. 2024.

94 Ministério da Ciência, Tecnologia e Inovação; CGEE. *Estratégia Brasileira para a Transformação Digital (E-Digital) – Ciclo 2022-2026*. Brasília, 2022. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf>. Acesso em: 13 jul. 2024.

gerenciar a estratégia e permitir seu monitoramento e avalição"[95]. A decisão do TCU, que realizava processo de acompanhamento para verificar a implementação das medidas estabelecidas pela E-Digital, recomendou que a Casa Civil da Presidência da República e o MCTI promovam metas objetivas para cada indicador, apresentem um diagnóstico claro dos problemas e desafios a serem enfrentados e indiquem as estruturas de governança necessárias para a implementação da estratégia.

Nesse sentido, a inexistência de uma estratégia centralizada de regulamentação da economia de dados pode não apenas se tornar um empecilho ao fomento tecnológico, como também expor o país a consequências negativas de perda de competitividade da indústria nacional e de concentração de poder econômico e político. Enquanto a União Europeia apresentou um plano em constante adaptação e com claro enfoque no desenvolvimento de uma moldura regulatória adequada para os desafios das novas tecnologias, o legislador brasileiro deixou de apresentar medidas concretas para a efetivação da transformação digital após a entrada em vigor da LGPD.

A proteção dos dados pessoais, apesar de relevante, não é, sozinha, capaz de garantir a plena inserção do Brasil no mercado internacional da economia de dados. Para garantir a competitividade da indústria nacional, é preciso assegurar que os participantes do mercado brasileiro tenham acesso às informações necessárias para o avanço tecnológico e que possam alocar de maneira justa os efeitos positivos gerados pelo compartilhamento de dados. No entanto, a geração de valor a partir dessas informações, como as que circulam com os dispositivos conectados, por exemplo, depende da existência de um arcabouço regulatório sofisticado e que traga impactos concretos para os agentes que atuam em tais mercados.

95 TCU. *Acórdão nº 870/2024 – TCU – Plenário*. Processo nº 029.178/2022-3 – Relatório de Acompanhamento. Relator: Min. Walton Alencar Rodrigues. J. 14 maio 2024. Disponível em: <https://contas.tcu.gov.br/sisdoc/ObterDocumentoSisdoc?codVersao=editavel&codArqCatalogado=29529449>. Acesso em: 13 jul. 2024.

4. CONCLUSÃO

Este artigo buscou demonstrar que a implementação da estratégia de dados brasileira é insuficiente para garantir a competitividade do mercado nacional diante de novas tecnologias relacionadas à Internet das Coisas, mas também com relação a todos os mercados que envolvam novas tecnologias. Quando comparado com a moldura regulatória proposta pela União Europeia, o planejamento brasileiro a respeito da transformação digital carece de efetividade prática e da criação de instrumentos normativos que permitam a captura dos benefícios decorrentes do avanço tecnológico de uma forma distributiva, ou seja, impondo custos aos monopólios e facilitando a entrada de pequenos concorrentes, como *start-ups* brasileiras, em tais mercados.

A crescente conectividade dos produtos relacionados à Internet das Coisas traz consigo desafios a respeito da mitigação de potenciais efeitos concorrenciais danosos para a economia, mas também oportunidades de geração de valor por meio do aumento do fluxo de informações na sociedade. No entanto, o legislador brasileiro parece excessivamente focado na mera proteção aos dados pessoais e à privacidade, sem considerar que o planejamento efetivo do desenvolvimento econômico envolve aspectos mais amplos relacionados à governança de dados.

A LGPD, nesse sentido, figura como um importante, porém isolado, avanço na agenda regulatória da economia da informação. Mas tal isolamento poderá levar até mesmo a LGPD a tornar-se, com o tempo, em uma legislação inócua. Somente um ecossistema normativo robusto e sofisticado, como o proposto pela União Europeia, é capaz de fazer frente aos desafios impostos pelo progresso técnico e de garantir a liderança dos Estados-Membros na transição para ambientes cada vez mais digitais. Perder a janela de oportunidade de regular esse novo mercado antes de sua completa consolidação significa adotar uma posição de subalternidade global em relação aos produtos relacionados à Internet das Coisas, por exemplo. Uma prática que poderá representar uma submissão não apenas no sentido

de manutenção dos patamares atuais de subdesenvolvimento da sociedade brasileira, mas efetivamente em graus muito mais elevados causados pelo potencial muito superior de geração de desigualdades pelas novas tecnologias da informação, particularmente pelo uso sistêmico da inteligência artificial. Sem uma visão abrangente, capaz de implementar uma regulação estrutural e distributiva, ao Brasil resta continuar como mercado consumidor cada dia mais empobrecido dos frutos do avanço tecnológico que continuará a enriquecer outras sociedades[96].

96 Portugal Gouvêa, Carlos; Baruhm, Michelle. *Data Act da União Europeia: Um Modelo de Regulação de Dados?* Portal Jota. 12 mar. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/data-act-da-uniao-europeia-um-modelo-de-regulacao-de-dados-12032024>. Acesso em: 13 jul. 2024.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Matheus Chebli de. O processo legislativo e a identificação dos transplantes jurídicos: Uma proposta de análise da elaboração legislativa da Lei Geral de Proteção de Dados. *Revista de Direito Mercantil, Industrial, Econômico e Financeiro*, v. 184-185, p. 291-369, ago. 2022/jul. 2023.

AMIT, Raphael; ZOTT, Christoph. Value creation in E-business. *Strategic Management Journal*, [S.L.], v. 22, n. 6-7, p. 493-520, jun. 2001.

ANPD. *Relatório de Instrução nº 1/2023/CGF/ANPD*. Processo SEI/ANPD nº 00261.000489/2022-62. Autuado: Telekall Infoservice. 5 jul. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf>. Acesso em: 10 jul. 2024.

_____. *Processos Administrativos Sancionadores*. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-administrativos-sancionadores>. Acesso em: 13 jul. 2024.

_____. *Processos de Fiscalização em Andamento*. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao>. Acesso em: 13 jul. 2024.

_____. *Processos de Fiscalização Concluídos*. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao-concluidos>. Acesso em: 13 jul. 2024

_____. *Relatório de Ciclo de Monitoramento – 1º Semestre de 2023*. Brasília, 2023. p. 28. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/

documentos-de-publicacoes/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf>. Acesso em: 13 jul. 2024

Basaure, Arturo; Vesselkov, Alexandr; Töyli, Juuso. Internet of Things (IoT) Platform Competition: Consumer Switching versus Provider Multihoming. *Technovation*, v. 90-91, p. 102101, fev. 2020.

_____. Exporting standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics*, Amsterdam, v. 42, p. 158–173, 2015.

Bioni, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019.

Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press, 2020.

Brasil. *ANPD aplica a primeira multa por descumprimento à LGPD*. 07 jul. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd>. Acesso em: 10 jul. 2024.

_____. *Plano Nacional de Internet das Coisas*. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/plano-nacional-de-internet-das-coisas>. Acesso em: 13 jul. 2024

Carovano, Gabriele; Finck, Michèle. Regulating Data Intermediaries: The Impact of The Data Governance Act on the EU's Data Economy. *Computer Law & Security Review*, [S.L.], v. 50, p. 105830, set. 2023.

Cervi, Giulio Vittorio. Why and How Does the EU Rule Global Digital Policy: An Empirical Analysis of EU Regulatory Influence in Data Protection Laws. *Digital Society*, [S.L.], v. 1, n. 2, p. 1-24, set. 2022.

CGEE. *Diagnóstico da E-Digital – Atualização da Estratégia Brasileira para a Transformação Digital*. Brasília, 2021. p. 97. Disponível em: <https://www.cgee.org.br/documents/10195/734063/Diagnostico+E-digital.pdf>. Acesso em: 13 jul. 2024.

CSIS. Center for Strategic & International Studies. *The EU Data Act: The Long Arm of European Tech Regulation Continues*. Disponível em: <https://www.csis.org/analysis/eu-data-act-long-arm-european-tech-regulation-continues>. Acesso em: 14 abr. 2024.

Derbli, Ludimila Santos. O Transplante Jurídico do Regulamento Geral de Proteção de Dados da União Europeia ("GDPR") para o Direito Brasileiro. *E-legis*, Brasília, v. 30, p. 181-193, set./dez. 2019.

Doneda, Danilo. *Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados*. São Paulo: Thomson Reuters, 2020.

Goddard, Michelle. *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*. International Journal of Market Research, v. 59, n. 6, p. 703-705, 2017.

Eckardt, Martina; Kerber, Wolfgang. Property rights theory, bundles of rights on IoT data, and the EU Data Act. *European Journal Of Law And Economics*, [S.L.], p. 1-31, 19 jan. 2024.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data*. 2020. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>. Acesso em: 14 abr. 2024.

_____. *Data Act – Factsheet*. Download the factsheet to find out more about the Data Act. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet>. Acesso em: 14 abr. 2024.

_____. *Data Act*. Shaping Europe's digital future. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/data-act>. Acesso em: 28 abr. 2024.

_____. *Impact Assessment Report Accompanying the Document 'Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)'*. Disponível em: <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-study-accompanying-proposal-regulation-data-governance>. Acesso em: 17 abr. 2024.

_____. *Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act)*. Explanatory Memorandum. 23 fev. 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068>. Acesso em: 28 abr. 2024.

Gellert, Raphaël; Graef, Inge. *The European Commission's proposed Data Governance Act: Some initial reflections on the increasing complex EU regulatory puzzle of stimulating data sharing*. TILEC Discussion Paper 2021-006. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3814721>. Acesso em: 17 abr. 2024.

Greenleaf, Graham. *Global Data Privacy Laws: 89 Countries and Accelerating*. 6 fev. 2012. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034>. Acesso em: 28 abr. 2024.

Gunst, Simon; De Ville, Ferdi. The Brussels Effect: How the GDPR Conquered Silicon Valley. *European Foreign Affairs Review*, v. 26, n. 3, p. 437-458, 2021.

Kerber, Wolfgang. EU Data Act: Will New User Access and Sharing Rights on IoT Data Help Competition and Innovation?. *Journal Of Antitrust Enforcement*, [S.L.], v. 0, n. 00, p. 1-7, 13 abr. 2024.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões Iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, v. 120. ano 27, p. 469-483, nov./dez. 2018.

METZGER, Axel; SCHWEITZER, Heike. *Shaping Markets: A Critical Evaluation of the Draft Data Act*. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4222376>. Acesso em: 14 abr. 2024.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. *Estratégia Brasileira para a Transformação Digital – E-Digital*. Brasília, 2018. Disponível em: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>. Acesso em: 13 jul. 2024.

_____. *Internet das Coisas – Ações Estratégicas*. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/nternet-das-coisas-acoes>. Acesso em: 13 jul. 2024.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO; CGEE. *Estratégia Brasileira para a Transformação Digital (E-Digital) – Ciclo 2022-2026*. Brasília, 2022. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf>. Acesso em: 13 jul. 2024.

MONTEIRO, Renato Leite; BIONI, Bruno; GOMES, Maria Cecília Oliveira. *GDPR matchup: Brazil's General Data Protection Law*. International Association of Privacy Professionals (IAPP). 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em: 09 jul. 2024.

OCDE. *Recommendation of the Council OECD Legal Instruments concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OCDE, 2014.

Oliveira, Marco Aurélio Bellizze; Lopes, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2020.

Parlamento Europeu. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016R0679-20160504>. Acesso em: 14 abr. 2024.

Portugal Gouvêa, Carlos. *Análise dos Custos da Desigualdade: Efeitos Institucionais do Círculo Vicioso de Desigualdade e Corrupção*. São Paulo: Quartier Latin, 2021.

_____. *A Estrutura da Governança Corporativa*. São Paulo: Quartier Latin, 2022.

Portugal Gouvêa, Carlos; Fucci, Eduardo; Forti, Gabriela. *A Nova Lei Geral de Proteção de Dados Brasileira*. Bluepaper PGLaw. Ago. 2018. Disponível em: <https://www.academia.edu/117646375/A_Nova_Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_brasileira_Bluepaper_PGLaw_24_ago_2018>. Acesso em: 09 jul. 2024.

Portugal Gouvêa, Carlos; Baruhm, Michelle. *Data Act da União Europeia: Um Modelo de Regulação de Dados?* Portal Jota. 12 mar. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/data-act-da-uniao-europeia-um-modelo-de-regulacao-de-dados-12032024>. Acesso em: 26 abr. 2024.

TCU. *Acórdão nº 870/2024 – TCU – Plenário*. Processo nº 029.178/2022-3 – Relatório de Acompanhamento. Relator: Min. Walton Alencar Rodrigues. J. 14 maio 2024. Disponível em: <https://contas.tcu.gov.br/sisdoc/Obter9449>. Acesso em: 13 jul. 2024.

União Europeia. *Regulamento (UE) 2022/868*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CEL>. Acesso em: 17 abr. 2024.

_____. *Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202302854>. Acesso em: 28 abr. 2024.

Zeeuw, Alex van Der; Van Deursen, Alexander Jam; Jansen, Giedo. *The Orchestrated Digital Inequalities of the IoT: How Vendor Lock-In Hinders and Playfulness Creates IoT Benefits in Every Life*. New Media & Society, [S.L.], p. 1-19, 23 nov. 2022. p. 4.