PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Programa de Pós-Graduação em Direito

Heloisa de Carvalho Feitosa Valadares

SOCIEDADE INFORMACIONAL E EXECUÇÃO DA POLÍTICA PÚBLICA DE PROTEÇÃO DE DADOS NO BRASIL: estudo comparado das estratégias adotadas no Brasil e na Austrália e o *enforcement* como diferencial de efetividade

Belo Horizonte
2024

Heloisa de Carvalho Feitosa Valadares

SOCIEDADE INFORMACIONAL E EXECUÇÃO DA POLÍTICA PÚBLICA DE PROTEÇÃO DE DADOS NO BRASIL: estudo comparado das estratégias adotadas no Brasil e na Austrália e o *enforcement* como diferencial de efetividade

Tese apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica de Minas Gerais como requisito parcial para obtenção do título de Doutor em Direito.
Orientadores: Prof. Dr. Flávio Couto Bernardes e Prof. Dr. Kieran Tranter.

Belo Horizonte
2024

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Valadares, Heloisa de Carvalho Feitosa
V136s Sociedade informacional e execução da política pública de proteção de dados no Brasil: estudo comparado das estratégias adotadas no Brasil e na Austrália e o *enforcement* como diferencial de efetividade / Heloisa de Carvalho Feitosa Valadares. Belo Horizonte, 2024.
245 f.: il.

Orientador: Flávio Couto Bernardes
Orientador: Kieran Tranter
Tese (Doutorado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito

1. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 2. Sociedade da informação. 3. Proteção de dados pessoais - Regulação. 4. Proteção de dados pessoais – Brasil. 5. Proteção de dados pessoais – Austrália. 6. Direito à privacidade. 7. Política pública. 8. Aplicação da lei. 9. Direito comparado. I. Bernardes, Flávio Couto. II. Tranter, Kieran. III. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito. IV. Título.

CDU: 342.721
Ficha catalográfica elaborada por Fabiana Marques de Souza e Silva - CRB 6/2086

Heloisa de Carvalho Feitosa Valadares

SOCIEDADE INFORMACIONAL E EXECUÇÃO DA POLÍTICA PÚBLICA DE PROTEÇÃO DE DADOS NO BRASIL: estudo comparado das estratégias adotadas no Brasil e na Austrália e o *enforcement* como diferencial de efetividade

Tese apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica de Minas Gerais como requisito parcial para obtenção do título de Doutor em Direito.

_____
Prof. Dr. Flávio Couto Bernardes – PUC Minas

_____
Prof. Dr. José Adércio Leite Sampaio – PUC Minas

_____
Prof. Dr. Marciano Seabra de Godoi – PUC Minas

_____
Prof. Dr. Hugo de Brito Machado Segundo – UFC

_____
Prof. Dr. Kieran Tranter - QUT

Belo Horizonte, 26 de abril de 2024.

Para Elisa, minha inspiração e fonte de energia para seguir em frente e enxergar todos os eventuais obstáculos como oportunidades de crescimento pessoal. Para as gerações futuras, com o desejo de que sempre acreditem que o mundo pode ser melhor com a mudança promovida por cada um de nós.

AGRADECIMENTOS

A realização de uma formação tão intensa quanto o doutoramento nunca é um trabalho solitário. A longa jornada em alguma medida sempre conta com auxílios e suportes das mais variadas ordens. Dito isso, gostaria de agradecer inicialmente à minha família: aos meus pais pelo apoio incondicional, em especial à minha mãe por todo o suporte dado à minha filha durante os últimos quatro anos; ao meu esposo que aceitou embarcar comigo no sonho de ir um pouco além e apostar na oportunidade de aprimoramento que uma experiência como pesquisadora no exterior poderia agregar à minha formação; aos tios Nadir e Carlos pela presença constante e pelo incentivo incessante. Agradeço à minha filha Elisa, razão dos meus melhores sorrisos e das minhas mais profundas preocupações por me inspirar a superar as adversidades e manter sempre a minha essência e o foco no que realmente importa. Ao irmão Guilherme pelo apoio na disponibilização de material de pesquisa deixado no Brasil enquanto estive na Austrália, e pelo apoio como assistente de pesquisa, sempre que enfrentava obstáculos para acessar domínios eletrônicos brasileiros. A Camila e ao Guilherme pelos momentos de alívio ao me fazer rir das adversidades.

Agradeço à rede de apoio que encontrei no PPGD PUC Minas, desde os membros da Secretaria, a quem agradeço fazendo especial referência à Erinalda, até a Coordenação, com especial gratidão ao Professor Marciano pelo seu absoluto comprometimento com os interesses do programa e suporte ao Corpo Discente, que é a alma do PPGD (sua postura e exemplo de verdadeiro educador que incentiva e quer sempre extrair o melhor dos seus alunos me inspiram). Agradeço aos colegas Ícaro Moreira Ursine, Paola Alcântara Lima Dumont, Gabriela Cabral Pires, Raphael Boechat Alves Machado, Larissa Almeida, Cleisson Júnior e Meire Aparecida Furbino Marques, por todo apoio e pelas conversas que tanto me auxiliaram a seguir em frente. Aos colegas que à época eram da graduação e que me auxiliaram a amadurecer o recorte da minha pesquisa através da participação na "Família Proteção de Dados e Capacidade Jurídica" no Segundo Ciclo do "Adote um Pesquisador": Andressa Cristina da Silva Souza, Márcia Maria Wengerter da Silva, Roger Patrick de Souza Gomes e Rosiane Paula Rodrigues.

Manifesto minha gratidão a CAPES, por ter me proporcionado o fomento sem o qual não poderia ter concluído o doutorado, tampouco ter me aventurado em terras estrangeiras. Agradeço aos orientadores que me auxiliaram na trajetória a burilar minhas habilidades e os resultados encontrados: Prof. Dra. Marinella Araújo Machado, Prof. Dr. Flávio Couto Bernardes e Prof. Dr. Kieran Tranter. Ao Professor Kieran manifesto meu carinho, admiração e gratidão eternos por todo o apoio fornecido, pelas fundamentais sugestões para reestruturação

do plano de prova, pela apurada crítica construtiva à minha escrita, pela mentoria quanto à escrita acadêmica em língua inglesa e por todo o aprendizado proporcionado (seu compromisso com a missão de supervisor é irrepreensível, espero poder impactar positivamente a vida dos meus alunos assim como o senhor segue impactando a minha, tendo sempre no seu exemplo a lição de que o conhecimento deve ser difundido, e o educador estimula habilidades sem rivalidade, ampliando as conexões e as redes de apoio à pesquisa).

Por fim, agradeço aos colegas do Algolatr.IA e do HTLC pela intensa troca e pelo suporte. A pesquisa pode ser um trabalho muito solitário e pesado, mas com o auxílio de vocês pude lidar com as "pedras" que apareceram no caminho com mais leveza, compreendendo que todas fazem parte do processo de aprimoramento. Agradeço, ainda, a QUT e a todo o seu *staff* pelo acolhimento e por me oferecerem recursos materiais e intelectuais que foram fundamentais para a conclusão da tese (tenho orgulho de me sentir um pouco filha da QUT, carregarei essa experiência sempre comigo, divulgando as extraordinárias pesquisas gestadas nessa instituição).

O presente trabalho foi realizado com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brazil (CAPES) – Finance Code 001.

"Everyone is a product of his and her data."
Werner Boote

"[...] We do not live in a peaceable kingdom of private walled gardens; the contemporary world more closely resembles a one-way mirror. Important corporate actors have unprecedented knowledge of the minutiae of our daily lives, while we know little to nothing about how They use this knowledge to influence the important decisions that we – and They – make."

Frank Pasquale

[...] Para mudar a perspectiva da nossa privacidade, temos que escrever sobre isso, persuadir outros a proteger a sua e a nossa privacidade, organizar-nos, revelar o funcionamento interno do sistema abusivo que é a sociedade de vigilância, apoiar alternativas, vislumbrar novas possibilidades e recusar-nos a cooperar com nossa própria vigilância.
[...] as escolhas que você fizer hoje determinarão quanta privacidade você terá no futuro. Mesmo que você pense que – hoje não tem nada a esconder, você pode ter algo a esconder daqui a alguns anos, e até lá pode ser tarde demais – os dados que foram fornecidos muitas vezes não podem ser recuperados. Seu país pode respeitar seus direitos humanos hoje, mas você tem certeza absoluta de que continuará assim daqui a cinco ou dez anos?

Carissa Véliz

"My work in that Expert Group taught me a number of lessons which I have held in my mind ever since. First, the importance of international law. We live at a moment in history when international law, which has always operated in a world where law has been such a domestic or municipal phenomenon, something confined to a particular jurisdiction, is increasingly going to be important to every country and to every society. Secondly, it taught me that people can cooperate on developing legal principles, even though they have vastly different cultures, different legal traditions, different systems of legal enforcement. As it turned out, in the field of privacy, they also have quite different economic interests to guard. They can nonetheless come together and develop principles which can be useful throughout the world. Of course in the field of privacy there was a special need for international cooperation because of very global features inter-active technology. In the twenty years since the work of the OECD Expert Group on Privacy we have seen the principles which were developed become highly influential in many countries [...] together. I believe we will see more of this, not least in areas of the law such as privacy where the technology forces us together to cooperate in our local responses."

Michael Kirby (discurso proferido no Privacy Issues Forum – Nova Zelândia – em 10 de Julho de 1997, falando sobre a experiência em grupo especializado da OCDE).

RESUMO

Com o surgimento do digital, a vida humana tornou-se mais obviamente dicotômica. Na sociedade informacional (CASTELLS, 2013; DE LIMA, 2020), onde os dados foram transformados em mercadorias, as plataformas digitais (SRNICEK, 2017) influenciam constantemente a existência material. O material e o digital se interconectam e se sobrepõem, afetando a autonomia dos sujeitos dos dados, já que eles são alvo de feedback que afeta sua vontade e que seus dados são usados para apoiar decisões sobre eles (RODOTÀ, 2008; ZUBOFF, 2019; VÉLIZ, 2021). Reconhecendo o potencial destrutivo dessa existência digital, especialmente no que toca violações de direitos fundamentais, a tendência para a regulação do tratamento de dados pessoais ganhou força, resultando na emissão de uma série de normas que contemplam a proteção de dados como um direito autônomo (SAMPAIO, 1998; RODOTÀ, 2008). Essas normas, que embasam a adoção de políticas públicas para fomento da proteção de dados, são inspiradas em *soft laws* desenvolvidas no âmbito de organizações internacionais, e progressivamente incorporadas nos sistemas jurídicos de estados nacionais. O tratamento de dados numa sociedade informacional constitui uma preocupação transnacional, demandando grau razoável de convergência entre a disciplina dos sistemas jurídicos nacionais para que seja exequível, haja vista a operação desterritorializada das plataformas. Considerando que a necessidade de convergência no âmbito da regulação do tratamento de dados pessoais resulta em normas de conteúdo principiológico similar, o *enforcement*, ou seja, as estratégias empregadas para reforço positivo e negativo de comportamentos e valores preconizados pela política pública desempenha papel determinante para a efetividade dos resultados. A Política Nacional de Proteção de Dados, que tem como suporte normativo a Lei Federal nº. 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), contempla dois grandes propósitos, quais sejam, de estabelecer um ambiente de negócios e de prestação de serviços mais respeitoso e transparente, e a promoção do empoderamento do titular de dados, a partir da autodeterminação informativa como fundamento. A tese investigou, a partir da comparação da implementação da Política Nacional de Proteção de Dados brasileira com a política de privacidade existente em nível federal na Austrália, lastreada pelo *Privacy Act 1988* (Cth), que medidas de *enforcement* seriam mais adequadas para dotar a política pública de proteção de dados de maior efetividade, para que o titular disponha de meios mais democráticos e acessíveis para pleitear seus direitos? Em que pese a tese explore as noções de norma, de regulação (BRAITHWAITE, 2016; BARAK-CORREN, KARIV-TETELBAUM, 2021) e de política pública, por serem complementares e interrelacionados, o objeto de pesquisa da tese é a política pública, entendida como um conjunto de ações governamentais coordenadas em escala ampla para a resolução de um problema complexo que a motivou (BUCCI, 2006, 2019). E o foco da investigação é a aferição de efetividade, entendida na tese como relativa ao alcance dos ideais da política (BUCCI, 2006), isto é, atinente à busca da concretização dos objetivos e valores que orientaram o planejamento da política pública. Para responder ao problema de pesquisa, a tese é desenvolvida em cinco capítulos, além da Introdução e das Conclusões, valendo-se do emprego de pesquisa bibliográfica, exploratória e crítica, com emprego de raciocínio hipotético abdutivo (ALISEDA, 2006), mesclando abordagens qualitativas dedutivas e indutivas. O método funcional de Direito Comparado (MICHAELS, 2019), que adota a função do fenômeno estudado como eixo de comparação foi adotado, por tratar-se de tese que investiga duas políticas públicas, igualmente vocacionadas a disciplinar o tratamento de dados pessoais e a estabelecer um ambiente relacional mais respeitoso entre agentes de tratamento de dados e titulares de dados pessoais. As técnicas de pesquisa empregadas foram revisão bibliográfica e análise documental, realizada através da análise das normas que figuram como suporte normativo das políticas comparadas (LGPD e *Privacy Act 1988* (Cth)), que traçam o desenho

geral da política a ser implementada, de decisões administrativas e judiciais tomadas com base nas normas mencionadas de 2020 a 2022, de relatórios de pesquisas realizadas para aferir a efetividade das políticas, além de documentos emitidos pelas Autoridades Nacionais de Proteção de Dados Pessoais brasileira (Autoridade Nacional de Proteção de Dados) e australiana (*Office of Australian Information Commissioner).* A preocupação com a efetividade da política pública foi determinante para a adoção da vertente jurídico-sociológica de pesquisa (GUSTIN, DIAS, 2010).

Palavras-chave: Sociedade Informacional; Proteção de Dados Pessoais; Privacidade; Políticas Públicas; Regulação, *Enforcement*.

ABSTRACT

With the rise of the digital, human life has become more obviously dichotomous. In the informational society (CASTELLS, 2013; DE LIMA, 2020), where data has been transformed into commodities, digital platforms (SRNICEK, 2017) constantly influence material existence. The material and the digital interconnect and overlap each other, affecting data subjects' autonomy since they are the target of feedback that affects their will and their data is used to support decisions about them (RODOTÀ, 2008; ZUBOFF, 2019; VÉLIZ, 2021). Recognising the destructive potential of this digital existence, especially when it comes to violations of fundamental rights, the trend towards regulating the processing of personal data has gained momentum, resulting in the issuance of a series of norms that contemplate data protection as an autonomous right (SAMPAIO, 1998; RODOTÀ, 2008). These standards, which underpin the adoption of public policies to promote data protection, are inspired by soft laws developed by international organisations and progressively incorporated into the legal systems of national states. Data processing in an informational society is a transnational concern, requiring a reasonable degree of convergence between the disciplines of national legal systems to be feasible, given the de-territorialised operation of platforms. Considering that the need for convergence within the scope of regulating the processing of personal data results in rules with similar principles, enforcement, i.e. the strategies employed to positively and negatively reinforce the behaviours and values advocated by the public policy, plays a decisive role in the effectiveness of the results. The National Data Protection Policy, whose normative support is Federal Law nº. 13.709/2018, better known as the General Personal Data Protection Law (LGPD), has two main purposes, namely, to establish a more respectful and transparent business and service environment, and to promote the empowerment of the data subject, based on informational self-determination as a foundation. The thesis investigated, based on a comparison of the implementation of the Brazilian National Data Protection Policy with the existing privacy policy at the federal level in Australia, backed by the Privacy Act 1988 (Cth), what enforcement measures would be most appropriate to make the public data protection policy more effective, so that the data subject has more democratic and accessible means to claim their rights? Although the thesis explores the notions of norm, regulation (BRAITHWAITE, 2016; BARAK-CORREN, KARIV-TETELBAUM, 2021) and public policy, as they are complementary and interrelated, the research object of the thesis is public policy, understood as a set of coordinated government actions on a broad scale to solve a complex problem that motivated it (BUCCI, 2006, 2019). The focus of the investigation is the measurement of effectiveness, understood in the thesis as relating to the achievement of the policy's ideals (BUCCI, 2006), i.e. the search for the realisation of the objectives and values that guided the planning of the public policy. To answer the research problem, the thesis is developed in five chapters, in addition to the Introduction and Conclusions, using bibliographical, exploratory, and critical research, adopting abductive hypothetical reasoning (ALISEDA, 2006), which mixes deductive and inductive qualitative approaches. The functional method of Comparative Law (MICHAELS, 2019), which adopts the function of the phenomenon studied as the axis of comparison, was adopted, as this thesis investigates two public policies, equally aimed at disciplining the processing of personal data and establishing a more respectful relational environment between data processing agents and personal data subjects. The research techniques used were a literature review and documentary analysis, carried out by analysing the laws that are the normative support for the compared policies (LGPD and Privacy Act 1988 (Cth)), which outline the general design of the policy to be implemented, administrative and judicial decisions taken based on the aforementioned rules from 2020 to 2022, research reports carried out to assess the effectiveness of the policies, as

well as documents issued by the Brazilian (National Data Protection Authority) and Australian (Office of Australian Information Commissioner) National Data Protection Authorities. The concern with the effectiveness of public policy was a determining factor in adopting the legal-sociological research approach (GUSTIN, DIAS, 2010).

Keywords: Informational Society; Personal Data Protection; Privacy; Public Policy; Regulation, Enforcement.

LISTA DE FIGURAS

Figura 1 – Pirâmide Regulatória.....100
Figura 2 – Pirâmide regulatória com *enforcement* em rede 102
Figura 3 – Infográfico Direitos do titular de dados 120
Figura 4 – Organograma ANPD.....121
Figura 5 – Fluxo da petição ANPD.....122
Figura 6 – Mapa estratégico ANPD.....123
Figura 7 – Gráfico quantitativo de acórdãos STF/STF.....128
Figura 8 – Infográfico reclamação de privacidade OAIC.....166
Figura 9 – Gráfico Decisões Administrativas e Judiciais – Privacy Act 1988 (Cth).....170
Figura 10 – Estrutura Organizacional OAIC.....172
Figura 11 – Gráfico APPs reclamações OAIC 2020.....175
Figura 12 – Gráfico APPs reclamações OAIC 2021.....177
Figura 13 – Gráfico APPs reclamações OAIC 2022.....178
Figura 14 – Gráfico APPs reclamações OAIC 2022-2022.....180

LISTA DE TABELAS

Tabela 1..89

LISTA DE ABREVIATURAS E SIGLAS

AAT	Administrative Appeal Tribunal
ADI	Ação Declaratória de Constitucionalidade
ADPF	Ação por Descumprimento de Preceito Fundamental
Ag.	Agravo
ALRD	Australian Law Reform Commission
ANPD	Autoridade Nacional de Proteção de Dados
APEC	Asia-Pacific Economic Cooperation
APF	Australian Privacy Foundation
APP	Australian Privacy Principle
ARENA	Partido Político Aliança Renovadora Nacional
BPP	Behavioural Public Policy
CE	Conselho Europeu
CEDIS	Centro de Direito, Internet e Sociedade
CMAG	Comitê de Monitoramento e Avaliação de Gastos Diretos
CMAS	Comitê de Monitoramento e Avaliação de Subsídios da União
CMAP	Conselho de Monitoramento e Avaliação de Políticas Públicas
CF	Constituição Federal
CNIL	Commission Nationale de l'Informatique et des Libertés
CPI	Comissão Parlamentar de Inquérito
DT	Design Thinking
ENEM	Exame Nacional do Ensino Médio
EC	Emenda Constitucional
FCA	Federal Court of Australia
FCFCOA	Federal Circuit and Family Court of Australia
GDPR	General Data Protection Regulation
IA	Inteligência Artificial
IBGE	Instituto Brasileiro de Geografia e Estatística
ICCPR	International Covenant on Civil and Political Rights
ICO	Information Commissioner's Office

IDP	Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa
IoT	Internet of Things
INEP	Instituto Nacional de Estudos e Pesquisas
IPP	Information Privacy Principle
LGPD	Lei Geral de Proteção de Dados
MP	Medida Provisória
NDB	Notifiable Data Breach
NPP	Nacional Privacy Principle
OAIC	Office of Australian Information Commissioner
OBPR	Office of Best Practice Regulation
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OIA	Office of Impact Analysis
OMS	Organização Mundial da Saúde
PDS	Partido Democrático Social
PEC	Projeto de Emenda Constitucional
PIA	Privacy Impact Assessment
PL	Projeto de Lei
PLS	Projeto de Lei do Senado
PMDB	Partido Movimento Democrático Brasileiro
PROCON	Programa de Proteção e Defesa do Consumidor
RE	Recurso Extraordinário
Reg.	Regimental
RENAPE	Registro Nacional de Pessoas Naturais
REsp	Recurso Especial
RSI	Regulamento Sanitário Internacional
SENACON	Secretaria Nacional do Consumidor
SISU	Sistema de Seleção Unificada
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCU	Tribunal de Constas da União
TEP	Teoria da Encriptação do Poder

SUMÁRIO

1 INTRODUÇÃO 19

1.1 Breves considerações sobre o problema de pesquisa, hipótese, objetivos gerais e específicos 22

1.2 Aspectos metodológicos 23

1.3 Originalidade da tese e contribuições para o conhecimento 27

1.4 Estrutura da tese 29

2 SOCIEDADE INFORMACIONAL: ubiquidade da tecnologia, vigilância, datificação, humanidade digital e proteção de dados como um direito fundamental autônomo 31

2.1 Derivação e especialização da tutela dos direitos da personalidade: direito à proteção de dados como meio de tutela do corpo digital 34

2.2 Por que não aplicar a TEP? 49

2.3 Sociedade informacional, plataformas e a mitigação do livre desenvolvimento da personalidade 51

2.4 Fluxos transnacionais de dados e a mitigação da soberania na regulação 73

3 PROTEÇÃO DE DADOS: busca de convergência regulatória na era do capitalismo de vigilância e de plataforma 82

3.1 Da Privacidade à proteção de dados como direito autônomo no mundo: repercussões da sociedade informacional e conectada em rede 82

3.2 Convergência regulatória da privacidade e da proteção de dados: emulação e a emergência das estratégias de *enforcement* como diferencial 92

3.3 Estado como regulador e regulado: elementos de regulação responsiva e a construção da cultura de privacidade e proteção de dados 97

4 PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL: da elaboração da LGPD à implementação da Política Nacional de Proteção de Dados 106

4.1 LGPD como suporte normativo da Política Nacional de Proteção de Dados Pessoais 108

4.1.1 Previsões e tutelas no plano normativo 114

4.2 ANPD e CNPD: design de *enforcement* da Política Nacional de Proteção de Dados Pessoais 120

4.3 Aplicação da LGPD e a tutela do direito à proteção de dados: a construção da política e o papel preponderante do judiciário no cenário brasileiro 123

4.3.1 Proteção de dados nos Acórdãos do STJ 128

4.3.2 Proteção de Dados nos Acórdãos do STF 130

4.4 Política Pública de Proteção de Dados Brasileira e Cultura de Compliance com a privacidade e a proteção de dados 139

5 CONTEXTO AUSTRALIANO DE PRIVACIDADE: por que buscar outras referências para além dos países Europeus? 148

5.1 O foco nas normas do *Commonwealth* 149

5.2 Privacidade e proteção de dados na Austrália: uma breve contextualização 152

5.3 *Enforcement* da privacidade na aplicação do *Privacy Act 1988* (Cth) 168

5.3.1 Decisões do *Office of Australian Information Commissione*r – OAIC 170

5.3.2 Privacidade nas decisões do *Administrative Appeal Tribunal* - AAT 187

5.3.3 Privacidade nas decisões da *Federal Court of Australia* - FCA 189

5.4 Privacidade e cultura de compliance com o *Privacy Act 1988* (Cth) na Austrália 194

6 ESTRATÉGIAS DE *ENFORCEMENT* E O MELHORAMENTO CONTÍNUO DA POLÍTICA NACIONAL DE PROTEÇÃO DE DADOS BRASILEIRA 199

6.1 Estratégias de *enforcement* 200

6.2 O *enforcement* e a modulação da cultura de privacidade e proteção de dados 204

6.3 Transparência, aposta na abordagem dialógica, e possibilidade de ter perdas compensadas na esfera administrativa 207

6.4 Temas a serem incluídos na regulação da Proteção de Dados e na política pública 212

7 CONCLUSÕES 218

REFERÊNCIAS 227

1 INTRODUÇÃO

Esta tese consiste em uma investigação crítica da efetividade das políticas públicas de proteção de dados do Brasil e do *Commonwealth* australiano, por meio do método funcional de direito comparado (MICHAELS, 2019). O sentido de efetividade adotado parte do ponto de vista da proteção dos titulares dos dados e do poder de disseminação dos valores da privacidade nas culturas social, organizacional e econômica. Como política pública, a tese designa um sistema de ações coordenadas para garantir e promover direitos e valores, com foco na privacidade e na proteção de dados, nos casos estudados. O direito à proteção de dados é concebido como um direito dinâmico detido por uma pessoa natural para controlar o tratamento de informações pessoais com potencial para identificar o indivíduo, independentemente de essas informações serem armazenadas em dispositivo digital ou analógico. A comparação levou em conta a estrutura em implementação no Brasil desde a entrada em vigor da *Lei Federal nº. 13.709 de 14 de agosto de 2018* - LGPD, em 2020, e na Austrália, desde a entrada em vigor do *Privacy Act 1988* (Cth).

É importante destacar que a LGPD é um suporte normativo da Política Nacional de Proteção de Dados, sendo um de seus componentes, ao formalizar o direito à proteção de dados e criar uma espécie de mapa que orienta a estruturação do sistema de proteção a esse direito. Esta tese se dedica ao estudo e à avaliação da Política Nacional de Proteção de Dados, entendida como o conjunto de ações coordenadas em larga escala para a resolução de problemas oriundos do tratamento de dados pessoais e promoção da privacidade, da proteção de dados e da autodeterminação informativa, em alinhamento ao conceito de política pública proposto por Maria Paula Dallari Bucci (2019). Assim, a LGPD não se confunde com a Política Nacional de Proteção de Dados Pessoais. É inegável que a LGPD é considerada um modelo normativo alinhado às "melhores práticas de governança", haja vista que se espelha no *General Data Protection Regulation - GDPR*, elevado ao nível de padrão internacional no campo da proteção de dados. O objeto de pesquisa da tese, entretanto, é a análise da efetividade da política pública de proteção de dados no que tange a proteção desse direito fundamental dos titulares, assim como o estudo e propositura de estratégias para o incremento dessa proteção.

Por sociedade informacional trata-se do contexto em que as relações sociais e comerciais são guiadas por dados e transitam entre os mundos digital e material de forma onipresente. Na sociedade informacional os dados se tornam uma *commodity* e um ativo (DE LIMA, 2020; CASTELLS, 2013). As interações são frequentemente realizadas por meio de

estruturas digitais, designadas de plataformas (SRNICEK, 2017), que funcionam como uma porta para a exploração de dados pessoais[1] (SRNICEK, 2017, p. 48). Nesse cenário em que a informação se torna o próprio serviço ou produto e fonte de poder, os dados pessoais, que consistem em informações sobre uma pessoa natural que têm o potencial de identificá-la ou torná-la identificável (BRASIL, 2018), têm um valor monetário e estratégico ainda maior, pois proporcionam oportunidades de explorar as vulnerabilidades dos titulares para influenciar a formação de sua vontade e seus atos futuros.

Os dados pessoais constituem o titular dos dados no ambiente digital, formam seu corpo digital. Esse corpo digital é utilizado para julgamentos que impactam as chances reais do titular dos dados no ambiente material. Vale reforçar, os dados pessoais de uma pessoa natural são essa pessoa no ambiente digital, constituem a pessoa, seu corpo eletrônico (RODOTÀ, 2008, p. 19-20), merecendo especial proteção jurídica por integrarem o objeto de proteção dos direitos da personalidade (RODOTÀ, 2008, p. 19). Nesta tese, adota-se a nomenclatura de corpo digital, ao invés de "corpo eletrônico", por considerá-la mais adequada à natureza desse perfil formado por dados pessoais, ao passo que a designação remete ao digital, ambiente que se mescla com o material na sociedade informacional.

A identificação da nocividade da extração e do uso dos dados pessoais (RODOTÀ, 2008; ZUBOFF, 2019; VÉLIZ, 2021) impõe diversos desafios ao direito e à regulação. Para a tese a regulação é entendida como o processo de estabelecimento de regras, bem como seu monitoramento e reforço, para sua efetiva aplicabilidade (BARAK-CORREN, KARIV-TEITELBAUM, 2021), como forma de direcionar o fluxo de eventos (BRAITHWAITE, 2016, p. 21) para promover a proteção aos titulares de dados, em relação a seus corpos físicos e digitais.

A regulação pela instituição de uma norma é o primeiro passo para a concretização de um direito, e a política pública é responsável por implementar as disposições legais e operacionalizar o sistema de proteção criado. Entretanto, há que se ter em mente que lei (que veicula a norma), regulação e política pública, embora complementares, não se confundem. Enquanto a lei é um instrumento de disciplinamento da vida em sociedade que opera inicialmente no plano jurídico dogmático, a regulação e a política pública operam no mundo

[1] "[...] Platforms in sum, are a new type of firm; they are characterised by providing the infrastructure to intermediate between different user groups, by displaying monopoly tendencies driven by network effects, by employing cross-subsidisation to draw in different user groups, and by having a designed core architecture that governs the interaction possibilities. [...] All these characteristics make platforms key business models for extracting and controlling data. By providing a digital space for others to Interact in platforms, position themselves so as to extract data from natural processes (weather conditions, crop cycles, etc.) and from other businesses and users (web tracking, usage data, etc.). They are an extractive apparatus for data." (SRNICEK, 2017, p. 48).

dos fatos, lastreando-se na lei como suporte. A regulação compreende a instituição de um sistema para o controle de regras e standards estabelecidos para um dado setor, segmento ou atividade. Já a política pública consiste em um conjunto de ações coordenadas para a resolução de problemas complexos, com foco no fomento de determinados comportamentos e valores desejáveis e na coibição de outros, que coloquem em risco o interesse público o os objetivos sociais que visa resguardar.

Pode-se dizer que a regulação amplia a esfera de operação da norma, por lidar com exercício de poder por meio de arranjos institucionais instituídos para responder ao comportamento dos regulados, e que a política pública extrapola o âmbito da regulação por ser ainda mais multidisciplinar e contar com o exercício de poder para além da estrutura institucional, lidando com os efeitos da norma e da regulação no mundo dos fatos, como esse funcionamento impacta na cultura para engajamento com os valores e comportamentos que a política pública visa fomentar. Analisando o objeto da pesquisa para tese, tem-se que, estudar a efetividade da Política Nacional de Proteção de Dados Pessoais implica em analisar a regulação do processamento de dados pessoais, disciplinado pela LGPD (lei, instrumento inicial da regulação do processamento de dados pessoais e suporte normativo da política pública).

Tanto a regulação quanto a política pública demandam planejamento e medição de resultados para se aferir níveis de efetividade e se projetar eventuais correções para melhoramento contínuo. Para atingir os resultados a regulação e a política pública se valem de estratégias de reforço, de *enforcement.* A designação em inglês, *enforcement*, é adotada porque tem significado mais amplo do que simplesmente aplicar a lei, incluindo esforços para medir os resultados da implementação da regulação e reformular estratégias para alcançar a efetividade, atingir os resultados esperados, ou seja, para resolver os problemas que levaram à criação da regulação. Quando uma norma entra em vigor, ela já possui eficácia (já existe a concretização normativa, no dizer de Marcelo Neves (2011, p. 43-47)), em termos de aplicabilidade e de capacidade para a produção de efeitos. O *enforcement* tem lugar como meio de buscar a efetividade (o que Marcelo Neves (2011, p. 47-48) designa de vigência social), que une a eficiência quanto aos meios empregados e aos processos com o alcance dos objetivos traçados, isto é, com a realização da finalidade da norma. A política pública se utiliza da regulação como instrumento para o alcance dos seus objetivos. Tanto a regulação quanto a política pública resultam de processos de tomada de decisão administrativa, mas devem levar em conta na medição de resultados a ação de entes não estatais.

Entre os objetivos nos quais se baseiam as normas de proteção de dados está a promoção da cultura de privacidade e de proteção de dados, além do empoderamento do titular (BRASIL,

2018). Ademais, na realidade dinâmica da sociedade informacional, o titular dos dados e os agentes de tratamento (regulados) têm papel decisivo na efetividade do direito à proteção de dados. Considerando que cultura tem um conceito contestado, cabe ressaltar que o termo é utilizado no sentido semiótico, proposto por Geertz (2008, p. 16), como um emaranhado de signos interpretáveis, tidos como atos simbólicos que constituem um discurso (GEERTZ, 2008, p. 18), cuja interpretação leva a uma investigação da importância não aparente para a reprodução e compartilhamento de determinados comportamentos e crenças. Assim, para esta tese, cultura significa as concepções e práticas compartilhadas entre as pessoas na sociedade, entre as organizações no mercado e entre as entidades públicas no governo.

1.1 Breves considerações sobre o problema de pesquisa, hipótese, objetivos gerais e específicos

Considerando que a necessidade de convergência no âmbito da regulação do tratamento de dados pessoais na sociedade informacional, conectada em rede transnacional, resulta em normas de conteúdo principiológico similar, o *enforcement*, ou seja, as estratégias empregadas para reforço positivo e negativo de comportamentos e valores preconizados pela política pública desempenha papel determinante para a efetividade dos resultados. A Política Nacional de Proteção de Dados contempla dois grandes propósitos, quais sejam, de estabelecer um ambiente de negócios e de prestação de serviços mais respeitoso e transparente, e a promoção do empoderamento do titular de dados, a partir da autodeterminação informativa como fundamento. A tese dedicou-se a investigar, a partir da comparação da implementação da Política Nacional de Proteção de Dados brasileira com a política de privacidade existente em nível federal na Austrália: quais medidas de *enforcement* seriam aptas a dotar a política pública brasileira de maior efetividade para que o titular de dados não precise apelar para a judicialização? E a hipótese testada é a de que a regulação deve apostar em estratégias que incentivem a responsividade e o foco na prevenção por parte dos agentes de tratamento e o acesso, sem ônus para os titulares dos dados, a meios de reivindicação de seus direitos que sejam adicionais à via judicial, como forma pedagógica de fortalecer a cultura da privacidade e da proteção de dados (entre os titulares dos dados e entre os agentes de tratamento).

A pesquisa foi orientada pelos objetivos gerais de identificar elementos e efetividade e inefetividade na Política Nacional de Proteção de Dados Pessoais em estruturação no Brasil, sob a perspectiva da proteção do corpo digital do titular de dados pessoais, e, a partir dessa identificação, propor medidas para o seu contínuo aprimoramento. As atividades de pesquisa

buscaram atingir os seguintes objetivos específicos: 1. contextualizar a dinâmica da sociedade informacional (RODOTÀ, 2008, CASTELLS, 2013; DE LIMA, 2020) em que os dados pessoais passam a figurar como mercadoria, destacando os meios empregados pelas plataformas digitais (SRNICEK, 2017) para viabilizar a operação do ciclo de despossessão de dados pessoais (ZUBOFF, 2019). O ciclo de despossessão é a fonte para a composição do corpo digital formado a partir da criação de uma identidade composta de informações construídas sobre o titular dos dados. A noção de corpo digital ilustra a complexidade enfrentada pelos Estados-nacionais para lidar com a regulação dos dados pessoais em movimento, tendo em vista a natureza transfronteiriça dos fluxos e as modificações existentes nas relações internacionais, com o encurtamento das fronteiras físicas em um mercado transnacional em rede. Outros objetivos específicos foram: 2. analisar criticamente a estrutura da Política Nacional de Proteção de Dados Pessoais no Brasil; 3. investigar a estrutura existente na Austrália em seu sistema de proteção à privacidade e como esse sistema tem sido progressivamente aprimorado; 4. destacar o papel relevante dos mecanismos de *enforcement* no regime regulatório para a eficácia da proteção de dados pessoais em movimento; e, 5. propor modificações nas políticas públicas brasileiras e australianas em prol do aumento da efetividade da proteção ao titular de dados.

1.2 Aspectos metodológicos

A pesquisa bibliográfica, exploratória e crítica foi desenvolvida com emprego de raciocínio hipotético abdutivo[2], mesclando abordagens qualitativas dedutivas e indutivas. As técnicas de pesquisa empregadas foram revisão bibliográfica e análise documental. A verificação da efetividade das políticas públicas sob o ponto de vista dos meios disponíveis ao titular dos dados para buscar a efetivação de seus direitos foi realizada a partir da análise das normas que dão suporte às políticas públicas (LGPD e *Privacy Act 1988* (Cth)), assim como de decisões judiciais e administrativas sobre a aplicação dos suportes normativos, proferidas entre os anos de 2020 e 2022, a fim de averiguar como a execução do sistema de proteção instituído pelos suportes normativos é executada, de fato. O recorte temporal se deve ao período de vigência da LGPD, que entrou em vigor em setembro de 2020, bem como se justifica por um

[2] O raciocínio hipotético abdutivo trata-se de resolver o problema de pesquisa partindo de observações e evidências para construir explicações. Atocha Aliseda (2006, p. 28) destaca que "*abduction* is a reasoning process invoked to explain a puzzling observation. A typical example is a practical competence like medical diagnosis. [...] Abduction is thinking from evidence to explanation, a type of reasoning characteristic of many different situations with incomplete information."

aumento da preocupação com a privacidade na Austrália, em razão de uma série de violações de dados ocorridas no país a partir de 2019. Além disso, o mundo foi colocado em alerta em relação à privacidade e à proteção de dados após o advento da pandemia da COVID-19, que acelerou o fenômeno da disseminação das comunicações e interações remotas, para trabalho e estudo, devido às políticas de distanciamento social. Da mesma forma, as relações sociais e o consumo também mudaram e passaram a ser intermediados por plataformas durante a pandemia, consolidando-se em hábitos corriqueiros no contexto pós-pandêmico.

Para o levantamento de decisões judiciais e administrativas foram utilizados os indexadores "LGPD", "Lei nº. 13.709/2018" e "Lei Geral de Proteção de Dados", para o contexto brasileiro, e "Privacy Act 1988 (Cth)", para o contexto australiano. Para o contexto brasileiro, a pesquisa foi realizada junto à Autoridade Nacional de Proteção de Dados (ANPD) e aos tribunais superiores, Superior Tribunal de Justiça (STJ) e Supremo Tribunal Federal (STF), com o objetivo de identificar os temas mais sensíveis da *LGPD* e como os tribunais superiores têm aplicado a lei. Na Austrália, a pesquisa foi realizada no *Office of the Australian Information Commissioner* (OAIC), no *Administrative Appeal Tribunal* (AAT) e nos tribunais federais competentes, o *Federal Courts of Australia* (FCA) e o *Federal Circuit and Family Courts of Australia* (FCFCOA).

A pesquisa também explorou o método funcional de direito comparado (MICHAELS, 2019), a partir do estudo do contexto brasileiro de privacidade e proteção de dados em justaposição por contraste com o contexto australiano de privacidade. A respeito do emprego de direito comparado, Ana Lucia de Lyra Tavares (2000) destaca que o papel do direito comparado é realizar a comparação entre sistemas jurídicos que possuem elementos comuns quanto às suas características históricas, estruturais e de hierarquia das fontes de produção do direito, para identificar semelhanças e diferenças, com vistas ao aperfeiçoamento desses sistemas, e, por vezes, à sua harmonização (TAVARES, 2000, p. 151). Trata-se, portanto, de instrumento capaz de lidar com elementos variados além dos aspectos jurídicos, em uma necessária perspectiva interdisciplinar, podendo-se admitir, inclusive, em pesquisa de direito comparado entre direito, ou um dado sistema jurídico com outro campo de conhecimento, por exemplo, direito e literatura, direito e arte, direito e geografia etc. (MCEVOY, 2012, p. 156).

Marc Ancel (1980) afirma que, inicialmente, a aplicação do direito comparado era vista como adequada apenas para comparar normas com a mesma origem e em um contexto privado. No período entre as duas guerras mundiais, o método comparativo passou a ser utilizado como instrumento de aperfeiçoamento dos sistemas jurídicos, para orientar a modelagem de novas normas, tanto privadas quanto públicas, a partir do confronto, inclusive, de sistemas com

diferentes vieses, como o *civil law* e o *common law* (ANCEL, 1980, p. 36). Portanto, não há qualquer prejuízo ou obstáculo metodológico em relação à pesquisa realizada, uma vez que a comparação foi feita entre sistemas de diferentes tradições (o sistema australiano de *common law* e o sistema brasileiro de *civil law*).

Quanto a opção pela modalidade funcional de direito comparado, destaca-se que decorre dos seus elementos basilares, que coadunam com os objetivos da tese. Conforme menciona Ralf Michaels (2019), entre os elementos do método funcionalista citam-se: trata-se de método não doutrinal, ao passo que expande a investigação das normas para além da sua estrutura e argumentos, focando nos efeitos e consequências delas decorrentes na realidade; a compreensão de que o objeto de investigação deve ser entendido sob a luz da sua relação funcional com a sociedade, ao passo que o direito e a sociedade, embora distintos, se conectam e impactam mutuamente (vale dizer, o direito é criado para desempenhar uma função na sociedade e ao mesmo tempo constitui parte dela); a função em si é o eixo de comparação entre os sistemas sob investigação; a análise da função pode ser tomada como um critério avaliativo que direcione para o aprimoramento (MICHAELS, 2019, p. 348). Dito isso, convém destacar que embora a pesquisa dedique-se nos primeiros capítulos à contextualização da sociedade informacional e a uma breve digressão histórica da derivação do direito de privacidade em direitos à proteção de dados pessoais e à autodeterminação informativa, a pesquisa não tem viés dogmático, ou foco nos detalhes atinentes à Teoria do Direito. Por ter a política pública de privacidade e proteção de dados como objeto de pesquisa, e o objetivo geral de investigar a efetividade dessa política, a tese adota viés sociojurídico.

Conforme asseveram Miracy Barbosa de Sousa Gustin e Maria Tereza Fonseca Dias (2010, p. 22), a vertente jurídico- sociológica de pesquisa investiga o fenômeno jurídico em ambiente mais amplo, preocupando-se com a facticidade do direito e com sua interação, além da interdependência com os campos sociocultural, político e antropológico. Assim, enquanto a vertente de pesquisa jurídico-dogmática preocupa-se, prioritariamente, com a noção de eficiência, a vertente jurídico-sociológica, partindo do sentido de eficácia,

> estuda a realização concreta dos objetivos propostos pela lei, por regulamentos de políticas públicas ou sociais. A análise de efetividade que essa vertente também faz, cumpre o mesmo papel da eficácia, complementando-o com a análise de demandas e de necessidades sociais e de sua adequação aos institutos jurídicos, sociais e políticos (GUSTIN, DIAS, 2010, p. 22).

Impende reiterar que a tese se ocupa da investigação dos elementos de efetividade e de inefetividade da Política Nacional de Proteção de Dados, com intuito de avaliar a concretização dos seus objetivos. Ademais, as conclusões aportadas possuem sugestões para o melhoramento

contínuo da política pública em questão, de maneira a torná-la mais vocacionada à concretização daqueles objetivos.

Quanto ao marco teórico, por ter como objeto uma política pública de natureza interdisciplinar, a tese adota referenciais teóricos temáticos, destacados ao referir-se aos conceitos que permeiam o problema de pesquisa e a hipótese. O conceito de proteção de dados como direito autônomo tem como referências Danilo Doneda (2014), Laura Schertel (2014) e Marion Albers (2014). Quanto à compreensão do conceito de política pública, o referencial teórico adotado é o contorno conceitual desenvolvido por Maria Paula Dallari Bucci (2006; 2019). Bucci entende política pública como

> o programa de ação governamental que resulta de um processo ou conjunto de processos juridicamente regulados […] visando coordenar os meios à disposição do Estado e as atividades privadas para a realização de objetivos socialmente relevantes e politicamente determinados. (BUCCI, 2006, p. 39).

Bucci destaca ainda em artigo com foco na abordagem direito e políticas públicas que política pública "é a ação governamental coordenada e em escala ampla, para estender as conquistas civilizatórias a todas as pessoas." (BUCCI, 2019, p. 809), sendo traduzida numa "ação governamental coordenada e em escala ampla, atuando sobre problemas complexos, a serviço de uma estratégia determinada, tudo isso conformado por regras e processos jurídicos." (BUCCI, 2019, p. 816).

A tese adota como referencial teórico para "efetividade" a compreensão de Maria Paula Dallari Bucci (2006), de efetividade como o ideal da política pública, que extrapola os âmbito da validade e da eficácia. Ou seja, que vai muito além da mera conformidade do seu texto com o regramento jurídico que lhe lastreia (validade), e exorbita, ainda, o simples cumprimento das normas do programa de ação instituído pela política pública. Assim, para Bucci, efetividade de uma política pública consiste em "resultar no atingimento dos objetivos sociais (mensuráveis) a que se propôs, obter resultados determinados em certo espaço de tempo" (BUCCI, 2006, p. 43). Reiterando o viés sociojurídico da pesquisa, a tese adota como referencial teórico para efetividade a noção esposada por Miracy Barbosa de Sousa Gustin e Maria Tereza Fonseca Dias (2010), que destacam que a efetividade consiste na busca pela facticidade do direito em meio a sua relação com os demais campos (sociocultural, político, antropológico, entre outros) (2010, p. 22). Em outras palavras, a efetividade passa pela mensuração da realização concreta de objetivos propostos pela política pública, no caso do objeto da tese, a tutela à dignidade pela proteção do corpo digital formado pelos dados pessoais em fluxo (em adaptação à noção forjada por Stefano Rodotà de corpo eletrônico (RODOTÀ, 2008)).

Os referenciais teóricos para regulação são John Braithwaite (1992; 2006; 2008; 2016), Netta Barak-Corren e Yael Kariv Teitelbaum (2021), compreendendo por regulação o estabelecimento de regramentos para determinada atividade ou campo. E para *enforcement* a tese adota como referencial teórico John Braithwaite (1988) e Peter Grabosky (1988; 2013).

A tese se dedica aos desafios impostos à preservação e concretização dos direitos fundamentais pela sociedade informacional. Para tratar de direitos fundamentais a tese adota José Adércio Leite Sampaio (1998; 2010) e George Marmelstein (2019) como referenciais teóricos, e Otto von Gierke (2016) para tratar especificamente do conceito de direitos da personalidade.

1.3 Originalidade da tese e contribuições para o conhecimento

A pesquisa ora apresentada é pioneira ao analisar a Política Nacional de Proteção de Dados sob o olhar e perspectiva da política pública. Parte-se do estudo da derivação da privacidade em proteção de dados, explorando de maneira panorâmica as normas apontadas pela doutrina como mais relevantes no caminho até o reconhecimento da proteção de dados como direito autônomo. Passa, ainda, pelo estudo da LGPD, abordando o contexto prévio e contemporâneo à sua aprovação e o caminho até a sua entrada em vigor, destacando, entretanto, que assim o faz para observar o que estava contido no desenho original da política pública. Ou seja, a LGPD é estudada enquanto suporte normativo da Política Nacional de Proteção de Dados, em que está contido o design da política. Entretanto, para cumprir com sua proposta de contribuir para o melhoramento contínuo da política pública em estudo, a tese vai além ao analisar como a política tem sido implementada, como tem funcionado o sistema de proteção por ela instituído e o quão efetivo ele é na proteção do titular de dados.

A presente tese é pioneira na abordagem da proteção de dados sob a perspectiva da política pública[3] com intuito de averiguar pontos de inefetividade. O único trabalho acadêmico encontrado adotando a perspectiva de política pública é a monografia de autoria de Raquel Gitirana Torquato dos Santos[4] (2020), submetida ao Instituto Serzedello Côrrea do Tribunal de Contas da União, como requisito para a obtenção de grau de especialista. Entretanto, a referida

[3] Vide pesquisa do portal "Periódicos CAPES" que não retorna resultado para o indexador "política pública de proteção de dados", de 1981 à 2023 https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php/buscador-primo.html. Acesso em 15 Nov. 2023. O mesmo ocorre com o uso do indexador "política nacional de proteção de dados".

[4] DOS SANTOS, Raquel Gitirana Torquato. **A Lei Geral de Proteção de Dados Brasileira: uma política pública regulatória.** 2020. Monografia (Especialização em Avaliação de Políticas Públicas). Instituto Serzedello Corrêa – Escola Superior do Tribunal de Contas da União, Brasília, 2020.

monografia contextualiza de maneira descritiva os projetos de lei que resultaram na aprovação da LGPD e analisa o desenho da lei, traçando considerações sobre a futura implementação da política que ela subsidia. A autora ressalta que os atores envolvidos na concretização da política pública desenhada são os cidadãos, as empresas privadas, o poder público e a ANPD (DOS SANTOS, 2020, p. 56) e enfatiza o papel crucial dos cidadãos para a efetividade da política pública, ao passo que são os titulares de dados pessoais e a força motriz das interações, destacando o quanto a mudança cultural seria crucial para o entendimento da importância dos dados (DOS SANTOS, 2020, p. 56-57), sendo esse o único ponto congruente entre a tese e a monografia. Vale ressaltar, a tese explora além do plano normativo, adotando um viés sociojurídico, com propositura de ações corretivas, extrapolando a simples análise do desenho da norma.

A grande maioria dos livros e pesquisas científicas no campo da proteção de dados adota uma visão dogmática, enfocando os aspectos inerentes ao seu reconhecimento como direito autônomo fundamental no âmbito jurídico (PANITZ, 2007; RODRIGUEZ, 2010; AGUIAR, 2015; MENDONZA, BRANDÃO, 2016; DONEDA, 2020; TEPEDINO, FRAZÃO, OLIVA, 2020; SOMBRA, 2020; GROSSI, 2022) e o seu impacto em determinados campos, como nas relações de trabalho (RAMOS, GOMES, 2019; GULARTE, 2020), na contabilidade, na atividade de cartórios (ALMEIDA, 2022), nas fusões e aquisições empresariais (SANTOS, 2022), no exercício da medicina e na gestão de bancos de dados genéticos (BERNASIUK, 2016; SIMÕES, 2018; BELLARMINO, 2018; BOTRUGNO, 2023), na defesa do consumidor (DENNY, LEÃO, 2020; CAVALCANTI, 2021; ALVES, SOUZA, 2021; FERNEDA, ZILIOTTO, KLEIN, 2023), aplicação de técnicas de rastreamento durante a pandemia da COVID-19 (MARTINS, FERREIRA, CASTRO, MACEDO JÚNIOR, LIMA, 2020; JORGE, OLIVEIRA, MACHADO, LIMA, OTRE, 2020; SAAVEDRA, MENEZES, 2020; CAMARGO, SANTOS, ARIENTE, GOMES, 2020; SANTOS, 2021; NEGRI, BATISTA, 2021).

Algumas produções acadêmicas se debruçam sobre o entendimento da proteção de dados numa era de vigilância e de existência digital (GUTWIRTH, LEENES, HERT, 2014; GUTWIRTH, POULLET, HERT, LEENES, 2011). Outras são dedicadas a aspectos específicos da aplicação da LGPD, sobre o consentimento como base legal (BIONI, 2021), o legítimo interesse e sua aplicabilidade como base legal (GLITZ, 2019), o dever de *accountability* dos agentes de tratamentos de dados (BIONI, 2022), as atividades de *profiling* (MACHADO, 2018; MARTINS, 2022), sobre a Autoridade Nacional de Proteção de Dados – ANPD (DE LIMA, 2020), o tratamento de dados pessoais sensíveis (TEFFÉ, 2022), os direitos do titular (GONÇALVES, 2022; RIEMENSCHNEIDER, MUCELIN, 2021), responsabilidade civil dos

agentes de tratamento (MAIMONE, 2022), o encarregado de proteção de dados (QUEIROZ, 2022), a caracterização dos agentes de tratamento (LIMA JÚNIOR, SILVA, CÂMARA, RODRIGUES, 2022), o uso de câmeras com tecnologia de reconhecimento facial para a persecução penal (ALMEIDA, 2022). Existe uma gama de trabalhos voltados a orientar agentes de tratamento na adequação aos requisitos da LGPD (DONDA, 2020.; GARCIA, AGUILERA-FERNANDES, GONÇALVES, PEREIRA-BARRETO, 2020) e quanto à interpretação da lei (PINHEIRO, 2023; MARTINS, LONGHI, FALEIROS JÚNIOR, 2022; MALDONADO, BLUM, 2023). Em linhas gerais, os trabalhos científicos encontrados sobre proteção de dados adotam uma abordagem de viés dogmático, focando no que o texto legal preconiza e na potência que tem caso seja executado e concretizado no mundo dos fatos.

Assim, a originalidade da tese decorre não somente da análise do tema sob a perspectiva da política pública, mas também pelo emprego de direito comparado, utilizando para a comparação política instituída na Austrália, cujo sistema jurídico é raramente explorado em pesquisas de direito comparado brasileiras. Ademais, a política pública de proteção de dados foi instituída para contingenciar um problema transnacional no âmbito da sociedade informacional, e a tese busca contribuir com o aprimoramento dessa política pela inclusão de mecanismos de *enforcement* vocacionados a endereçar as demandas individuais dos titulares de dados pessoais, incrementando a tutela ao corpo digital. Conforme mencionado, a noção de efetividade adotada na tese parte do ponto de vista da tutela dos dados pessoais em fluxo. Impende ressaltar que a comparação realizada prezou pela diversidade, ao investigar e justapor o objeto de estudo a um sistema pouco estudado no Brasil: o sistema jurídico australiano. Cumpre destacar que inúmeros estudos que empregam direito comparado o fazem com parâmetro à sistemas jurídicos europeus ou ao norte-americano.

Além da óbvia importância do tema, é fundamental ressaltar que a tese está alinhada à Estratégia Nacional de Ciência, Tecnologia e Inovação, registrada na redação da *Portaria nº 6.998 do Ministério da Ciência, Tecnologia e Inovação (MCTI), de 10 de maio de 2023*, apresentando resultados científicos de inovação que contribuem para a melhoria das condições de vida da população e para a resolução de problemas sociais, propondo soluções para a formulação, implementação, monitoramento e avaliação de políticas públicas, conforme o art. 2º, §4º, II, da Portaria (BRASIL, 2023).

1.4 Estrutura da tese

A tese é desenvolvida em cinco capítulos, além da Introdução e das Conclusões. O Capítulo 2 contextualiza as implicações dos direitos à privacidade e à personalidade na sociedade da informação. O Capítulo 3 discute como a regulamentação da privacidade foi desenvolvida até a derivação para a lei de proteção de dados e contempla os desafios impostos aos estados-nação pelas plataformas. O Capítulo 4 explora a política pública brasileira de proteção de dados, desde a publicação da *Lei nº. 13. 709/2018* (LGPD) até a implementação de seus requisitos, abrangendo as estruturas e estratégias para fazer valer a privacidade e a proteção de dados. O Capítulo 5 argumenta que olhar para a experiência australiana, em vez de examinar apenas os países europeus, pode beneficiar a melhoria contínua da referida política pública, explorando os mecanismos de *enforcement* da privacidade existentes na *Commonwealth* australiana. O Capítulo 6 aponta estratégias, como a adoção de uma abordagem dialógica durante as investigações e a existência de uma forma administrativa de tratar as reclamações de privacidade, com a possibilidade de indenizações por perdas, que podem aumentar a eficácia da proteção de dados no Brasil, com foco na proteção efetiva dos direitos da personalidade. A tese conclui que embora nenhuma estrutura regulatória existente possa garantir a proteção de dados com máxima efetividade, a fiscalização e a existência de uma esfera administrativa para endereçar individualmente as petições e denúncias relativas às violações ao direito de proteção de dados desempenha papel crucial na formação da cultura, promovendo a conscientização sobre a importância de preservar os direitos de privacidade. Propõe-se a reflexão acerca da importância de que o acesso a essa esfera administrativa seja sem custo para o titular de dados, como meio de assegurar a democraticidade dos instrumentos de concretização do direito de proteção de dados, tanto para fins de empoderamento do titular, quanto para assegurar protagonismo da ANPD em liderar o melhoramento contínuo da política pública. A partir das evidências encontradas na análise comparativa efetuada sugerem-se modificações na execução da política pública brasileira.

2 SOCIEDADE INFORMACIONAL: ubiquidade da tecnologia, vigilância, datificação, humanidade digital e proteção de dados como um direito fundamental autônomo

Este capítulo argumenta que com o avanço tecnológico e com a reformulação do capitalismo a partir da crise econômica de 2008 (SRNICEK, 2017; ZUBOFF, 2019; VÉLIZ, 2021), fomentando o espraiamento das plataformas digitais, os dados, especialmente os dados pessoais, foram convertidos em *commodity*. A adoção da plataforma como modelo predominante de interação, consequentemente colocando os sujeitos na posição de fornecedores de matéria prima bruta para acumulação de riquezas, os expõe a uma vulnerabilidade que é perigosa para a livre formação da personalidade e para a dignidade humana (RODOTÁ, 2008). A constatação de que a proteção ao corpo digital composto pelos dados pessoais expropriados é importante para a manutenção dos direitos da personalidade e para a preservação da vida humana passa a ser a justificativa para a regulação de direitos fundamentais derivados da privacidade: direitos à proteção de dados e à autodeterminação informativa.

Vive-se em uma sociedade informacional (DE LIMA, 2020; CASTELLS, 2013), na qual o indivíduo está gradativamente mais vulnerável[5] a ser manipulado e objetificado, devido à exploração de seus dados pessoais. Reconhecer isso e considerar que essa informação compõe um corpo digital, e merece especial proteção, é a justificativa para o movimento de regulamentação do tratamento de dados pessoais ao redor do mundo. A adoção do termo "sociedade informacional" em vez de "sociedade da informação" é feita para sublinhar como a informação é a *commodity* mais poderosa nos dias de hoje. Na sociedade informacional (vale a pena reforçar) a própria informação se torna o produto ou serviço, é um valor em si mesma. O termo sociedade da informação permite uma interpretação falaciosa de que se vive num tempo em que a informação reina, no sentido de um amplo acesso ao conhecimento. Ao contrário, o contexto da sociedade informacional é o de que o processamento eficiente da informação mede

[5] Pesquisas recentes demonstram a possibilidade de se inferir estados emocionais e mesmo características psicológicas com base na análise de pegadas digitais, ou seja, da análise das interações feitas em redes sociais (likes, seguir ou não seguir páginas) e postagens. Importante notar que aqui estou tratando de posts públicos e cujo conteúdo por si só não constitui dado pessoal. A respeito do uso de psicométricas para identificar potenciais alvos para persuasão indico os artigos "*Psychological targeting as an effective approach to digital mass persuasion",* de Matz, Kosinski, Nave e Stillwell e "Human and computer personality prediction from digital footprints", de Joanne Hinds e Adam Joinson. Na Austrália tive contato com pesquisas em psicologia comportamental e da linguagem que, a partir da medição de estados emocionais acerca de questões contemporâneas que o Direito e os sistemas legal e político buscam responder (como o enfrentamento da pandemia da COVID-19, o combate ao terrorismo, entre outros) propõem medir o nível de engajamento dos cidadãos com o sistema legal, para aferir o quão efetivo ele está sendo em termos de cumprir com os objetivos que usa como justificativa. Para aprofundamento, recomenda-se a leitura dos trabalhos da Professora Cassandra Sharp.

o nível de poder que se tem e a aptidão para influenciar e gerar riqueza, e para garantir a competitividade muitas vezes o uso de desinformação é feito como estratégia de dominação. O desenvolvimento da tecnologia, sobretudo no que diz respeito à facilidade e acessibilidade de armazenamento de quantidades massivas de dados, transformou o indivíduo na principal fonte de matéria-prima para a produção de riqueza, aumentando a vulnerabilidade à modulação e à objetificação da vida humana.

Com a escalada da internet e da interconectividade, os fluxos de dados tendem a ocorrer de forma transnacional, exacerbando essa vulnerabilidade individual e o poder das empresas, que, utilizando plataformas (SRNICEK, 2017, p. 6) em seus negócios, podem expandir seu universo de atuação de forma ampla e capilarizada na vida cotidiana[6] (SRNICEK, 2017, p.89-90). A interação com as plataformas torna os indivíduos suscetíveis a estímulos contínuos e à coleta de dados comportamentais, sobre hábitos e preferências de maneira a traçar um perfil acurado sobre as tendências de cada um. A pessoa natural tornou-se alvo do poder instrumentário que utiliza a vigilância como ferramenta de despossessão (ZUBOFF, 2019, p. 203). Os dados extraídos são utilizados para criar um perfil detalhado, permitindo a previsão comportamental e a capacidade de influenciar ações futuras. Numa sociedade informacional, cada interação contribui para o processamento de dados e gera informações valiosas.

À medida que a vida humana se torna mais interativa e digitalmente dependente, é criada uma versão digital de todos, uma versão que não é necessariamente um reflexo de quem a pessoa é, mas produto de dados interrelacionados e pegadas digitais. Conforme argumentado por Couldry e Mejias (2019, p. 84-87), os seres humanos vivem em um esquema neocolonial, no qual as relações de dados, entendidas como "novo tipo de relações humanas que dão às corporações uma visão abrangente de nossa socialidade, permitindo que a vida humana se torne um insumo ou recurso para o capitalismo" (COULDRY, MEJIAS, 2019, p. 85). Então, os recursos que formam o corpo digital representam uma nova colônia não como uma localização geográfica, como no ocorrido na colonização tradicional, mas traduzida numa realidade onipresente em que associações, conhecimento e significado que são centrais na vida humana ocorrem no digital, permitindo a extração contínua de dados (COULDRY, MEJIAS, 2019, p. 85). Histórico de pesquisa, hábitos de consumo, lugares visitados, interações com outras

[6] "[...] The platform, on the Other hand, has data extraction built into its DNA, as a model that enables Other services and goods and technologies to be built on top of it, as a model that demands more users in order to gain network effects, and a digitally based médium that makes recording and storage simple. All of these carachteristics make platforms a central model for extracting data as a raw material to be used in various ways. [...] collecting massive amounts of data is central to the business model and the platform provides the ideal extractive apparatus." (SRNICEK, 2017, p. 89-90).

pessoas, crenças religiosas, meios de transporte utilizados, *hobbies*, atividades físicas realizadas, posse material de objetos *smart*, estado emocional, tempo gasto em plataformas digitais e atividade pessoal, acadêmica ou profissional são exemplos de entradas traduzidas em recursos colonizados.

Por meio de plataformas, a Inteligência Artificial (IA), seus componentes e derivados extraem informações para criar um perfil quantificável que objetifica o ser e sua vida - o corpo digital. Esse corpo digital é utilizado para classificar os sujeitos e subsidiar a tomada de decisões sobre seus interesses, com repercussões na vida material (RODOTÀ, 2008; COULDRY, MEJIAS, 2019; ZUBOFF, 2019). Por exemplo, esses dados podem ser usados para determinar quem tem o melhor desempenho físico, quem é mais produtivo em um contexto profissional e tem maior probabilidade de atingir as metas de uma empresa; até mesmo quem tem maior probabilidade de adoecer por causa de seus hábitos e representa um risco maior para um serviço de seguro ou quem tem maior probabilidade de ter filhos e ter possíveis problemas de gerenciamento de tempo por ter que cuidar das crianças. Considerando que o corpo digital desempenha papel relevante e inegável nas oportunidades da vida material, o entendimento de que ele merece proteção e reconhecimento como parte importante da dignidade humana é incorporado aos sistemas jurídicos (RODOTÀ, 2008, p. 151-152).

A justificativa para a regulação do tratamento de dados pessoais, com a necessidade de melhor proteção do corpo digital como integrante da dignidade da pessoa humana, leva à derivação da privacidade como gênero (proteção geral e estática - o direito a ser deixado em paz, a ter uma esfera íntima da vida) em dois direitos autônomos mais específicos: a proteção de dados (proteção dos dados pessoais em movimento; proteção dinâmica) e a autodeterminação informativa (o poder de definir como os dados pessoais vão ser usados, quem pode aceder-lhes, com que finalidade) (ALBERS, 2014, p. 214-215). O presente capítulo esclarece como a sobreposição entre o material e o digital impacta na influência da autonomia, e como a constatação dessa ameaça é o fio condutor da derivação da privacidade em proteção de dados e autodeterminação informativa. Esse esclarecimento é importante para a tese à medida em que elucida questões emergentes da sociedade informacional e do capitalismo de plataformas e de vigilância, assim como demonstra a complexidade da regulação de direitos fundamentais no contexto da sociedade informacional.

2.1 Derivação e especialização da tutela dos direitos da personalidade: direito à proteção de dados como meio de tutela do corpo digital

Esta seção demonstra como a derivação da privacidade como direito da personalidade em direito de proteção de dados e direito de autodeterminação informacional ocorreu para promover o empoderamento do titular dos dados na sociedade informacional. A privacidade, a proteção de dados e a autodeterminação informativa são direitos fundamentais e, portanto, relacionados à dignidade humana. Com fulcro na crescente influência dessa interação com plataformas digitais e com novas tecnologias, houve progressiva modificação na interpretação da privacidade e das suas barreiras. O direito à privacidade remonta à modernidade e à concepção do homem como sujeito de direitos, sendo pensado inicialmente como limitador das interferências estatais na vida privada e na intimidade, como um direito de ser deixado só (WARREN, BRANDEIS, 1890; SAMPAIO, 1998; RODOTÀ, 2008). Essa concepção estática passa a ser tida como insuficiente ante à dinamicidade da realidade da sociedade informacional, aflorando a movimentação em organismos internacionais e em decisões jurisdicionais locais pelo reconhecimento de um direito dinâmico, que tutelasse os dados em movimento (RODOTÀ, 2008).

A definição e a origem dos direitos da personalidade são controversas. Entretanto, existe um consenso razoável em torno do reconhecimento de que a concepção contemporânea de direitos da personalidade encontra fundamento na obra de Otto von Gierke (SAMPAIO, 1998, p. 51; LUZ, BRITO, 2018; DONEDA, ZANATTA, 2022), ainda no século XIX. Por personalidade entende-se a capacidade jurídica, no dizer de Adriano de Cupis (2008, p. 19), geralmente definida como a susceptibilidade do sujeito de ser titular de direitos e obrigações jurídicas. A personalidade em si não se identifica com os direitos ou com os deveres, mas é condição para que se possa cogitar a legitimidade de obrigações, para que o sujeito possa ser responsabilizado pelas obrigações que assume. Assim, entende-se por direitos da personalidade os direitos que são essenciais para que o sujeito preserve essa aptidão de ser titular de obrigações, sendo, entre outros aspectos, essencial à proteção da sua consciência, da sua capacidade de discernimento e de escolha, de autorrepresentação e de autoconstrução do seu eu no mundo jurídico. Dito isso, é fato que a qualidade jurídica da personalidade é efetivada normativamente pelo direito positivo, assim como destacado por de Cupis[7] (2008, p. 19), ainda

[7] "Uma tal qualidade jurídica é produto do direito positivo, e não uma realidade que este encontre já constituída na natureza e que se limite a registrar tal como a encontra. A susceptibilidade de ser titular de direitos e obrigações

que tendo a origem justificada no resgate de conceitos do jusnaturalismo (SAMPAIO, 1998, p. 50).

Os direitos da personalidade ganham maior expressão e escalabilidade com o racionalismo moderno, que consagrou a ideia de direitos fundamentais em documentos como o *Bill of Rights* (1689) e a *Declaração Universal dos Direitos do Homem e do Cidadão* (1789). E o reconhecimento desses direitos ganha impulso num contexto de pós-guerras mundiais, com a sua previsão em declarações internacionais de direitos, como a *Declaração Universal dos Direitos do Homem* (1948) e a *Convenção Europeia dos Direitos Humanos* (1950) e com a emergência da dignidade como conceito chave nas Constituições Nacionais (especialmente após a II Guerra Mundial) (MARMELSTEIN, 2019, p. 8-18).

A distinção entre direitos humanos e direitos fundamentais se dá com base no nível jurisdicional em que a tutela é estabelecida e no meio pelo qual se opera a sua formalização. Dessa forma, os direitos humanos são direitos fundamentais tutelados e assegurados em âmbito internacional, formalizados em Convenções, Declarações e Tratados internacionais. Doutro lado, os direitos fundamentais referidos como tal pela doutrina são tutelados no âmbito dos Estados nacionais, em geral formalizados nas Constituições (VALADARES, 2023). A distinção entre direitos fundamentais e direitos humanos ocorre no plano doutrinário conforme destacado, apesar de em essência não haver distinção substancial quanto ao conteúdo desses direitos, apesar de que se prefere a expressão "direito fundamental", coadunando com o entendimento expresso pelo professor José Adércio Leite Sampaio (SAMPAIO, 2010, p. 26).

Os direitos fundamentais se diferenciam dos demais, inicialmente pelo seu conteúdo ético e por serem compostos de valores intimamente ligados à dignidade da pessoa humana. Conforme assevera George Marmelstein (2019, p. 17), a dignidade humana é a base axiológica para esses direitos. Dessa forma, a dignidade da pessoa humana passa a ser medida tanto da fundamentalidade, quanto da sua negação para a classificação de um direito. Como decorrência da amplitude semântica do que seria dignidade da pessoa humana, assim como em face da mutabilidade contextual que impacta no que se entende por vida digna com o passar do tempo, a verificação do respeito a essa dignidade demanda esforço de análise concreta. Dessa maneira, em âmbito teórico é mais fácil apontar o que viola essa dignidade, ou seja, se estabelecer uma acepção com base em critério negativo, do que definir um conceito taxativo de dignidade.

---

não está, no entanto, menos vinculada ao ordenamento positivo do que estão os direitos e as obrigações. Nem sempre o direito positivo atribuiu aos homens enquanto tais, uma qualificação deste gênero; e quando lha dê, pode ser ela tanto geral como circunscrita. [...]" (CUPIS, 2008, p. 19).

Nesse esforço de identificar contorno conceitual para dignidade humana, muitos autores identificam que existe violação sempre que um ser humano é tratado como objeto, e não como um fim em si mesmo. A partir da definição traçada por Ingo Sarlet[8], George Marmelstein (2019, p. 17) identifica alguns atributos para a dignidade da pessoa humana: "(a) respeito à autonomia da vontade, (b) respeito à integridade física e moral, (c) não coisificação do ser humano e (d) garantia do mínimo existencial." O autor complementa que os atributos elencados representam uma síntese da noção de respeito ao outro, sem distinção. No mesmo sentido, Luiz Edson Fachin e Carlos Eduardo Pianovski Ruzyk (2008, p. 108-109) destacam que a dignidade humana é "aferível no atendimento das necessidades que propiciam ao sujeito se desenvolver com efetiva liberdade".

A importância de se atribuir a classificação de fundamental a um direito reside em aspectos atinentes à sua tutela e ao controle subjetivo da sua concretização. Marmelstein (2019, p. 16) reforça que as características dos direitos fundamentais facilitam a sua proteção e a efetivação judicial. O autor frisa, ao tratar especificamente do contexto brasileiro, que

> no Brasil, os direitos fundamentais:
> a) possuem aplicação imediata, por força do art. 5º, §1º, da Constituição de 88, e, portanto, não precisam de regulamentação para serem efetivados, pois são diretamente vinculantes e plenamente exigíveis;
> b) são cláusulas pétreas, por força do art. 60, §4º, inc. IV, da Constituição de 88, e, por isso, não podem ser abolidos nem mesmo por meio de emenda constitucional;
> c) possuem hierarquia constitucional, de modo que, se determinada lei dificultar ou impedir, de modo desproporcional, a efetivação de um direito fundamental, essa lei poderá ter sua aplicação afastada por inconstitucionalidade (MARMELSTEIN, 2019, p. 16-17).

Como ressaltam Danilo Doneda e Rafael Zanatta (2022, p. 38), em capítulo do livro *Personality and Data Protection Rights on the Internet: Brazilian and German Approaches*, os direitos da personalidade foram influenciados pelo processo de codificação do direito civil, marcada pelo trabalho de Teixeira de Freitas, culminando no *Código Civil de 1916*, assim como pela dogmática jurídica no direito civil, cujo início foi fortemente influenciado pela teoria jurídica alemã, e mais tarde pelo direito civil italiano e francês. Tendo essa influência em mente, necessário frisar que no sistema jurídico brasileiro, a concepção de direitos da personalidade é bem próxima da proposta por Otto von Gierke, que argumentava sobre a insustentabilidade da divisão absoluta entre Direito Privado e Direito Público, tipicamente fomentada no Direito

[8] George Marmelstein cita o seguinte conceito elaborado por Ingo Sarlet: "onde não houver respeito pela vida e pela integridade física e moral do ser humano, onde as condições mínimas para uma existência digna não forem asseguradas, onde não houver uma limitação do poder, enfim, onde a liberdade e a autonomia, a igualdade em direitos e dignidade e os direitos fundamentais não forem reconhecidos e assegurados, não haverá espaço para a dignidade da pessoa humana." (MARMELSTEIN, 2019, p. 16-17).

Romano. Para von Gierke[9] (2016, p. 5-6) essa divisão é uma abstração jurídica que expressa visão dual da existência humana: do ser como um indivíduo e como parte de um grupo. Entretanto não se pode prescindir dessa dualidade[10], sempre buscando encontrar em cada ramo do direito a unidade que proteja o indivíduo e a sociedade, a um só tempo. Dessa forma, o direito privado tem que atender a um papel social, sendo dedicado a proteger todas as vontades, e não a vontade de um indivíduo isolado, servindo ao bem comum. Da mesma forma, o direito público deve ser vocacionado a responder as demandas da coletividade, sem perder, no entanto, a sensibilidade de ser justo para os indivíduos. Logo, os direitos da personalidade constituem tutelas estabelecidas para a pessoa natural e oponíveis contra particulares e contra o Estado.

Para Gierke, os direitos da personalidade estavam ligados aos direitos necessários para assegurar que um indivíduo mantivesse a sua essência, o que lhe faz ser único, a sua diversidade,

---

[9] *The social role of private law (Die soziale Aufgabe des Privatrechts - Berlin 1889).* Traduzido para o inglês por *Ewan McGaughey (2016). "*Insofar as the law, as an external world order, encounters this two dimensional content of human life, and accordingly constitutes itself in two distinct empires, on one side it must constrain and protect the external sphere of individuals' lives, and on the other side its goal must be to build and secure the life of the community as a whole. Yet it becomes immediately clear that this division cannot be the last word. It remains the same person who acts out both an individual existence and as a player in community life. Both are intertwined in reality as an indissoluble unity and are distinct only in our imaginations. What we call the individual and the whole are merely indispensable conceptual abstractions of, what is for us in its totality, the incomprehensible reality of historical humanity. The legal order, if it splinters into private and public law, can certainly ignore the importance of the individual for the whole and the whole for the individual (all for one and one for all), for a while. But in the end, the law cannot forget the Unity of the goal. Private law, though it cares foremost for individual interests, must serve the common good. Public law, though it looks first to the whole, must be just toward individuals."

[10] "The sharp, basic opposition is inviolable for us. We cannot eliminate it entirely without sacrificing the very achievements we seek to protect. If public law ceases to be a unity of an existentially higher order, with an independent purpose, in place of the noble idea to serve na everlasting common existence, it is reduced to be the means of everybody to follow individual purposes, or simply the majority's purpose. With this, the hard-won sovereignty of the state would fall! In private law, if we cease to recognise the individual as an autonomous end in itself, if we paralyse its arrangements as a means for corporate purposes, the Christian revelation of each person's unique and immortal worth would be lost in vain. World history would have developed the ideas of freedom and justice for nothing! Again and again, ideals and aspirations stir with elementary force, that indulge a desolate monism in one way or another. Educated and uneducated minds are still haunted today by the extreme natural law position on contractual theories, which, because they acknowledge only an individual reality, always begin with the individual and get to public law last. Always directed toward the individual, it is therefore nothing more than a befuddled private law. On the other side, the socialist school of thought is threatening, as it sees and values people exclusively as members of society, and would translate all of private law into a branch of state administration. [...]But if we are unable to abandon this antithesis entirely, we must still find and realise unity despite the opposition, and do so with all our power. We cannot abandon the great Germanic ideal of the unity of all law without giving up our future. This ideal will always be incompatible with an absolute public law, and it is equally incompatible with an individualistic private law. We need a public law, which through and through follows the rule of law; which recognises reciprocity between the whole and its members, between the highest generality and the smallest associations, between the community and the individual; which binds and penetrates the state from peak to valley, even when coercion fails, and the protection of the courts is enjoyed; which certainly envisages duties toward the Whole but at the same time gives members rights in the whole, guaranteed and secured in the smallest part of the state; which acknowledges the necessity and permanence of social life and yet embraces freedom. But also we need a private law, where despite the revered and inviolable sphere of the individual, the thought of community lives and weaves. Stated simply: our public law should be blown a scent of natural law freedom and our private law must absorb a drop of socialist ointment. But are we not demanding the reincarnation of old errors, such that" (GIERKE, p. 10-12).

em harmonia com a sua posição de membro de uma coletividade. Von Gierke defendia, assim, a proteção de direitos essenciais à personalidade como o direito à vida, ao corpo, à liberdade, e à honra, mais outros direitos intangíveis que à época (1889) somente eram tutelados na Alemanha de maneira reflexa, como o direito ao nome, à imagem e outros símbolos da personalidade (GIERKE, 2016, p. 35). Em que pese o direito privado tenha sido pensado inicialmente como ramo para disciplinar a relação de indivíduos com coisas, o direito de propriedade somente tem sentido quando encarado em face da unicidade do homem, se pensado a partir do seu cunho social.

> But there is no more dangerous error than the widespread view that the role of private law is limited to property. All property exists merely for the sake of the person, and surrounding every proprietary relationship is the right of developing one's personality. Private law must use the means at its disposal first and foremost to guarantee and protect the personalities of individual people, to both acknowledge and limit the rights of personality (rights of the individual) in their general and equal manifestation, in their condition as being members of a community, with their unique eccentricities, and in their individually acquired or otherwise attained development, to use civil obligations next to criminal sanctions to vindicate rights where they are harmed, and to secure compensation and redress. (GIERKE, 2016, p. 34).

Orlando Gomes, autor do anteprojeto do *Código Civil de 1916*, em clássico artigo denominado "Direitos da Personalidade" (1966, p. 40-41), ressaltou que embora o desenvolvimento doutrinário dos direitos da personalidade já decorresse desde o século anterior, não havia uma unidade no que diz respeito à sua conceituação, natureza e os exemplos de sua expressão:

> Tomou-se famosa a definição de GIERKE segundo a qual são os direitos que asseguram ao sujeito o domínio sôbre uma parte da própria esfera da personalidade. Procedente, no entanto, a crítica de DERNBURG, porque a honra não dá êsse domínio sôbre a própria pessoa, nota distintiva da categoria. Seriam, como os conceitua FERRARA, faculdades específicas sôbre diferentes partes de nossa esfera pessoal (Tratatto di Diritto Civile Italiano, página 389, Athenacum, Roma, 1921). DE CASTRO define-os como os direitos que concedem um poder às pessoas para protegerem a essência de sua personalidade e suas qualidades mais importantes (in CASTAN TOBENAS, Derecho civil español, comum y foral, t. I, vol. 2, pág. 735, Madri, 1956). Já DIEZ DIAZ conceitua-os por seu conteúdo especial, que consistiria em regular as diversas projeções, físicas ou psíquicas, da própria pessoa **(**Los derechos físicos de la personalidad**,** pág. 56, Ediciones antillana, Madri, 1963).

Em que pese a dificuldade de se conceituar os direitos da personalidade, Gomes o faz destacando que o seu objeto são os bens jurídicos, ou seja, toda utilidade material ou imaterial que incide na capacidade de agir do sujeito, em que se convertem projeções físicas ou psíquicas da pessoa humana que a individualizam (GOMES, 1966, p. 41). Esses direitos seriam caracterizados por serem "absolutos, extrapatrimoniais, intransmissíveis, imprescritíveis, impenhoráveis, vitalícios e necessários. Por sua própria natureza, opõem-se *erga omnes*, implicando o dever geral de abstenção." (GOMES, 1966, p. 42). Gomes segue esmiuçando cada

uma das características[11] para culminar na constatação de que os direitos da personalidade são "direitos subjetivos privados", cuja proteção visa "assegurar o desenvolvimento e a expansão da individualidade física e espiritual da pessoa humana" (GOMES, 1966, p. 43). A sua classificação, segundo Gomes (1966, p. 44), poderia se dar em duas categorias gerais, entre direitos à integridade física e direitos à integridade moral.

Conforme mencionado, o desenvolvimento da teoria dos direitos da personalidade no Brasil tem também forte influência da doutrina legal italiana, com especial relevância para os trabalhos do jurista Adriano de Cupis. De Cupis (2008, p. 23-24) define os direitos da personalidade a partir da sua essencialidade, do que é imprescindível para a manutenção do conteúdo, ou seja, da própria personalidade.

> Por outras palavras, existem certos direitos sem os quais a personalidade restaria uma susceptibilidade completamente irrealizada, privada de todo o valor concreto; direitos sem os quais todos os outros direitos subjetivos perderiam todo o interesse para o indivíduo – o que equivale a dizer que, se eles não existissem a pessoa não existiria como tal. São esses os chamados "direitos essenciais" com os quais se identificam precisamente os direitos da personalidade. Que a denominação de direitos da personalidade seja reservada aos direitos essenciais justifica-se plenamente pela razão de que eles constituem a medula da personalidade (CUPIS, 2008, p. 24).

Ante o exposto, convém ressaltar que os direitos da personalidade e os direitos humanos são direitos fundamentais. Os direitos humanos são reconhecidos e pleiteáveis em âmbito internacional, enquanto os direitos da personalidade contam com proteção nos sistemas jurídicos nacionais, constituindo núcleo fundamental de direitos à integridade moral e física do sujeito que repercutem na sua autoconstrução e autoexpressão no mundo (VALADARES, 2023). Dessa forma, o corpo digital criado a partir dos dados pessoais em circulação é componente da integridade moral do indivíduo, sendo sua proteção necessária para o resguardo dos direitos da personalidade, por refletir uma tutela da própria dignidade.

---

[11] "Os bens jurídicos sôbre os quais incidem não são suscetíveis de avaliação pecuniária, embora possam alguns constituir objeto de negócio jurídico patrimonial e a ofensa ilícita a qualquer dêles se tenha como pressuposto de fato do nascimento da obrigação de indenizar, ainda quando se trate de puro dano moral.Dizem-se inalienáveis no sentido de que o titular não pode transmiti-los a outrem, privando-se de seu gôzo, por isso que nascem e se extinguem *ope legis* com a pessoa (MESSINEO, Manuale di Diritto Civile e Commerciale, vol. 1, pág. 386, 7.ª edição, Dolt. A. Giuffré, Milão, 1947). Não se transmitem sequer mortis causa, embora gozem ·de proteção depois da morte do titular. [...] Do seu teor extrapatrimonial decorre a impossibilidade de cumprimento e execução coativos. São impenhoráveis e imprescindíveis, não se extinguindo, quer pelo não-uso, quer pela inércia na sua defesa. A vitaliciedade e a necessariedade são caracteres que acentuam mais vivamente seus traços distintivos. São necessários no sentido de que não podem faltar, o que não ocorre com qualquer dos outros direitos (BARBERO, Sistema istituzionale dei diritto privato italiano, vol. 1, pág. 532, 4.ª edição U.T.E.T., Turim, 1955). Em conseqüência, jamais se perdem êsses direitos, enquanto viver o titular, sobrevivendo-lhe a proteção legal em algumas espécies." (GOMES, 1966, p. 42-43).

No âmbito da Teoria dos Direitos Fundamentais existe uma tensão no que diz respeito à criação excessiva de novos direitos fundamentais e à visão geracional. Alguns doutrinadores[12] compreendem que o alargamento dos direitos da personalidade é um dos fatores que leva a uma banalização da invocação desses direitos, bem como impacta numa fragmentação da sua abordagem, que permite que Estados que não cumprem com o compromisso com a dignidade da pessoa humana aleguem que são defensores de direitos fundamentais, por assegurarem parcialmente esses direitos, mesmo sendo violadores contumazes de outros, igualmente fundamentais. A visão geracional, que admite essa derivação de direitos fundamentais, militaria em desfavor da sua unicidade, fragilizando a sua tutela.

Em que pese a concordância com o reconhecimento de que os direitos fundamentais formam um bloco único, que possui superioridade sobre os demais, assim como sem olvidar a importância de se reconhecer que todos os direitos fundamentais possuem como fonte primeira o direito à propriedade[13], entende-se que o papel da positivação constitucional e do reconhecimento em âmbito internacional de novos direitos é um meio de se assegurar a unicidade, para além do simbólico, conclamando os sujeitos interessados a exercerem o controle, buscando a sua concretização sempre que necessário.

Conforme disposto por Cançado Trindade (2006, p. 413), o reconhecimento de direitos humanos e a disciplina do Direito Internacional dos Direitos Humanos são permeados por princípios básicos no seu amadurecimento, de forma que a especialização não acarreta a fragmentação da tutela:

> [...] São eles os princípios da *universalidade*, da *integralidade* e da *indivisibilidade* dos direitos protegidos, inerentes à pessoa humana e por conseguinte anteriores e superiores ao Estado e demais formas de organização político-social, assim como o princípio da *complementaridade* dos sistemas e mecanismos de proteção (de base

[12] Gomes argumenta que o excessivo alargamento de direitos resulta em confusão na sua abordagem, entretanto o autor não condena a derivação, a especialização de direitos, ao passo que entende a sua historicidade. Entretanto, atesta que a derivação nem sempre resultará na autonomia do direito: "Tal delimitação é necessária para prevenir a tendência ao alargamento exagerado do cam4po dos direitos de personalidade, acentuada no sentido de elevar a direitos subjetivos várias projeções da individualidade que não possuem êsse teor, e, ainda, de arrastar para seu território direitos de outra natureza, corno, por exemplo, o direito aos alimentos e o direito à liberdade do pensamento. Desta necessidade de defini-los com precisão, não **se** deve inferir que constituem *numerus clausus***,** se considerados histàricamente, mas de sua natureza de direitos absolutos, e, portanto, oponíveis erga omnes**,** segue-se que devem estar instituídos em lei, muito embora constituamcategoria elástica em face da ampla compreensão de muitos dêles." (GOMES, 1966, p. 45). E finaliza o texto destacando a importância de a proteção acompanhar o "progresso da ciência" que pode resultar em ameaças à integridade moral: "Os progressos da ciência o ameaçam no que tem de mais intimo e inviolável. À condenação a êsses abusos e práticas não basta, evidentemente, a repressão legal, mas, inquestionàvelmente, a consagração dos direitos de personalidade nos Códigos traduz convicções e sentimentos que nêles encontram considerável refôrço. Tais ameaças não existem apenas em relação à integridade física dos indivíduos. Alcançam-lhes a integridade moral lato sensu, do que resulta a necessidade do reconhecimento de dois novos e interessantes direitos: 1) o direito à imagem; 2) o direito ao recato." (GOMES, 1966, p. 48).

[13] Como abordado em Sampaio (1998) e reforçado ao longo do curso da disciplina "Tópicos Especiais em Teoria dos Direitos Fundamentais". Ministrada pelo Prof. Dr. José Alfredo Baracho Júnior no primeiro semestre de 2022.

> convencional e extraconvencional, de âmbito global e regional). O presente *corpus juris* de proteção forma, desse modo, um todo harmônico e indivisível. Neste universo conceitual, e por força do disposto nos tratados de direitos humanos, os ordenamentos jurídicos internacional e interno mostram-se consagrados, prevalecendo a norma – de origem internacional ou interna – que em cada caso melhor proteja o ser humano. (TRINDADE, 2006, p. 413).

O reconhecimento de que todos os direitos fundamentais descendem em alguma medida da propriedade privada, decorre da constatação de que a sua construção remonta a própria concepção da ideia de individualidade, de sujeito de direito e de autonomia da vontade. Essas construções são fruto da modernidade, impulsionadas pela ascensão da burguesia, e pela consequente demanda por maior liberdade dos indivíduos burgueses (FRANK, 2019).

O professor José Adércio Leite Sampaio (1998), já no final da década de 1990, faz uma análise da transformação dos direitos de propriedade e liberdade para o reconhecimento da intimidade e da vida privada como direitos fundamentais, com um prenúncio da proteção de dados como vertente[14], como parte integrante desses direitos. Sampaio (1998) analisa, assim como Rodotà (2008), a progressiva modificação na concepção de privacidade, inicialmente de cunho patrimonialista, para depois haver o reconhecimento de uma dimensão extrapatrimonial. Para Sampaio (1998), vida privada consiste na autodeterminação da existência e na possibilidade de autodefinição pessoal, sexual e familiar, e a intimidade é um dos seus aspectos, referente às informações pessoais e ao controle dos seus *inputs* e *outputs.* A concepção de intimidade dada por Sampaio se aproxima bastante do que se entende hoje por autodeterminação informativa.

Na obra "Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais da vida e da morte", Sampaio (1998) demonstra que os direitos fundamentais são construídos com sucessivos avanços e retrocessos[15], sendo reflexos da realidade contextual em que são tutelados, sem que essa decorrência da sua historicidade represente fraqueza substancial, mas somente reflita a natureza dinâmica da vida. E aponta que a sua gênese remete à proteção da propriedade privada e ao tratamento dos direitos derivados dela como domínio sobre bens, sobre coisas, ou seja, com

[14] O autor não aborda especificamente a proteção de dados como direito autônomo, mas a sua concepção de privacidade contempla o que é doutrinariamente considerado direito à proteção de dados contemporaneamente.

[15] Em sentido similar, Antônio Augusto Cançado Trindade (2006, p. 409-410) dispõe que "Os avanços e retrocessos lamentavelmente são próprios da triste condição humana, o que deve nos incitar a continuar lutando até o final. O importante é a luta incessante pela prevalência do Direito. [...]
Não podemos supor, neste ou naquele domínio, um progresso linear, constante e "inevitável", porquanto as instituições públicas (nacionais e internacionais) são, em última instância, as pessoas que nelas se encontram, e oscilam, pois, como as nuvens ou as ondas, como é próprio da vulnerável condição humana. [...]"

uma visão patrimonialista. Quanto ao conteúdo da intimidade e da vida privada o autor traz reflexões que se aplicam aos direitos fundamentais de forma geral:

> Embora determinável em um certo tempo e lugar, esse conteúdo estará sempre aberto a novas interpretações, acréscimos e reduções, acompanhando as intempéries, contingências, mutações, enfim, a própria evolução da história humana, sem que isso importe "fraqueza substancial". Quer-se dizer que seu sentido é dinâmico, como dinâmica é a vida e mutável, como mutável é a compreensão humana de si mesmo e de seu devir. (SAMPAIO, 1998, p. 274).

Derivam diretamente do direito de propriedade (SAMPAIO, 1998) os direitos à inviolabilidade de domicílio, a partir da máxima da *Common Law*, *"Man's house is his castle"*, o direito autoral, partindo-se da concepção de valor histórico e de propriedade material do conteúdo, para uma noção de propriedade imaterial, pautada na quebra de confiança ou rompimento de um contrato, e o direito à imagem, também lastreado na propriedade imprescritível de toda pessoa sobre sua imagem, seu rosto e seu retrato. Todas essas derivações e o amadurecimento de interpretação jurisprudencial acerca das tutelas estabelecidas são cruciais para o desenvolvimento e para a sedimentação da ideia de proteção de dados como direito autônomo, assim como de autodeterminação informativa como vertente de empoderamento do titular e meio para que ele exerça o controle subjetivo quanto ao tratamento[16] dos seus dados pessoais.

A partir de uma digressão histórica e da abordagem de julgados de Cortes Constitucionais, como a Suprema Corte e o Tribunal Constitucional Alemão, entre outras, Sampaio (1998) demonstra o quanto o amadurecimento dos direitos fundamentais contemplados à intimidade e à vida privada se deu a partir da propriedade privada e da valoração patrimonial desses direitos, para posteriormente se alargar a visão para caracteres morais e espirituais, considerando a repercussão na formação da subjetividade.

O mesmo fenômeno ocorreu com o direito à proteção de dados pessoais, cuja justificativa de tutela específica inicialmente partiu da constatação de que existe uma monetização no tratamento dos dados pessoais, isto é, no reconhecimento de que essas informações pessoais são uma *commodity* na sociedade informacional. Para posteriormente haver um entendimento de que a proteção enquanto parte integrante do patrimônio dos titulares de dados pessoais é frágil e vulnerabiliza a fundamentalidade, ao permitir que existam violações

[16] Entende-se tratamento de dados pessoais no sentido previsto no art. 5º, X, da *Lei Federal nº. 13.709/2018 (Lei Geral de Proteção de Dados* - LGPD*)*, de "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". Ressaltamos que o rol de atividades de tratamento é exemplificativo, de maneira que tudo que é feito com um dado pessoal pode ser enquadrado como tratamento para fins da Lei em questão.

permissíveis, mediante pagamento ao titular (RODOTÀ, 2008, p. 153). A partir do reconhecimento de que a proteção de dados não pode ser convertida em um patrimônio disponível, existe a ampliação da defesa de um núcleo duro dessa proteção com uma construção da ideia de limitação do consentimento sobre seu uso. Vale dizer, o consentimento não pode valer para justificar todo tipo de tratamento de dados pessoais. Stefano Rodotà (2008, p. 15) destaca que o direito à privacidade concebido e reforçado a partir da década de 1950, década em que começam a ser desenvolvidas tecnologias computacionais, apresentava uma concepção estática, como um direito de ser deixado só, de não ser incomodado. Essa tutela estática passa a ser insuficiente ante o cenário de interligação transnacional e de transformações tecnológicas, fazendo surgir a necessidade de se construir um direito atinente ao fluxo de informações, ao dado em movimento, uma proteção dinâmica (RODOTÀ, 2008, p. 15-17).

A concepção de privacidade para além do direito de ser deixado só, em sentido literal e físico, é impulsionada com o artigo de dois advogados norte-americanos, Warren e Brandeis, publicado em 1890 na *Harvard Law Review: The Right to Privacy.* O artigo é considerado marco doutrinário para a noção de privacidade com bases pautadas na inviolabilidade da personalidade. Sampaio (1998, p. 59-60) comenta o artigo e menciona fatores marcantes dessa virada da privacidade, para a vinculação com "bases espirituais". Os seguintes traços distintivos começam a ser notados: o objeto de proteção passa a contemplar pensamentos, emoções e sentimentos do indivíduo, independentemente do meio e da forma de expressão; distingue-se do direito à reputação, por proteger o sentimento íntimo das pessoas mesmo contra a imputação de fatos verdadeiros, e independente do intuito malicioso ou não do emissor; difere-se do direito de propriedade intelectual ou artística por oferecer proteção que independe do valor pecuniário, artístico ou histórico da informação violada; existe o reconhecimento de que o direito à privacidade pode ser violado de múltiplas formas, por se tratar de uma imunidade geral da pessoa, do direito à sua personalidade.

O direito à privacidade não seria absoluto para Warren e Brandeis (1890), assim como os demais direitos fundamentais, admitindo-se sua mitigação em determinados contextos: não impediria a publicação de matéria que fosse de interesse geral ou público (levando em consideração a pessoa sobre a qual versa a informação, a sua postura em sentido de demonstrar a vontade de manter o assunto na esfera privada); não vedaria a publicação de fatos de cunho privado se realizada dentro de circunstâncias autorizadas pela lei (por exemplo, o tratamento da informação em Cortes de justiça, para a solução de um litígio); não teria o condão de impossibilitar a divulgação oral sem danos ao titular; e também não alcançaria a publicação de fatos da vida privada promovida pelo próprio titular. Por fim, o violador ainda poderia se valer

da exceção da verdade e da comprovação de ausência de malícia, fatores a serem levados em consideração na análise dos casos concretos.

Em que pese a grande repercussão gerada pelo artigo de Warren e Brandeis, ele não chegou a influenciar de imediato o posicionamento jurisprudencial nos Estados Unidos, que seguiu vinculado a uma visão patrimonialista e pautada em parâmetros materiais, físicos da privacidade[17]. Somente na década de 1970, com o avanço da ciência da computação e com o desenvolvimento de novas tecnologias (e com a chegada às Cortes de diversos casos em que a violação à privacidade era alegada a partir do uso dessas tecnologias e da sua recorrência) é que as leis voltadas a proteção de dados começam a surgir, inicialmente considerando essa proteção como vertente da privacidade (SAMPAIO, 1998).

Na década de 1980 as *Diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para a Proteção da Privacidade e para o Fluxo Transfronteiriço de Dados Pessoais (1980)* e a *Convenção 108 do Conselho da Europa (1981) (Convention for the Protection of Individuals with regard to Automatic Processing of Personal*, revisada e modernizada em 2018, cuja versão atualizada é referida como *Convenção 108+*) foram determinantes para o espraiamento de normas atinentes à proteção de dados. Essas normas conferiram amplitude à noção de privacidade e reconhecimento da necessidade de uma convergência regulatória, à medida que o resguardo à vida privada, com o avanço da tecnologia da informação, demandava, a partir de então, uma proteção também transfronteiriça.

Cumpre salientar que a especialização é um fenômeno próprio da modernidade e a estratificação dos direitos e sua derivação a partir desse núcleo formado pela tríade "propriedade – liberdade – igualdade" é característica da cientificidade moderna. Essa tendência é justificada tanto pela impossibilidade de se cogitar um panorama perfeito e acabado dos direitos fundamentais (que se renovam conforme a concepção vigente e, se adequando à dinamicidade da vida), quanto por esses direitos serem influenciados pelo contexto histórico, pelo que em cada época é considerado dignidade humana. É, ainda, efeito da globalização que impacta na necessidade de convergência na abordagem de certos direitos cuja tutela envolve a atuação de uma pluralidade de Estados nacionais, como o caso da proteção de dados.

Nesse contexto, o direito à proteção de dados pessoais representa um amadurecimento das concepções de vida privada e de intimidade e, juntamente com o direito à autodeterminação

[17] Ao mencionar que a aferição de violações ao direito à privacidade adotava parâmetros materiais, físicos, busca-se esclarecer que a constatação de violações estava ligada ao transpasse de barreiras físicas. A utilização de tecnologias para ultrapassar essas barreiras e captar sons, por exemplo a escuta telefônica, ou a escuta ambiente realizada por fora de uma construção, não eram consideradas violações à privacidade.

informativa, passa a integrar o núcleo dos direitos da personalidade. No sistema jurídico brasileiro, proteção de dados pessoais consiste na tutela dos tratamentos de informações de pessoas naturais (titulares) com o potencial de identificá-las ou torná-las identificáveis, sejam esses tratamentos realizados por pessoas físicas ou jurídicas, de direito público ou de direito privado (BRASIL, 2018). Trata-se de proteção pertinente aos dados em movimento, ao que é feito com esses dados, estejam eles inseridos em meios físicos ou digitais. Impõe a exigência de que todo tratamento de dados pessoais, que não esteja inserido nas exceções de aplicabilidade do art. 4º da LGPD, respeite os princípios do art. 6º[18] da referida lei, atenda aos fundamentos do art. 2º e se encaixe em uma das hipóteses de tratamento que gozam de presunção de legitimidade (Bases Legais dos artigos 7º e 11, para dados pessoais sensíveis[19], da LGPD). Trata-se, assim, de proteção que pressupõe a autodeterminação informativa, ou seja, a tutela do controle por parte do titular dos seus *outputs*, da formação do seu corpo digital e do que é feito com ele.

Ante o exposto, necessário frisar que a proteção de dados vai além da proteção contra decisões automatizadas. Dessa maneira, a regulação do desenvolvimento e operação de sistemas de IA não contempla a inteireza do que a proteção de dados significa. Da mesma forma, a regulação das plataformas no que tange ao seu funcionamento também é insuficiente para abarcar a proteção de dados. Extrapola, também, a mera adoção de standards de segurança da informação. Visa em última instância proteger a autonomia dos titulares, no que diz respeito à sua consciência, à sua visão de mundo e à expressão da sua vontade, sendo de extrema relevância para a livre formação da sua personalidade.

Em âmbito internacional as violações à proteção de dados têm sido encaradas como aviltes à privacidade, falando-se com maior recorrência (e de maneira imprecisa tecnicamente) em privacidade de dados como um direito humano[20] (VALADARES, 2023). No sistema

[18] Princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação, da responsabilização e prestação de contas. Todos esses princípios militam em prol da autodeterminação informativa, em sentido de fornecer informações ao titular para que este se posicione sobre os tratamentos e somente entre em relações que envolvam esse processamento estando ciente da extensão, das finalidades e de como será o uso do dado. Ademais, os princípios refletem um convite à mudança de mentalidade dos agentes de tratamento: de coleta e armazenamento irrestrito de dados pessoais, para uma cultura de minimização, de utilização somente de dados absolutamente pertinentes às finalidades, e de apagamento, tão logo o tratamento do dado se encerre e não haja justificativa para mantê-lo em cadeia de tratamento.

[19] Para a LGPD são dados pessoais sensíveis aqueles referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Ou seja, são informações com potencial de expor o titular a tratamentos discriminatórios, violando a sua personalidade.

[20] Para maiores informações sobre os desafios trazidos pela crescente interação com novas tecnologias para a tutela dos Direitos Humanos, recomenda-se a leitura do artigo de Flávia Piovesan e Letícia Quixadá, de 2018. Conforme

jurídico australiano, como restará demonstrado no capítulo 5, a noção de proteção de dados não está sedimentada e tampouco encontra lastro na jurisprudência, existindo somente a concepção de interferência na privacidade, sendo inexistente um direito à privacidade como causa para ação no plano normativo do *Privacy Act 1988* (Cth).

Vale reforçar que muitas vezes a coleta de dados se dá com o consentimento do titular, mas sem o devido esclarecimento sobre a extensão do seu uso, com base em ofertas de personalização dos serviços ou de descontos no preço de serviços ou produtos. Com fulcro nas informações construídas a partir dessa coleta massiva de dados pessoais e do seu cruzamento direcionado, os titulares passam a ser alvo, na interação com as plataformas, de *feedbacks* orientados a modular o seu comportamento, a influenciar suas ações e a formação da sua vontade sem que possam perceber essa manipulação. E ficam vulneráveis a decisões e ações que afetam a sua vida e podem determinar o seu futuro, pautadas no seu corpo digital sem que tenham conhecimento disso. Existe inegavelmente uma assimetria no exercício do que Zuboff (2019) denomina de poder instrumentário[21].

O endosso à fundamentalidade pelo reconhecimento da proteção de dados como direito autônomo, ao contrário do que pode parecer, não fragmenta a proteção da dignidade, mas ratifica vertentes da privacidade e da livre formação da personalidade que têm sido vulnerabilizadas pelo avanço tecnológico e informacional. Representa a consagração de valores superiores, atribuindo a eles mecanismos de proteção mediante o exercício do direito de ação e os configurando como questão de ordem pública, à medida que houve a sua consagração no sistema jurídico brasileiro como direito fundamental. Por óbvio a simples existência de lei assegurando o direito não operará uma transformação na cultura e na forma com que as pessoais e organizações lidam com dados pessoais. Por isso a necessidade da estruturação da política pública para adoção de medidas que promovam essa proteção e as mudanças culturais necessárias. Toda mudança cultural demanda tempo, assim como a efetividade de políticas públicas. E toda "inovação" legislativa que suporte uma política pública tem que ser observada

destacam as autoras, as novas tecnologias representam uma dualidade de potencialidades, sendo instrumento capaz de promover os Direitos Humanos, mas também de oportunizar a sua violação.

[21] "[...] Instrumentarian power knows and shapes human behaviour for the purposes of others. Instead of armaments and armies, it enforces its will through the automated medium of an increasingly ubiquitous computational architecture composed of networked "smart" devices, things and spaces." (ZUBOFF, 2019, p. 15). Em outra parte a autora afirma: "Surveillance capitalists work hard to camouflage their purpose as they master the uses of instrumentarian power to shape our behavior while evading our awareness. That is why Google conceals the operations that turn us into the objects of its search and Facebook distracts us from the fact that our beloved connections are essential to the profit and power that flow from its network ubiquity and totalistic knowledge." (ZUBOFF, 2019, p. 415).

como processo, passível de melhoramento contínuo, desde que conduzido com o devido planejamento, medição de resultados e mecanismos de *enforcement*.

A proteção de dados pessoais é direito que merece tutela diferenciada, especialmente em âmbito internacional, por repercutir na autoconstrução e na autorrepresentação do sujeito. Os dados pessoais constituem, em uma sociedade informacional o corpo digital, comunicando mais do que o titular supõe a respeito dos seus hábitos e de quem ele é para as plataformas digitais. Esse corpo digital pode vir a se tornar (se já não é dada à datificação e à plataformização da vida) uma fronteira intransponível que prejudica a existência do indivíduo, tal qual já ocorreu com o corpo físico, no que diz respeito ao preconceito e às biopolíticas[22] que subsistem até hoje, em prejuízo de determinados fenótipos e origens[23]. O perigo de o poder dessa tecnologia ser concentrado nas mãos de entidades privadas, que passam a exercer poder de maneira tradicionalmente exercida por Estados (MBEMBE, 2019; KLEIN, 2015; BOOTE, 2015), torna o indivíduo objetificado, quantificado e reduzido ao perfil traçado, ainda mais vulnerável. Isso porque essas entidades privadas são orientadas pelo intuito de fidelização para que sigam sendo a porta de entrada de dados, assegurando mercados futuros e a dominância que ocupam. A despossessão dos dados fornece subsídio para a modulação comportamental, da influência na formação da vontade, de maneira a direcionar as ações dos indivíduos, garantindo a predição dos seus comportamentos e a criação de mercados futuros (ZUBOFF, 2019). Torna os indivíduos vulneráveis, ainda, à contenção da sua liberdade ambulatorial e do potencial de autoconstrução da vida e dos caminhos, ao torná-los alvo de decisões que impactam sua vida e podem resultar na sua limitação e no fatalismo de um destino taxativo, desprovido de diversidade e de possibilidades.

A partir da breve abordagem desse caminho não linear dos direitos fundamentais e humanos demonstrou-se que o processo de especialização e de derivação em novos direitos reforça a fundamentalidade de nuances demandadas pela modificação contextual na sociedade

---

[22] Na sociedade informacional as biopolíticas são coordenadas e conduzidas pelo capital financeiro, que progressivamente com o processo de globalização passa a ter poder páreo ao dos Estados Nação, mas ainda necessitam utilizar o aparato institucional do Estado para dotar seus atos de legitimidade, diversos exemplos como o caso de Myamar e de New Orleans após desastres naturais, assim como o caso do Afeganistão, invadido após o ataque às Torres Gêmeas, conhecido como 11 de setembro de 2001, e do Iraque, invadido em 2003, ainda sob a justificativa de Guerra ao Terror, são citados por Naomi Klein (2015) para exemplificar o que ela chama de desastre do capitalismo, a tomada de regiões com potencial de exploração para turismo e recursos naturais com a expulsão dos nativos, numa manobra bastante parecida com o que o colonialismo fez na ocupação do mundo além Europa.

[23] Vide palestra interessante de Achile Mbembe, proferida em 2019, que trata dos corpos como novas barreiras e fronteiras do indivíduo ante o crescente emprego de novas tecnologias, em especial tecnologias de reconhecimento facial, que podem ser utilizadas como instrumentos de contenção de pessoas indesejadas, de proibição do seu trânsito e da sua expressão, marginalizando e invisibilizando, ou seja, impedindo a sua agência, a sua diversidade. Disponível em: https://www.youtube.com/watch?v=JqreV_1FqtU . Acesso em 10 Jan. 2021.

informacional. Partindo da sua gênese na defesa da propriedade privada, numa visão patrimonialista, para após derivações resultar em direitos específicos e autônomos atinentes a valores extracorpóreos, que possuem implicações na autonomia do indivíduo e na sua integridade moral e psicológica. Referida derivação e especialização aparentam uma fragmentação desnecessária da tutela da dignidade da pessoa humana, que a fragilizaria. Ao contrário do que pode aparentar, o processo de reconhecimento de "novos" direitos fundamentais é congruente com a dinamicidade da vida e com os novos desafios do Direito em face das ameaças iminentes oriundas da crescente interação com novas tecnologias.

Como uma espécie de reação à crescente incidência da despossessão, que de tão naturalizada, passa despercebida, o Direito passa a desenvolver novas tutelas como atinentes à dignidade da pessoa humana, reconhecendo a influência que essa interação e sinergia humana com as plataformas digitais ocasiona em termos de quebra da autocomposição, da autoconstrução e da autorrepresentação, vertentes da dignidade que dizem respeito ao livre desenvolvimento da personalidade e à autonomia privada. Com a derivação de direitos motivada pelo contexto de violações pertinente à sociedade informacional, direitos como o de proteção de dados pessoais e de autodeterminação informativa passam a ser previstos em normas. Num primeiro momento esses direitos são aventados em organizações internacionais, por meio de recomendações (*soft law*) – diretrizes e diretivas de tratamento de informações, melhores práticas de gestão de bases de dados e orientações para lidar com a transferência internacional desses dados. Posteriormente, passam a ser incorporados nos sistemas jurídicos de Estados nacionais e reforçados por decisões jurisdicionais.

Assim, a incorporação desses direitos em sistemas jurídicos nacionais se opera mais por uma adesão ao que está posto por organizações internacionais, do que por uma genuína atividade legislativa autoral. Dessa forma, à luz da Teoria da Encriptação do Poder – TEP (SANÍN-RESTREPO, 2017), o fenômeno do espraiamento das normas de proteção de dados poderia ser visto como a criação de *potestas*, de estabelecimento de um *modelo transcendente* que filtra e define o que merece tutela ou não, que neutraliza e anula a possibilidade de diversidade e de manifestação do poder como *potentia* (expressão dessa diversidade, exercício de agência). Estaria encriptando as reais motivações de anestesiar os sujeitos e fomentar a continuidade das suas interações com novas tecnologias, a partir do estabelecimento de uma proteção fictícia, meramente simbólica, um simulacro. Poder-se-ia aventar, ainda, que consistiria num elemento encriptador da modificação da própria concepção de capacidade jurídica, que passa pela verificação da real capacidade de discernimento das pessoas naturais para serem legitimamente responsáveis por obrigações que adquiram.

Embora persista o reconhecimento de que as normas de proteção de dados de fato operam, num primeiro momento, a legitimação de tratamentos não realizados em prol do melhor interesse do titular, mas ao contrário, contra o que seria o mais benéfico a esses interesses, a pesquisa de direito comparado permitiu verificar que as normas de privacidade e de proteção de dados não são instrumentos de encriptação. Em verdade são indicadores de transformações atinentes à porosidade da soberania estatal e da autonomia individual. Indicam uma transformação profunda na concepção jurídica de vontade livre e discernida, impactando no conceito de capacidade jurídica. Entretanto, são efeitos e não a causa dessas modificações. Efeitos esses oriundos de uma nova forma de existência e de inter-relacionamento, intermediados por plataformas digitais, e atravessada pela dicotomia entre digital e material.

Na seção seguinte são apresentados elementos conceituais da TEP (SANÍN-RESTREPO, 2017), teoria filosófica que foi utilizada como lente crítica das reflexões preliminares da pesquisa. A seção tem por objeto elucidar que a TEP não é marco teórico da tese e não tem aplicabilidade prática para contribuir para o melhoramento da Política Nacional de Proteção de Dados Pessoais.

2.2 Por que não aplicar a TEP?

A TEP, desenvolvida por Ricardo Sanín-Restrepo (2017), foi utilizada como ferramenta crítica preliminar no início da pesquisa. Vale ressaltar que a TEP não é um marco teórico para a tese, que tem como objetivo propor soluções para déficits de efetividade da Política Nacional de Proteção de Dados, no que tange à proteção do corpo digital. Tendo em vista a nomenclatura aplicada pela TEP, o direito é um instrumento de contingência de conflitos, consistindo em uma manifestação do poder como *potestas*, por ser fonte de criação de estruturas sólidas e estáticas, que condicionam, hierarquizam e classificam a existência, o pertencimento, o que é legal ou não, quem pode falar e ser ouvido e quem é invisível à perspectiva da legalidade. Essa lógica operacional consistiria na forma primária de violência ao estabelecer imposições que criam uma dimensão simulada da realidade, que produz a negação da diferença (simulacro). É o poder, sob a aparência de dominação, um instrumento de privação da diferença.

Para a TEP, o poder consiste tanto no exercício da diferença imanente quanto em sua privação. Assim, sob o argumento de ser uma fonte de segurança e de garantias para os seres, a lei neutralizaria sua agência (ação política), docilizando, encapsulando e impedindo sua própria existência, na medida em que obstaculizaria o exercício da diferença. Toda forma de *potestas* cristalizaria e anularia a *potentia* (poder constituinte, poder democrático), ao fixar

conceitos, estruturas, noções e significados, impedindo a ressignificação (através da imposição de modelos transcendentes).

Encriptar o poder para a TEP é simular o poder. Sob a perspectiva da colonialidade e da globalização, com a crescente incorporação de leis sem força coercitiva (*soft laws*) criadas por organizações internacionais (sob influência do lobby das plataformas digitais), observa-se que a encriptação constituiria a característica definidora e central do poder na sociedade informacional, à luz da TEP. O poder seria simulado de forma mais sofisticada do que nunca. A encriptação como um processo de simulação da diferença, de ocultação de razões, intenções e significados de conformações pré-estabelecidas do mundo à vista de todos, estaria ocorrendo em relação à proteção de dados, beneficiando as plataformas digitais, sob o argumento de proteger o corpo digital, simulando proteção, criando um direito, mas sem pensar em estratégias de reforço que o viabilizem. Logo, o titular dos dados seria, na verdade, um *povo oculto* conceituado no plano normativo de forma abrangente como toda pessoa natural, mas na prática a proteção de dados existiria apenas para algumas pessoas. A noção de povo oculto para a TEP é operada por sinédoque, por metonímia, pela adoção de uma noção totalizante que não enxerga a diferença e a (in)viabilidade da totalidade.

Apesar de partir da premissa de que, na sociedade informacional, o poder do indivíduo no exercício de sua autonomia e o poder dos Estados nacionais no exercício de sua soberania são simulados, ou seja, sofrem com a encriptação do poder real das plataformas, a pesquisa resultou na conclusão de que o modelo predominante de privacidade e proteção de dados é um indicador dessa encriptação. Assim, a eventual inefetividade das políticas públicas decorrentes desse modelo também é um indicador e não um agente de encriptação. A TEP apresenta uma perspectiva filosófica muito interessante, mas é inaplicável ao contexto material das políticas públicas, esgotando sua relevância na denúncia da inefetividade. A encriptação e o estabelecimento de simulacros da realidade ocorrem conjunturalmente por meio de condicionamentos que forjam a mentalidade predominante e a forma de ver o mundo. Eles não são necessariamente o resultado de ações calculadas e orquestradas por grupos específicos. Eles refletem a colonialidade na disseminação e validação do conhecimento e no endosso de práticas como modelos (COULDRY, MEJIAS, 2019). No caso da proteção de dados, essa colonialidade é expressa pela divisão do aprendizado que permite o exercício de um poder instrumentário (ZUBOFF, 2019). O poder instrumentário é a base das "estratégias do capitalismo de vigilância" e, a partir da divisão do aprendizado, é produzida nova forma de analfabetismo "que aprofundaria ainda mais a lacuna entre os "*information-haves*" e "*information-have nots*"" (RODOTÀ, 2008, p. 40). Com a reestruturação do capitalismo, um modelo de expropriação da

informação é estabelecido e mediado por plataformas. Essa divisão (do aprendizado e do conhecimento) fomenta e retroalimenta a assimetria de poder entre as plataformas e os titulares dos dados.

Por mais que a adoção de normas de proteção de dados consista na repetição de um padrão por meio da criação de uma nova *potestas*, aparentemente servindo intenções diversas dos argumentos para o estabelecimento do *modelo transcendente*, na perspectiva da TEP, apostar em hackear o sistema utilizando a lacuna criada para guiar a política rumo à efetividade parece um caminho mais frutífero do que realizar pesquisas que se esgotam na denúncia, sem propor formas de modificar o que está posto. Em outras palavras, mesmo que a política pública de proteção de dados gere aparente conformidade em um primeiro momento, ela já abre caminho para pensar o que a proteção de dados deve efetivamente representar e exigir para proteger os direitos da personalidade e o corpo digital na sociedade informacional. Ademais, a medição e o melhoramento contínuo fazem parte do ciclo de vida das políticas públicas, sendo imperioso que os pesquisadores do campo sigam dedicados a fomentar estratégias que apoiem o propósito de aprimoramento.

Na seção seguinte são abordados os meios pelos quais as plataformas expropriam os dados pessoais como matéria prima, e como essa espoliação é utilizada para a geração de riquezas e criação de mercados futuros.

2.3 Sociedade informacional, plataformas e a mitigação do livre desenvolvimento da personalidade

A sociedade informacional, em que, conforme mencionado, a informação passa de elemento periférico para principal ativo de negócios, emerge como consequência da reestruturação do capitalismo após a crise de 2008 (SRNICEK, 2017, p. 24-35). Com essa reestruturação, o digital, se utilizando da automação da internet das coisas e da tecnologia de maneira crescente, passa a impactar todos os campos da vida, além de ser utilizado como instrumento para a expropriação de material bruto para a acumulação de riquezas, sendo esse material bruto composto por dados (SRNICEK, 2017, p. 23), sobretudo os dados pessoais, ou seja, informações relativas a pessoas naturais individualizadas ou individualizáveis (BRASIL, 2018). A comoditização dos dados pessoais é característica do capitalismo de plataforma, que se vale da vigilância (RODOTÀ, 2008; ZUBOFF, 2020) e do subsídio cruzado (SRNICEK, 2017) como fonte de extração de matéria prima. Quanto ao subsídio cruzado, Srnicek (2017, p. 46-47) esclarece que com frequência as plataformas digitais expandem e fidelizam pela oferta

de serviços ou comodidades gratuitas ou a baixo custo, que funcionam como elemento de atração para usuários, mesclada com serviços e produtos pagos. O valor de mercado da plataforma digital é medido pelo nível de engajamento que ela provoca nos seus usuários, pela quantidade de usuários que interagem no seu ambiente digital ou utilizam a sua estrutura.

No capitalismo de plataforma e de vigilância a dominação ocorre pela divisão do aprendizado e do conhecimento, ou seja, pela detenção de uma expertise que permite o refinamento de informações para a predição e criação de mercados futuros pelo mapeamento de vulnerabilidades e utilização desse conhecimento para o envio de estímulos que modulam à vontade. Outro fator que milita em favor do domínio das plataformas digitais é a ausência de regulação quanto à sua relação com os usuários, de maneira que os termos em que essa relação se estabelece, assim como os parâmetros para os limites no uso (tipo de conteúdo que pode ser postado, regras para retirada de conteúdo do ar ou cancelamento de perfil, entre outras) ficam à cargo das próprias plataformas, através da instituição dos Termos de Uso (expressão de um "quase-poder legislativo"). Uma sanção por retirada de conteúdo que fira os Termos de Uso, por exemplo, pode ser aplicada sem que isso demande qualquer atuação de autoridade pública. Muitas vezes o usuário não dispõe de meios para contestar a decisão pela sanção aplicada, em demonstração cabal da assimetria de poder existente entre as plataformas e seus usuários e entre as plataformas e as autoridades estatais. Note-se que o contrário ocorre caso uma autoridade estatal ou um usuário busque derrubar um conteúdo que considere aviltante, ao passo que somente terá qualquer possibilidade de solicitar isso para a plataforma digital que o hospede após obter uma decisão judicial favorável. A esse respeito, vide ênfase dada por João Pedro Quintais, Giovanni de Greggorio e João C. Magalhães (2023, p. 5-6):

> Besides, the exercise of quasi-legislation is not the only expression of platform power. Platforms can enforce contractual clauses directly without the need to rely on a public mechanism, such as a judicial order or the intervention of law enforcement authotities. For instance, the removal of copyright-protected content can be performed directly by platforms without the involvement of any public body. This technological asymmetry is the grounding difference from traditional offline boilerplates contracts. [...] the code – or the platform's internal systems – assumes the fuction of the law, and the network architecture becomes a modality of regulation. Platforms can directly enforce their rights through a quasi-executive function. This private enforcement is the resulto f na asymmetrical technological position in respect of users. [...] together with these normative and executive functions, platforms can also exercise a quasi-judicial power. This power mirrors the role of constitutional courts, namely the balancing of fundamental rights [...].

Para atender aos objetivos de reformulação do capitalismo era necessário um novo modelo de negócios que canalizasse essa vantagem de detenção de conhecimento tão poderoso. E esse novo modelo, que emerge na primeira década dos anos 2000 e se torna cada vez mais comum, é a plataforma digital. Por plataforma entende-se a infraestrutura digital que permite a

interação entre dois ou mais grupos ou sujeitos, se colocando num patamar de intermediadora dessa interação (SRNICEK, 2017, p. 24). A título de exemplo, o *Google* enquanto plataforma de busca, provê o conteúdo buscado pelo usuário e ao mesmo tempo, de posse dessa informação sobre termos de busca, intermedia a exposição a propagandas de serviços e produtos, de outras empresas, que estejam alinhados com os aparentes interesses desse usuário. Dessa forma, o grande poder das plataformas digitais reside no efeito de interligação em rede, tendo o seu valor e poder aumentados à medida que mais pessoas as utilizam como instrumento de intermediação para acesso de produtos e serviços (SRNICEK, 2017, p. 25), o que leva estudiosos[24] (VAROUFAKIS, 2021) a aventarem a possibilidade de uma nova reestruturação do capitalismo baseado na fidelização e na mudança de *mindset* quanto à maneira de acumular riqueza. Um clássico exemplo da mudança de paradigma quanto à acumulação de riqueza pela garantia de mercado futuro (com a fidelização), ao invés de pelo lucro imediato, é o da indústria de entretenimento televisivo, que de maneira quase unânime migrou para o *streaming*. Em que pese a audiência dos canais siga sendo relevante, o seu alcance é potencializado pela disponibilização de aplicativos para acesso ao conteúdo, e a fidelização garantida e incentivada, criando o consumo futuro pelas sugestões de títulos, pautadas no perfil traçado do usuário, com base no que foi consumido anteriormente. O mesmo acontece com a indústria da música. Não se busca mais ganhar quantitativamente (mantendo o parâmetro do preço unitário para o lucro), mas sim qualitativamente na criação de uma simbiose, de uma necessidade que gentilmente compele o usuário a se manter fiel ao fornecedor. Sendo assim, a noção de plataforma compreende um contorno conceitual muito mais amplo do que a internet, ou IA, embora as utilize na sua operacionalização e para a fidelização narrada.

As plataformas com todas as suas nuances e se valendo do dinamismo tecnológico, atravessam e modificam as formas de produção, de consumo, de trabalho, de interação interindividual, tendo, inclusive, forte impacto na formação da subjetividade e da vontade. Não somente pelo uso de técnicas de psicologia[25] para persuadir e induzir ao conforto cognitivo,

---

[24] A profunda transformação do capitalismo em virtude da economia pautada no fornecimento de bens não-rivais, ou seja, cujo uso de um não implica em prejuízo para o uso de outro consumidor, faz com que as organizações prescindam do lucro como alvo. A fidelização move ainda o mercado financeiro. Os bancos, para Varoufakis, também não são mais movidos pelo interesse de obter lucros, mas de fidelizar o cliente e mantê-lo numa trama de crédito/débito infinita. Alguns desses *insights* foram apresentados na entrevista de Savoj Zizek a Yanis Varoufakis, ex- Ministro das Finanças da Grécia. Disponível em: https://www.youtube.com/watch?v=XIgFnfHhcRc&list=PL59HwCw5piWPen5vhYuZ3jsWLExaVTdNc&index=31. Acesso em 14 Nov. 2021.

[25] No livro "Rápido e devagar: duas formas de pensar" (2012), Daniel Kahneman apresenta os modos com que o cérebro age para solucionar determinados problemas, pensando de maneira mais analítica e empreendendo esforço maior quando está em desconforto cognitivo (pensamento devagar), ou atuando de maneira mais automatizada,

mas por diversos componentes e derivados que permitem que grandes agentes de tratamento de dados possam traçar um perfil exato dos usuários, como mencionado. Esse perfil, esse corpo digital, pode ser determinante não somente para diversas atividades e intenções do presente, mas pode representar a fortuna ou desgraça dos sujeitos no futuro. Um futuro sobre o qual não se tem ingerência, tampouco a certeza do que o sistema legal e o arcabouço cultural considerarão características "adequadas" ou "desejáveis".

Desde sempre, na vida material, *off-line*, os sujeitos foram julgados por características externas (aparência, vestimenta, postura corporal, voz etc.) ao concorrer a uma vaga de emprego ou mesmo em relacionamentos amorosos ou de amizade. Na sociedade informacional, em decorrência da "plataformização" da vida, o corpo digital contempla muito mais do que está aparente, refletindo as tendências e vulnerabilidades mais íntimos (a ubiquidade tecnológica nessa realidade digital permite a inferência sobre como uma pessoa ou grupo se movimenta, com que ritmo anda, se é sedentário ou ativo, se possui alguma dificuldade de mobilidade ou não, onde vive (geolocalização), que dispositivos utiliza (endereço de IP e identificadores de dispositivos móveis e fixos), se dorme bem ou mal, o que compra, de que lojas consome, que conteúdo de entretenimento prefere, o que o preocupa, o que quer saber sem ter que perguntar a um especialista, com quem se relaciona, etc.. O simples fato de se usar um *smartphone*[26], que concentra uma série de plataformas em si, possibilita o conhecimento sobre todas as informações citadas.

Esse corpo digital não é somente formado por conteúdo gerado explicitamente (*posts*, *likes*, seguir uma página ou perfil etc.), mas também por manifestações comportamentais residuais (tempo de resposta aos e-mails, número de *logins* em plataformas, tempo gasto em cada aplicativo, manutenção do cursor do mouse num determinado local da tela, tempo de rolagem da tela etc.). Documentos passam a ser digitais, bancos de dados também, a internet

quando em conforto cognitivo (pensamento rápido). Ao discorrer sobre os motivos que induzem ao pensamento rápido ou devagar e como fatores são explorados para essa indução, o autor expõe entre elementos que contribuem para isso o uso de determinadas cores, de linguagem mais simples e direta ou mais rebuscada, a indução ao foco num determinado tópico, a vivência, a facilidade ou dificuldade em lidar com determinadas matérias entre outros.

[26] Os *smartphones* tem em sua composição acelerômetros (capazes de identificar a velocidade com o usuário se movimenta e inferir se estamos andando ou em algum veículo), sensores de proximidade com outros dispositivos (assim funciona a tecnologia do *bluetooth*, localizador (que permite que usemos o GPS e que possamos habilitar função de detectar onde o dispositivo está), funcionalidade de gravação de som ambiente (a partir da qual podemos acionar funções de comando de voz), entre outros. Ademais, o fato de celulares modernos acessarem a internet via *wifi* e contarem com funcionalidades de armazenamento de arquivos (fotos, áudios, textos) em nuvem possibilita ainda uma maior extração de dados comportamentais (redes de *wifi* utilizadas, contatos registrados na agenda, tempo de resposta aos e-mails, tempo de acesso em redes sociais, tempo de exploração de cada aplicativo, que aplicativos são instalados, entre outras informações) que nos tornam vulneráveis e contribuem para a formação do nosso corpo digital e da nossa personalidade digital (como realmente nos apresentamos na Sociedade Informacional).

das coisas domina os novos aparelhos e objetos desenvolvidos. Com a computação ubíqua tudo pode ser medido e "melhorado", mas para isso as informações a respeito do uso e dos usuários precisam ser registradas, armazenadas e comparadas. Os seres humanos são convertidos em "eus quantificados" (*quantified selves*) (PASQUALE, 2015, p. 4), em resultados das informações angariadas sobre si, que permitem que sejam analisados, classificados e ranqueados em cálculos de riscos em grande parte das atividades na vida (candidatura à empregos, pedido de empréstimo, pedido de auxílio assistencial, avaliação de produtividade, relevância de conteúdo a ser acessado em buscadores e em redes sociais, entre outras).

Assim, a vida digital intermediada por plataformas, seus componentes e derivados, tem acelerado a porosidade da autonomia da vontade, em âmbito individual, e da soberania, em âmbito (inter)nacional, com uma desfronteirização de questões atinentes ao tratamento de dados pessoais. Pela designação de "componentes e derivados das plataformas", trata-se de repercussões tecnológicas que são derivadas do funcionamento de sistemas de IA ou se utilizam de alguma maneira da IA para sua operacionalização. São exemplos de componentes e derivados que contribuem para a viciação da formação da vontade o uso de algoritmos, o *machine lerarning* e o *deep learning*, o *big data*, o emprego de *internet of things (IoT)* em objetos utilitários e vestíveis, as *câmaras de Eco* e os *filtros bolha* (ou bolhas virtuais), assim como o produto do emprego de mineração de dados por operações algorítmicas, que resulta num *perfilamento* (*profiling*) bastante apurado.

Muitos dos componentes e derivados das plataformas são apresentados aos indivíduos como altamente convenientes e vantajosos por proporcionarem a *personalização* e uma "melhor experiência do usuário" nas interações, seja por acesso a dispositivos inteligentes, aplicativos e ou páginas da web. Essa "conveniência" agregada a uma visão de inevitabilidade de todo esse contexto orientado por dados é uma das estratégias utilizadas pelos detentores desse conhecimento (as *big techs*, os detentores de capital financeiro, bancos e investidores, grandes indústrias e Estados nacionais) no *ciclo da despossessão* (ZUBOFF, 2019, p. 164), que enreda os seres na habituação e naturalização dessa intrusão nas suas esferas privadas e na sua intimidade.

A porosidade em estruturas de poder é refletida tanto na perda de autonomia pelo indivíduo, que tem a formação da sua vontade viciada pela interação com as plataformas, quanto no que tange o poder estatal[27]. Assim como os Estados nacionais têm se rendido às demandas

[27] Por óbvio, influências quanto ao exercício de autodeterminação por indivíduos e pelo Estado sempre existiram e são parte da convivência em sociedade. O documentário da BBC "*The century of the self*" (2002), aborda a

internacionais para seguir inseridos na rede global, o indivíduo tem a importância da sua vontade manifesta discernida relativizada, ante a flagrante viciação dos processos de tomada de decisão.

A economia colaborativa e de bens não rivais[28], com seus aplicativos, lida com a previsibilidade dos comportamentos, oferecendo serviços e produtos, e criando necessidades, de maneira cada vez mais assertiva. A sociedade informacional é permeada pela ação de algoritmos que influenciam as decisões, os gostos, as discussões e definem quais temas ganham os holofotes e a atenção. Na conjuntura descrita a vontade é inegavelmente relativizada, merecendo atenção a repercussão dessa relativização no que tange aos direitos da personalidade. Ante o exposto, cumpre trabalhar a definição dos componentes e derivados das plataformas. Em seguida, se explicitará como a interação com plataformas opera o sequestro da vontade livre e discernida, impactando na livre formação da personalidade, e na própria dignidade humana, por impossibilitar a autoconstrução e autorrepresentação, além de impossibilitar o controle dos *outputs* gerados na interação com as novas tecnologias, obstando a autodeterminação humana e impedindo com frequência a possibilidade de se contrapor a decisões feitas com base no corpo digital.

Conforme mencionado, as plataformas comumente utilizam IA na sua composição e funcionamento. O conceito de IA não é uníssono, assim, primeiramente necessário esclarecer o que se entende por sistemas de IA. Conforme assevera Henrique Alves Pinto (PINTO, 2019, p. 44), muitas definições de IA salientam semelhanças comportamentais (*behavior*) entre o funcionamento de máquinas em relação aos humanos, outras são pautadas nos estudos sobre a forma humana de pensar, de chegar a conclusões, de tomar decisões (*reasoning*). Entende-se

gênese da propaganda, e demonstra que essas modulações da formação da vontade já ocorriam em contexto analógico. Entretanto, com a escalabilidade da internet e a crescente interação com sistemas de IA e novas tecnologias, a vulnerabilidade dos sujeitos a essa modulação aumenta, pelo incremento do subsídio que os manipuladores passam a ter. Ademais, quando a intrusão e a influência são sutis e naturalizadas é onde ocorre o perigo de simulacros, de crescentes cooptações e simulações da realidade que impedem a diversidade em sentido de tomada de rumos diversos. Antes a "imposição" de posicionamentos e de orientações acontecia de maneira flagrante, com o uso da força bruta, da coação. Hoje em dia as manipulações e conformações da realidade se dão silenciosamente, sendo dotadas de aparente legitimidade. É notável o fato de que muitas das decisões automatizadas que são tomadas por organizações e pelo Estado e que afetam drasticamente a nossa vida não podem ser devidamente questionadas, ao passo que protegidas pela opacidade com que o processo de decisão ocorre. Como nos alerta Frank Pasquale (2015, p. 217-218), a sociedade em que vivemos orientada por informações, se seguir sem intervenções efetivas que quebrem a opacidade dos tratamentos de dados pessoais e de fato assegurem a autodeterminação informativa, desembocara numa aristocracia digital, que empodera somente os experts, a despeito das promessas de liberdade e autodeterminação conduzidas pelos mestres da inovação e dos avanços tecnológicos. Alerta similar é feito por Shoshana Zuboff (2019) ao tratar da "divisão do aprendizado" e sua importância em termos de excluir e classificar os sujeitos que não possuem o conhecimento sobre as novas tecnologias. A divisão do aprendizado conduz à assimetria de conhecimento e de poder entre as plataformas e os titulares de dados.

[28] Por bens não rivais entende-se os bens que não se esgotam pelo consumo e que possibilitam utilização mútua sem prejuízo para o uso por outros usuários. Como exemplo clássico da atualidade temos a assinatura de *streaming*.

por sistemas de IA os sistemas programados para a automatização de atividades comumente relacionadas à cognição humana, em uma mescla entre comportamento e processo de tomada de decisões. Sistemas de IA permitem às tecnologias computacionais aprenderem com os dados, sem serem explicitamente programadas quanto à sua operação. Dessa forma, em teoria, quanto mais robusto for o banco de dados que alimenta o sistema de IA, mais acurado será o resultado da operação dos algoritmos. No dizer de Alexandre Veronese, Alessandra Silveira e Amanda Nunes Lopes Espiñeira Lemos (2019, p. 237- 244), em sentido estrito, a IA consiste na formulação de uma máquina de Turing que possa aprender por meio de repetição, por tentativa e erro, sendo, de certa maneira, impróprio o emprego do vocábulo "inteligência", ainda que a maximização da capacidade de tratar dados para realizar inferências seja fenômeno decorrente da operação da IA. Sendo assim, o emprego da palavra "inteligência" diz mais respeito a essa capacidade da IA de aprendizado.

O funcionamento dos sistemas de IA, conforme mencionado, é realizado a partir de operações automatizadas, orientadas por algoritmos. Algoritmos são sequências matemáticas que estabelecem no desenvolvimento de um sistema os procedimentos percorridos para a solução de um problema, para atingir um objetivo específico. Em linhas bastante gerais, pode-se definir algoritmos como o "passo a passo" inserido na programação para a operação com dados. De maneira mais técnica[29], tem-se que "[...] *an algorithm is any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as output"* (YANOFSKY, 2011)[30]. Existem os algoritmos *black boxes*[31]

[29] De maneira ainda mais refinada é possível distinguir programas, que são criados por programadores e desenvolvedores de *softwares*, de algoritmos, que são criados por cientistas da computação. Já as funções computáveis, usadas para a resolução de problemas, que são usadas para a criação de algoritmos e para a programação são de interesse puramente matemático.

[30] "[...] um algoritmo é qualquer procedimento computacional bem definido que emprega um valor ou conjunto de valores, como input e produz um valor, ou conjunto de valores, como output." *Tradução nossa.*

[31] Conforme esclarece Frank Pasquale (2015, p. 3), o termo *Black Box* é utilizado comumente tanto para designar dispositivos de gravação como os existentes em aviões, que se prestam a monitorar dados do voo e manter registro desses dados e de sons ambientes da cabine de comando, quanto para tratar de sistemas que trabalham de maneira misteriosa, ou seja, em relação aos quais é possível observar os *inputs* e os *outputs*, ainda que não seja possível descrever como um resulta no outro. No livro *"The black box society: the secret algorithms that control money and information"*, Pasquale (2015. p. 6-7) explora três estratégias usadas pelas organizações da internet e do mercado financeiro para manter seus sistemas de funcionamento fechados, como *black boxes*, ou seja, incompreensíveis, não interpretáveis, opacos: segredo real (*real secrecy*) que ocorre com o estabelecimento de uma barreira física ou técnica para acesso ao conteúdo (o autor usa o exemplo das portas que trancamos e do uso de senhas para acesso aos e-mails); segredo legal (*legal secrecy*) operada pelas normas estatais ou organizacionais que impedem a revelação de informações a que se tem acesso pelo exercício de função privilegiada (por exemplo, a necessidade de um empregado do banco de manter sigilo quanto aos dados dos clientes, e de um advogado de manter sigilo sobre informações a que tem acesso dos clientes); e ofuscação *(obfuscation*), que consiste numa prestação de contas ou numa transparência deliberadamente confusa e repleta de informações desnecessárias, somente para confundir quem estiver analisando, ou atrasar os resultados da análise. Segundo Shoshana Zuboff (2019) essa tem sido a estratégia da Meta e de outras plataformas ao prestar esclarecimentos para autoridades de proteção de dados sobre suas práticas.

(CASTELVECCHI, 2016; HOLM, 2019) que se autoprogramam (quem os cria não tem como explicar o percurso dos *inputs* observados, assim não tem como definir as razões para os *outputs* recolhidos a cada operação). Em suma, os algoritmos *black boxes* não são transparentes e interpretáveis[32].

Com a sofisticação da tecnologia, os algoritmos utilizados comumente são predispostos ao aprendizado, possibilitando a autoprogramação dos sistemas de IA, com base na ampliação da base informacional que subsidia a sua operação, a partir da identificação de novos padrões, à medida em que a base de dados se torna mais ampla. Importante destacar que a IA se estrutura a partir de sistemas desenvolvidos e programados para identificar padrões mediante uma base de dados, que fornece subsídio para encontrar soluções probabilísticas[33] (EKEL, 2022) para os problemas que orientam a sua programação, ou seja, para traduzir dados pretéritos em informações específicas (vale reforçar, a IA orientada por informações do passado).

A capacidade de aprendizado – *machine learning*[34](IBM, 2020) – se concretiza por inferências, à medida em que a base de dados é alimentada, com a aptidão para desenvolver a capacidade de resolução de problemas que orientaram a programação de forma cada vez mais assertiva e autônoma, sem a existência de programações adicionais, ou seja, a máquina aprende com os dados, com os padrões identificados. Os sistemas pautados em *deep learning*[35]

---

[32] Importante salientar que existe diferença entre transparência, interpretabilidade, explicabilidade e auditabilidade de sistemas de IA. Consoante esclarecido em artigo elaborado em coautoria com Márcia Maria Wengerter da Silva (*no prelo*): transparência consiste na oferta de informações acerca da finalidade de operação do sistema de IA, sobre os agentes que integram a sua operação e, no que concerne os algoritmos, quais são os critérios gerais que orientam o seu funcionamento (o porquê do *output*); interpretabilidade consiste na viabilização da interpretação da decisão automatizada resultante da operação do algoritmo, ou seja, na possibilidade de o usuário de um dado sistema de IA entender e interpretar os critérios que conduziram a uma decisão, a um *output;* explicabilidade consiste no emprego de medidas técnicas e administrativas no desenvolvimento e monitoramento da IA para que cada processo decisório, cada *output*, possa ser rastreado e explicado; por fim, auditabilidade consiste na possibilidade de terceiro avaliar o método utilizado pelo algoritmo para o alcance do resultado apresentado. Neste ponto, recomendo a exploração do site da IBM que traz de forma clara e didática conceitos pertinentes às tecnologias que envolvem sistemas de IA. É possível verificar a diferenciação em análise no link: https://www.ibm.com/br-pt/watson/explainable-ai#:~:text=Explicabilidade%20versus%20interpretabilidade%20em%20IA&text=A%20interpretabilidade%20%C3%A9%20o%20grau,a%20IA%20chegou%20ao%20resultado. Acesso em: 06 ago. 2021. Interessante também a leitura do artigo de Laura Schertel Mendes e Marcela Mattiuzzo (2019) "Discriminação algorítmica: conceito, fundamento e tipologia", referenciado nesta tese.

[33] Diferentemente de outras tecnologias computacionais, a IA funciona com base em dados pertinentes a situações passadas. Vale ressaltar, ela atua em abordagem probabilística e não possibilística, por ser subsidiada por padrões encontrados no seu banco de dados, sem a habilidade de, de maneira automática, traçar cenários que nunca ocorreram. A programação de sistemas voltados a criação de cenários possibilísticos, que permitem o suporte a tomada de decisão em cenários complexos, que envolvem variáveis quantitativas e qualitativas inexatas, pode ser feita com o emprego de números *fuzzy*, através de modelos de tomada de decisão multicritério (pautados em função de objetivos, atributos ou mistos) (EKEL, 2022).

[34] São exemplos de *machine learning* recomendação de títulos em serviços de *streaming*, tecnologias de reconhecimento facial, sistemas de autoatendimento.

[35] São exemplos de *deep learning* a análise de estados emocionais e a identificação de sentimentos, além de sistemas de identificação de fraudes com base no comportamento de consumo usando cartões de crédito.

(CASTELVECCHI, 2016; HOLM, 2019) contam com redes neurais construídas em semelhança ao cérebro humano, mais complexas e cujo funcionamento se baseia em difusão das informações aprendidas (sem o seu armazenamento num bloco de memória digital), que implica capacidade de processamento de situações complexas do mundo real, usando algoritmos *black box*.

Os *smart objects*, entendidos como os objetos cujo funcionamento é pautado na ligação com a internet[36], são dotados de sistemas de IA, cuja tecnologia é designada de *Internet of Things (IoT)* e operam pela intermediação de plataformas. Conforme mencionado por Abhik Chaudhuri e Ann Cavoukian (2018, p. 2-3), a tecnologia de IoT, em rápida evolução, atualmente permite a captura em escala maciça, sendo que os sensores em uso "têm poder de computação limitado, dificultando a renderização de criptografia forte durante a comunicação de dados dos sensores para o gateway" (CHAUDHURI, CAVOUKIAN, 2018, p. 2-3). Da mesma forma, "enviar de volta o controle para o atuador em formato criptografado também não é viável pelo mesmo motivo" (CHAUDHURI, CAVOUKIAN, 2018, p. 3). Os dados coletados pela IoT estão impulsionando o design de novos modelos de negócios e serviços, incluindo a tecnologia como entrada para operar o feedback de dados por plataformas digitais. Como resultado, o aumento do uso da IoT também traz preocupações em relação à privacidade e à proteção de dados dos usuários.

Da mesma forma, as redes sociais, as plataformas de interação remota, os sites de compra *on-line*, os aplicativos de celular, entre outros, todas essas amenidades que trazem comodidades à vida cotidiana operam pela intermediação de plataformas digitais. Entre os objetos inteligentes com IoT é bastante comum o uso de objetos vestíveis, que possuem uma capacidade de coletar dados muito mais intrusiva, inclusive dados sensíveis, como os pertinentes à saúde, dados biométricos, entre outros. Por exemplo, os relógios *smart*, que, entre outras funcionalidades comuns, como a contagem de passos (cujo número é ligado à hábitos cotidianos, ser mais ativo, ou ser mais sedentário, passar o dia sentado ou em movimento mais intenso), possuem tecnologia que permite a geolocalização, a gravação de percurso, a aferição de pressão arterial, monitoramento de níveis de estresse, monitoramento cardíaco, capacidade de identificação de atividade física que está sendo realizada com base no cruzamento de informações (batimentos cardíacos, movimentos do corpo e geolocalização, podendo inferir se

[36] Importante lembrar que objetos que estão conectados à internet podem ser invadidos por hackers, de maneira que esse potencial de coleta de dados de maneira intrusiva pode vir a prejudicar o usuário diretamente em seus interesses, o vulnerabilizando em outras esferas, para além da esfera do consumo. Inclusive com falsidade ideológica, assumindo a identidade digital do usuário para cometer fraudes.

o usuário está realizando um treino na esteira, ou correndo em ambiente externo, por exemplo, se está nadando ou praticando remo), monitoramento da qualidade do sono, gravação de sons externos para identificação de ronco e apneia, entre outras funcionalidades muito úteis, mas perigosas, quando considera-se possibilidade de vazamento desses dados, e o poder que eles proporcionam às empresas privadas que administram os aplicativos (plataformas digitais).

Outro exemplo de produto de *IoT* bastante comum é o das televisões *smart*, que podem ser acionadas e operadas com reconhecimento de voz, ou seja, possuem a capacidade de gravar sons ambientes (da mesma forma os dispositivos inteligentes de música), muitas possuem câmeras também, o que significa que possuem a funcionalidade de capturar imagens. Os aspiradores de pó inteligentes podem mapear as superfícies que limpam, para possibilitar o seu acionamento remoto e a otimização da limpeza sem a supervisão do usuário. As geladeiras, máquinas de lavar roupa, os celulares e tablets que destravam com a leitura da íris ou com identificação facial, termostatos, fechaduras inteligentes e uma numerosa lista de objetos *smart* proporcionam a conveniência de personalização para melhor experiência do usuário, a partir da massiva coleta de informações sobre os seus hábitos e da captura de traços que o identificam inequivocamente (voz, íris, dados biométricos).

A capacidade e captura de dados é preocupante no que tange à privacidade, e ainda mais alarmante no que diz respeito à formação da vontade e à formação do corpo digital, em virtude do *big data*, ou seja, da existência de bancos de dados que armazenam e processam uma enorme gama de informações expropriadas dos indivíduos. Conforme destacam Rob Kitchin e Gavin McArdle (2016), a utilização do termo *big data* remonta aos anos 1990, inicialmente com John Mashey, para se referir à possibilidade de análise de uma quantidade massiva de dados. Em 2001, a partir do trabalho de Doug Laney, o conceito passou a integrar as características de tratamento de dados operacionalizado com *velocidade* (produção; publicação do dado em tempo real, imediatamente após o comando), *volume* (quantidades enormes de dados no banco a ser analisado) e *variedade* (banco de dados constituído de dados estruturados, semiestruturados e não estruturados). A partir dessa definição inicial, novas características foram agregadas ao contorno conceitual de *big data*: *exaustividade* (um sistema de dados inteiro é analisado, ao invés de somente uma parcela ou amostra); *refinamento* (específico na resolução) e *unicidade na indexação* (atua por indexação, pela escolha de termos-padrão); *relacionalidade* (possibilidade de conter campos comuns que habilitem a junção de diferentes conjuntos de dados); *extensionalidade* (possibilidade de adicionar ou modificar campos facilmente); *escalabilidade* (pode ser expandido em tamanho rapidamente); *veracidade* (os dados que compõem sua base podem ser bagunçados e conter incertezas ou erros); *valor* (muitos

insights podem ser extraídos da sua operação e a base redirecionada para uso em outros propósitos); *variabilidade* (o sentido dado aos dados pode ser constantemente modificado de acordo com o contexto em que são gerados ou analisados).

Fato é que o *big data* é qualitativamente diferente da tradicional análise *small data*[37] em diversos eixos, incluindo a qualidade dos dados, a possibilidade de redirecionamento do uso e a gestão. Enquanto o *big data* permite a utilização de dados em diversas formas de estruturação, o que possibilita maior relacionalidade, interoperabilidade e o redirecionamento de propósito da mesma base, e o dota de maior flexibilidade, permitindo a gestão contínua da mesma base que pode ser ampliada ao longo do tempo, o *small data* tem que operar com dados da mesma qualidade e com propósitos delimitados. Assim, a operação do *small data* é episódica e se esgota com a finalidade para a qual foi criado (KITCHIN, MCARDLE, 2016, p. 2). Analisando vinte e seis tipos de *big data* Kitchin e McArdle (2016, p. 8) destacam que as características de velocidade de processamento e exaustividade são as que mais distinguem *big data* de outras formas de sistemas de dados.

Com o *big data* é possível traçar um perfil bastante preciso dos sujeitos que interagem com plataformas. Esse processo de elaboração de um perfil eletrônico é denominado de *profiling*, também designado de perfilamento ou perfilização. O perfilamento é fruto do processamento de informações pertinentes às pessoas naturais resultando de uma decisão automatizada de categorização. Em suma, na sociedade informacional os seres são o que os seus dados informam, a partir da interação com organizações privadas e públicas, através de plataformas digitais e nas atividades da vida material. Tendo em vista que o perfilamento é resultado da operação de sistemas de IA, que lidam com raciocínio probabilístico, pautado em dados do passado, os perfis produzidos acabam por cristalizar premissas, assunções sobre os titulares de dados que podem não corresponder com o que o titular pensa e é na atualidade.

O perfilamento é pautado no reconhecimento de padrões, tendo como consequência a estereotipização, a categorização e a generalização, expropriando o titular dos dados da sua diversidade e unicidade. Dessa forma, a personalização, ou seja, o *output* ofertado pela plataforma ao usuário a partir do perfilamento viola a autonomia e paradoxalmente nega a individualidade do sujeito, apesar de apelar para ela. Bauman (em entrevista gravada no

[37] Mesmo que a utilização de *small data* possa se dar em relação a enormes bancos de dados, as outras características elencadas não são encontradas na sua operação, especialmente no que tange a possibilidade de reunião na base de dados de variedade estrutural, qualitativa dos dados a serem analisados. O uso de *small data* possibilita o emprego de análises de escopo reduzido, delimitado, cuja administração, portanto, é menos flexível. O *big data* pode ser administrado continuamente, com o redirecionamento do seu propósito e com a maior flexibilidade na exploração dos dados que compõem a sua base.

documentário *Everything's under control*, 2015) destaca que a personalização lida com sentimentos profundos e demandas existenciais do ser humano, de não ser abandonado, de ser cuidado, de importar, de ser significante. O apelo a essas necessidades existenciais anestesia e faz dos titulares de dados alvos fáceis e inconscientes de manipulação, de dominação sutil.

O *Information Commissioner's Office – ICO*[38], Autoridade Nacional de Proteção de Dados Britânica, descreve o *profiling* como a análise de aspectos da personalidade, comportamento, interesses e hábitos de um indivíduo, com o intuito de fazer previsões ou de tomar decisões sobre ele. O *GDPR*, no item 4 do artigo 4, define o *profiling* como qualquer forma de tratamento automatizado de dados pessoais que consista no seu uso para a avaliação de certos aspectos pessoais relativos a uma pessoa natural, em particular para analisar ou prever aspectos atinentes à performance no trabalho, situação econômica, saúde, preferências pessoais, interesses, aferir a confiabilidade, o comportamento, a localização e os movimentos de uma pessoa natural.

As análises oriundas do perfilamento classificam os indivíduos a partir de um cruzamento de informações e do estabelecimento de correlações entre diferentes comportamentos e características inferidas. Essas correlações em geral associam comportamentos a atributos de personalidade ou características de uma maneira taxativa que não necessariamente corresponde à realidade (por exemplo, o estabelecimento da assunção de que pessoas com filhos são menos inadimplentes; de que mulheres casadas provavelmente engravidarão se conseguirem um cargo efetivo; de que homens jovens solteiros dirigem de maneira mais ofensiva, entre outras generalizações subsidiadas por bancos de dados que lidam com probabilidades identificadas na sua base). As regras extraídas a partir de generalizações assumidas pela análise de perfis traçados são utilizadas para contingenciamento de riscos pelas organizações que utilizam plataformas e impactam nas chances reais de sucesso dos indivíduos que fujam aos padrões estabelecidos como ideias para a mitigação de prejuízos. O que foge ao padrão é tido como ruído do sistema, mas esses ruídos são vidas (COULDRY, MEJIAS, 2019; WALDMAN, 2019), são pessoas que têm suas potencialidades de realização diminuída pela automatização intermediada por plataformas na sociedade informacional.

Outro derivado da "plataformização" é o fenômeno dos *filtros bolha* (PARISER, 2012). A formação de bolhas de convivência, derivada da personalização dos buscadores, dos *feeds* de redes sociais e das plataformas em geral, é fruto da operação de mecanismos de seleção de

---

38 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/. Acesso em 10 Jan. 2023.

conteúdos que supostamente são mais pertinentes aos interesses de cada usuário. Entretanto, o critério de seleção do algoritmo, visando a fidelização e o engajamento, é no sentido de identificar o que é mais motivante para a continuidade da navegação para cada usuário especificamente, pautado no perfil traçado pela interação contínua com a rede. A inteligência utilizada é orientada a assegurar a manutenção do engajamento, ou seja, a continuidade da interação, alimentando ainda mais o ciclo da despossessão de dados pessoais.

> Over time, as smart environments will likely permeate societies, users – especially young people – may be automatically plugged in and guided through life along algorithm-driven pathways nudged in the best interests of whoever owns or pays to use people's data, at times with dramatic consequences. For example, addictive techniques are already concerning in the case of negative effects on children's well-being, including increased risk of suicide and depression, conflicts with parents and adverse effects on cerebral and social development (Kidron et al., 2018). (REVIGLIO, AGOSTI, 2020, p. 4).

Explicando como as bolhas virtuais são formadas, vale a lição de Cathy O'Neil (2016), que descreve como o algoritmo de refinamento das redes sociais funciona:

> As you know by now, I am outraged by all sorts of WMDs[39]. So let's imagine that I decide to launch a campaign for tougher regulation on them, and I post a petition on my Facebook page. Which of my friends will see it on their news feed?
> I have no idea. As soon as I hit send, that petition belongs to Facebook, and the social network's algorithm makes a judgment about how to best use it. It calculates the odds that it will appeal to each of my friends. Some of them, it knows, often sign petitions, and perhaps share them with their own networks. Others tend to scroll right past. At the same time, a number of my friends pay more attention to me and tend to click the articles I post. The Facebook algorithm takes all of this into account as it decides who will see my petition. For many of my friends, it will be buried so low on their news feed that they'll never see it. (O'NEIL, 2016, p. 179-180).

Esses filtros-bolha operam modulando o acesso a conteúdo, influenciando os processos de tomada de decisão dos indivíduos. Por modularem o acesso às informações, seja pelos buscadores ou mesmo nos *feeds* de redes sociais, ocasionam outro fenômeno, o fenômeno das *câmaras de eco*, refletido na retroalimentação de tendências e ideias que geram engajamento. Essas câmaras de eco, especialmente na era das *fake news*, em que o hábito de consumo de informação da população mundial mudou, com relevante percentual de pessoas utilizando as redes sociais e a internet como fonte de informação[40], o poder das grandes plataformas é ainda

---

[39] WMD, abreviatura usada para *Weapons of Massive Destruction.* Em seu livro, Cathy O'Neil reflete como a utilização de *big data* pode trazer efeitos nocivos para a democracia, fazendo uma metáfora de como essa tecnologia, lastreada na matemática, é perigosa como as armas de destruição em massa.

[40] Pesquisa realizada pelo PoderData em 2021 destacou que, em que pese 40% dos entrevistados usem a televisão como fonte de informação, 43% dos respondentes da pesquisa utilizam a internet, sendo que 22% usam redes sociais como principal fonte de informação. Vide pesquisa disponível em: https://www.poder360.com.br/midia/internet-e-principal-meio-de-informacao-para-43-tv-e-preferida-de-40/#:~:text=A%20internet%20e%20a%20televis%C3%A3o,21%25%20por%20sites%20e%20portais.. Acesso em 10 Jan. 2022.

mais incrementado, fazendo com que elas se tornem *players* inclusive na definição dos caminhos políticos dos Estados nacionais.

O fenômeno da bolha provoca exposição contínua a reverberações das crenças do usuário, que reforçam seu posicionamento e visão de mundo, o encapsulando e expondo somente a conteúdos que são congruentes com próprias convicções. As câmaras de eco são uma das justificativas apresentadas para o fenômeno da polarização, incidente em todo o mundo, por reforçarem o posicionamento pessoal de cada usuário das redes, incrementando o afastamento quanto ao que é diferente, anulando a existência e validade do que divirja desse posicionamento.

As implicações no que tange à popularização das plataformas de redes sociais e o alcance sem precedentes das *Fake News* consistem na potencialização do impacto da utilização dos dados como insumo, prejudicando os processos de tomada de decisão dos indivíduos, afetando inclusive o funcionamento e a legitimidade de escolhas democráticas. Isso porque, embora os usuários dessas plataformas não paguem pelo seu uso com moeda, eles acabam pagando com bem ainda mais valioso: os seus dados. De posse dos dados fornecidos voluntariamente, assim como das informações inferidas, geradas durante a interação do usuário e construídas, essas plataformas oferecem espaço para a veiculação de propagandas e exposição de conteúdo. Conforme alertam Tim Dwyer e Fiona Martin (2017, p. 1080), o formato de negócios das redes sociais é comercial e a obtenção de lucro se dá pelo emprego de mineração de dados e fornecimento de espaço para propaganda comportamental (*behavioural advertising*). "*On such platforms, traffic and user time (and their data) are importante parameters*"[41] (REISACH, 2020, p. 907). O potencial lesivo do engajamento nas mídias sociais é ainda mais potencializado pelo emprego de *"cross-domain tracking"*, isto é, pelo cruzamento de informações coletadas em diferentes plataformas e websites que permite um perfilamento ainda mais acurado e minucioso (REISACH, 2020, p. 908). Essa atividade de coleta cruzada permite que as plataformas de redes sociais coletem informações até mesmo sobre indivíduos que não possuem perfil em sua plataforma.

Por fim, soma-se aos componentes e derivados das plataformas brevemente apresentados, a utilização de artifícios na programação e diagramação de plataformas para a indução ao engajamento: o emprego dos chamados *dark patterns* (padrões obscuros). Trata-se do emprego de arquitetura e design pensados de maneira a dificultar (ou facilitar seletivamente) algumas ações do usuário, direcionando o seu comportamento. Entre os exemplos de padrões obscuros podemos citar os meios disponibilizados para aceitar ou negar um produto ou serviço

[41] "Nessas plataformas, o tráfico de dados e o tempo dos usuários conectados (assim como seus dados) são importantes parâmetros". Tradução nossa.

(com a facilidade para aceitar e maior dificuldade para negar, o que tem ocorrido com frequência em relação à seleção de *cookies*[42] nos sites), as letras miúdas que esclarecem a coleta agregada de mais dados do que razoavelmente esperado para a interação em curso, a inserção escondida[43] dos Termos de Uso e das Políticas de Privacidade, a elaboração desses documentos com linguagem muito técnica, evasiva[44] ou rebuscada dificultando o entendimento pelo usuário, ou o emprego de documentos excessivamente extensos como meio de desencorajar a leitura[45], e a inclusão padronizada de serviços e produtos em compras, que demandam do usuário atenção para desmarcar *checkboxes*.

---

[42] Os *cookies* são pequenos arquivos instalados no navegador ao interagirmos com páginas e aplicações que os utilizam na sua arquitetura. Os *cookies* coletam dados de navegação e são comumente utilizados para salvar senhas e nomes de usuário, assim como em sites de compras para salvar itens selecionados ou buscados para compras. Uma utilização comum é para o direcionamento de anúncios.

[43] Em que pese liste-se aqui a disponibilização camuflada de Termos de Uso e Política de Privacidade ou mesmo a utilização de documentos excessivamente extensos como *dark patterns*, muitas vezes, mesmo a disponibilização de documentos com *design* que facilite a consulta pelo usuário é ineficaz no que tange a proteção de dados e o exercício efetivo de uma autodeterminação informativa. Isso porque em muitos segmentos de mercado o titular de dados não tem opção de não fornecer os dados para ter acesso ao serviço ou produto, e as práticas nocivas aos interesses do titular são compartilhadas pelos concorrentes (uma simples pesquisa comparando Termos de Uso e Políticas de Privacidade de aplicativos médicos por exemplo, para agendamento de consultas entre outros serviços demonstra a similaridade dos documentos). Ademais, pesquisas demonstram que raramente as pessoas leem esses documentos antes de contratar um serviço, e que quando os leem somente uma parcela inferior de fato compreende o que está escrito e como os seus dados serão tratados. Vide resultados de *survey* realizado pelo *OAIC – Office of the Australian Information Commissioner* (autoridade Australiana de privacidade) em 2020, que demonstra que, em que pese os australianos confiem mais em um site ou serviço quando leem a política de privacidade, somente 20% dos respondentes leem esse documento e possuem a convicção de que de fato o entenderam. 87% gostariam de políticas de privacidade com linguagem mais simples e acessível, 86% entendem que um sumário para fácil acesso de tópicos específicos seria útil e desejável, e 73% acreditam que o uso de ícones e de comunicação mais visual ajudaria no entendimento. Pesquisa disponível em: https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey#:~:text=Australians%20are%20more%20likely%20to%20trust%20a%20website%20or%20service,are%20confident%20they%20understand%20them.. Acesso em 05 Jan. 2023. No mesmo sentido, relatório de pesquisa conduzida pelo *Pew Research Center* nos Estados Unidos em 2019 demonstrou que 74% dos estadunidenses não leem ou raramente leem as políticas de privacidade e termos de uso. Pesquisa disponível em: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf. Acesso em 05 Jan. 2023. Pesquisa conduzida em 2021 pela NordVPN verificou que apenas 38,7% dos brasileiros respondentes tem o hábito de ler Termos de Uso e Políticas de Privacidade. Disponível em: https://canaltech.com.br/seguranca/brasileiros-se-preocupam-com-seguranca-mas-nao-leem-termos-de-uso-diz-pesquisa-183554/. Acesso em 05 Jan. 2023.

[44] Muitos documentos utilizam termos excessivamente abertos que não permitem ao titular de dados se informar sobre o que de fato será feito com seus dados, por exemplo: "seus dados serão compartilhados com terceiros confiáveis", "o propósito da coleta dos seus dados é melhorar a sua experiência de usuário", entre outras formas de falsear uma conformidade com a lei, sem informar o titular de dados.

[45] Pesquisa britânica de 2020 conduzida pela empresa *Thinkmoney* constatou que para a efetiva leitura dos Termos de uso e Políticas de Privacidade dos aplicativos mais populares do Reino Unido, um usuário precisaria empenhar algo em torno de 17 horas e 5 minutos. Isso demonstra que a transparência e a prestação de contas por parte de agentes de tratamento também passam pela inteligibilidade da linguagem empregada nos documentos. Na Sociedade Informacional nos habituamos ao imediatismo, de maneira que apostar em técnicas diferentes para a comunicação, como uso de vídeos ou áudios pode ser benéfico para a efetiva comunicação com o usuário, titular de dados. Disponível em: https://www.thinkmoney.co.uk/blog/what-phones-know-about-you/. Acesso em 10 Jan. 2021.

Com base nessas explicações sobre problemas atinentes à limitação de escolhas e à autodeterminação no contexto digital, torna-se evidente que as plataformas e as novas tecnologias, celebradas como importantes ferramentas para a viabilização da transparência, da democratização da informação e da integração do mundo, podem ter efeito reverso. Esse potencial de dano é oriundo da divisão da aprendizagem (ZUBOFF, 2019), ou seja, da dominação e manipulação comportamental com base no monopólio do conhecimento sobre o funcionamento desse universo digital que invade o material. A transformação em mercadoria sob o capitalismo de plataforma sinaliza para um futuro social no qual o poder das plataformas é protegido por fossos de sigilo, ofuscação e expertise (ZUBOFF, 2019; VÉLIZ, 2021). Mesmo quando o conhecimento derivado do comportamento dos sujeitos os é retroalimentado, "melhorando sua experiência de usuário", como no caso da chamada "personalização", operações secretas paralelas buscam a conversão do superávit em modulação de comportamentos futuros em algum sentido (seja para o consumo de um produto ou para a adesão a uma ideia), operações essas que vão muito além dos reais e conscientes interesses dos titulares de dados (ZUBOFF, 2019).

Por todos os componentes e derivados apresentados, é forçoso reconhecer que não existe controle efetivo sobre os dados e tampouco sobre o *output* gerado ao interagir com plataformas, seus componentes e derivados. Assim, os titulares de dados são alijados do seu corpo digital e consequentemente neutralizados no seu potencial de autoconstrução ou autodeterminação no contexto da sociedade informacional. Como destacado por Shoshana Zuboff (2019, p. 132-133), os seres são exilados do próprio comportamento, sendo-lhes negado o acesso ao conhecimento – ou o controle dele – resultante da despossessão dos seus dados por parte de outros e para outros. Conhecimento, autoridade e poder permanecem com o capital de plataforma, para o qual os sujeitos não passam de "recursos naturais humanos". Esse *ciclo da despossessão*, explicado por Shoshana Zuboff (2019, p. 137-154) é estruturado pelos seguintes estágios: incursão, habituação, adaptação e redirecionamento. Zuboff esclarece que os estágios citados foram verificados nas operações do Google, Facebook (hoje Meta) e muitas outras plataformas, se repetindo como estratégia inerente ao capitalismo de vigilância e de plataforma para a extração de superávit comportamental.

O primeiro estágio da despossessão é a incursão unilateral, operada em espaços desprotegidos (computadores pessoais, páginas da internet, postagens em redes sociais, atividades monitoradas por *smart objects,* entre outros). A incursão ocorre quando operações de despossessão se baseiam nas aptidões de sequestrar superávit comportamental de espaços da vida cotidiana não pertencentes ao mercado (ZUBOFF, 2019, p. 140). Esse sequestro é operado

pela sedução com ofertas de conveniências ou facilidades nos serviços, e com base em ignorar as eventuais oposições iniciais. Esse estágio se desenrola até que resistências mais robustas passem a ocorrer (por exemplo com a regulação do setor, aqui entendida como a criação e aplicabilidade de normas legais a respeito da atividade).

Ante oposições que resultem em investigações e interpelações judiciais, as organizações que se valem da vigilância passam ao segundo estágio do ciclo: a habituação (ZUBOFF, 2019, p. 144). Consistente em explorar e fomentar a dependência dos usuários em relação aos produtos e serviços que estão sob alvo da oposição, com a utilização da repetição de discursos sobre a irreversibilidade do *modus operandi* na sociedade informacional. As práticas contestadas passam a ser naturalizadas e incorporadas à rotina das pessoas, e a intrusão na sua vida privada é mostrada sob o véu da inevitabilidade, como se a conveniência fornecida tivesse que vir atrelada com a violação à intimidade e à privacidade. E como se num mundo conectado em rede não houvesse mais que se falar em privacidade.

Num terceiro momento, sendo a resistência apresentada persistente, o agente de tratamento passa ao estágio da adaptação (ZUBOFF, 2019, p. 147). São promovidas modificações superficiais (e inevitáveis) para simular uma conformidade com as exigências imediatas apresentadas sobre as práticas questionadas. É o caso dos Termos de Uso e Políticas de Privacidade evasivos ou indecifráveis, dos *banners* de *cookies* advertindo que sem a aceitação de todos os *cookies* a página não operará como esperado, entre outras práticas comuns em face da emergência de normas de proteção de dados.

O último estágio consiste no redirecionamento (ZUBOFF, 2019, p. 148), ou seja, na reorganização das operações apenas o suficiente para demonstrar aderência às exigências, sem modificações substanciais do *modus operandi*. Acontece pelo emprego de retórica, de propaganda e de novos produtos para apaziguar as oposições enfrentadas e aparentar adequações. A despossessão se vale da dinamicidade da tecnologia e da divisão do aprendizado e do conhecimento para neutralizar a regulação, sempre colocando as plataformas num passo adiante dos agentes reguladores, operando em campos ainda não identificados pelos sistemas legais como riscos. A habituação juntamente com o senso de urgência pela tecnologia e com a noção de que se privar das facilidades obtidas em contrapartida da despossessão seja uma perda de oportunidade, criam uma percepção de que não se render equivale a não pertencer, a não existir na sociedade informacional. Todas essas estratégias de modulação comportamental fomentam a docilização em face da perda de autonomia.

O ciclo se lastreia na abissal assimetria de poder existente entre usuários e plataformas, agentes de tratamento de dados. O enorme desconhecimento dos usuários sobre o

funcionamento das plataformas, dos vestíveis e demais tecnologias com as quais convivem, somado à sedução da comodidade da personalização de serviços é uma vantagem competitiva para os agentes de tratamento e um fator de aumento da vulnerabilidade dessas pessoas naturais, de quem o superávit comportamental[46] é extraído. Vale mencionar que essa mesma disparidade quanto ao efetivo conhecimento sobre linguagem de programação e sobre o funcionamento das tecnologias é um dificultador da atividade de regulação e do seu *enforcement* (que envolvem a necessidade de fiscalização da conformidade) por parte de autoridades competentes pelo controle da política pública de proteção de dados pessoais. Importante destacar, ainda, que essas mesmas autoridades muitas vezes também figuram como agentes de tratamento, devendo se submeter às exigências previstas nas normas de proteção de dados.

Em face das estratégias de vigilância abordadas pelo uso dos componentes e derivados das plataformas digitais, assim como tendo em vista o reconhecimento da ampliação da vulnerabilidade e dependência de uma situação de autorregulação das plataformas que atuam como agentes de tratamento de dados pessoais, é que ganha impulso a tendência de normatização dos tratamentos desse tipo de informação relativa a pessoas naturais. Mesmo com todas as dificuldades no que concerne à fiscalização e o *enforcement* (*nudge*[47] positivo, com a conscientização e estímulo à conformidade, e *nudge* negativo, com a efetiva punição de violações para efetiva aplicação da norma) da proteção de dados, ou seja, da tutela dos dados pessoais em movimento, a regulação inicial é vista como um passo no caminho do amadurecimento dessa proteção para que progressivamente se aproxime da efetiva salvaguarda dos direitos da personalidade.

Enxergar a validade da regulação da proteção de dados foi um passo de amadurecimento da pesquisa em registro, sendo que inicialmente a hipótese testada era no sentido de que as normas de privacidade e proteção de dados se prestavam pura e simplesmente a simular segurança para anestesiar os titulares de dados pessoais. Ante às reflexões realizadas ao longo

---

[46] A esse respeito, pesquisas comprovam que o conhecimento acerca da própria vulnerabilidade diminui drasticamente a efetividade dos *hyper-nudges*, dos *feedbacks* que intencionalmente visam modular comportamentos: "[...]when people have knowledge regarding their own vulnerabilities, the efficacy of persuasive attempts diminish. Developing such a critical and aware approach to persuasion – "persuasion knowledge" (Friestad &Wright, 1994) – is indeed fundamental for citizens of information societies. Yet, it might not be sufficient to resist undesirable consequences of personalization and, ultimately, to fully benefit from its potential." (REVIGLIO, AGOSTI, 2020, p. 5).

[47] Conceituado como a intervenção comportamental para incentivar determinadas escolhas. Consiste em gênero que engloba diferentes tipos de intervenção comportamental que incentivem uma escolha (tida como desejável), sem haver a proibição da adoção da alternativa existente (RIDDER, KROESE, VAN GESTEL, 2022). Trata-se de conceito cunhado na economia comportamental, para se referir ao uso de técnicas de persuasão, lastreadas na psicologia, para a modulação comportamental. Tanto do ponto de vista ético quanto do ponto de vista dos direitos da personalidade existe a problematização da legitimidade da utilização dessas intervenções.

de toda a trajetória de pesquisa, passou-se a reconhecer que a regulação, ainda que com déficits de efetividade, em que pese não resolver os problemas sobre os quais se debruça, tem o condão de empoderar as partes mais vulneráveis, no caso em estudo, os titulares, por fornecer a eles a possibilidade de autotutela do seu direito e por municiá-las com uma causa para ação. Ainda que essa normatização represente uma aderência a interesses gestados em organizações internacionais, muitas vezes coadunando com o interesse das plataformas, traduzindo-se numa transformação "controlada", a possibilidade de judicialização tem o potencial de progressivamente mudar a cultura e conscientizar para um futuro engajamento genuíno com o direito assegurado na lei (seja pela judicialização ou pela atuação de controle por parte de órgãos responsáveis pelo reforço da política pública). Assim ocorreu no Brasil com os direitos do consumidor, com a obrigatoriedade do uso de cinto de segurança, entre outros casos cujo amadurecimento da tutela ocorreu com o tempo.

Os dados, especialmente os pessoais, que contém informações com potencial de identificar uma pessoa natural, falam mais sobre esses sujeitos do que eles têm consciência, e fornecem subsídios para uma leitura absolutamente detalhada dos seus anseios e tendências mais íntimos. Essa leitura resulta na elaboração de perfis que torna os sujeitos vulneráveis a influências na formação da sua vontade e impulsionados a agir com base nos *feedbacks* recebidos na interação com as plataformas, seus componentes e derivados. Esse processo de despossessão e de utilização dos dados de pessoas naturais como ativos passa a ser mais explorado nos anos 2000 (ZUBOFF, 2019), inicialmente em âmbito estritamente digital, para depois avançar para o mundo "material", analógico, com a disseminação de novos hábitos de consumo relativos aos *smart objects* vestíveis ou não, utilizados de forma corriqueira.

A sociedade informacional é marcada por sua economia pautada na datificação, ou seja, na exploração do superávit comportamental para predição e criação de mercados futuros. A renderização dos dados, sobretudo dos dados pessoais, passa a predominar, inaugurando o que Shoshana Zuboff (2019) aborda como um mundo de diferenças pautadas numa nova divisão da aprendizagem, como fonte de poder e da manutenção da dominação. Essa divisão da aprendizagem se dá com a digitalização da vida e com a ruptura das barreiras antes existentes entre o mundo "material" e o mundo "digital". E se opera com base no ciclo de despossessão abordado.

Conforme enfatizado, muitas vezes o fornecimento de dados se dá voluntariamente, por iniciativa própria (tome-se por exemplo a cultura da exposição e a proliferação da figura do

influenciador digital[48]), ou por imposição de alguma política pautada na racionalidade falaciosa[49] de que a automatização do Estado é o caminho para a eficiência e para a neutralidade e impessoalidade nas decisões administrativas, a exemplo do que ocorre com a instituição da identidade digital na Índia pelo Projeto Aadhaar, em que a identidade digital, que contempla ampla coleta de dados pessoais, incluindo dados biométricos – digitais e mapeamento da íris – passou a ser exigida para a inclusão em programas assistenciais. O mesmo se aplica ao Brasil, que tem automatizado o acesso a serviços públicos, através da plataforma *gov.br,* que utiliza o número do Cadastro de Pessoa Física (CPF) como chave de entrada para diversos sistemas do governo[50]. Na plataforma *gov.br* alguns serviços dependem do status da conta do usuário que pode ser "bronze", "prata" ou "ouro". Quanto mais dados forem fornecidos e quanto mais autorizações para o compartilhamento de dados de diferentes bases (Receita Federal, banco em que é correntista etc.) para a "segurança" quanto a veracidade da identidade, e para a garantia da "qualidade dos dados", mais a conta tenderá a ser ouro. Alguns serviços são inacessíveis se a conta não for ouro, por exemplo o registro de uma microempresa individual (MEI). A Austrália também tem automatizado o acesso a serviços públicos, centralizados a partir de conexões de bancos de dados de diversas autoridades à plataforma *Mygov*[51].

A questão central para a proteção de dados que seja vocacionada a proteger o titular é não somente atinente à coleta e armazenamento, mas muito pertinente com a finalidade do

---

[48] A plataforma Educa+Brasil publicou reportagem acerca de pesquisa realizada pela consultoria Nielsen em 2022, que constatou que o Brasil é o segundo país no mundo com mais pessoas se tornando influenciadores digitais (ficando apenas atrás dos Estados Unidos). Segundo essa pesquisa, estia-se que, apenas no Instagram, o Brasil conte com 10,5 milhões de influenciadores, número oito vezes maior do que o número de advogados e quase vinte vezes maior do que o número de médicos brasileiros. Para maiores informações ver a reportagem, disponível em https://www.educamaisbrasil.com.br/educacao/noticias/brasil-ja-tem-mais-influenciadores-digitais-do-que-advogados-e-medicos. Acesso em 19 Abr. 2023.

[49] Diversas pesquisa têm comprovado a crescente inserção de novas tecnologias de suporte a decisões administrativas e mesmo para a automatização da decisão. Conforme explicitado no artigo "*Gender data in the automated administrative state*", de Ari Ezra Waldman (2023), existem camadas de discricionariedade que são exercidas desde a concepção da lei que autoriza a automatização, até a efetiva implementação da ferramenta tecnológica que tendem a resultar na reprodução de preconceitos e exclusões predominantes na cultura vigente, resultando em ferramentas que excluem populações marginalizadas, ao passo que na programação a busca pela eficiência toma a suposta maioria como padrão, e quem desvia do padrão como ruído do sistema, sujeito à prejuízos e incremento da marginalização. Como o autor frisa, esses "ruídos" são pessoas que tem sua dignidade vilipendiada e a sua identidade negada, apagada. A origem do problema da automatização não é a tecnologia em si, mas o m*indset* por trás da alimentação da base de dados e do parâmetro aplicado na programação. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4358437. Acesso em 10 Abr. 2023.

[50] Vide reportagem recente que lida com dados fornecidos pelo governo federal e afirma que 90% dos serviços no Brasil são digitais. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2023/04/14/cpf-e-chave-para-acessar-diversos-servicos-do-governo-veja-como-funcionam.htm. Acesso em 24 Mai. 2023.

[51] Vide: https://login.my.gov.au/las/mygov-login?execution=e1s1. Acesso em 10 Nov. 2023. A *Mygov* centraliza todo o acesso aos serviços públicos relativos: fiscais (conectando a conta do *Australian Taxation Officer – ATO* à plataforma), de saúde (*Medicare*), entre outros. Da mesma maneira que ocorre no Brasil, quanto amis dados forem fornecidos e documentos emitidos por autoridades australianas que confirmem a identidade do titular da conta, maior amplitude de medidas podem ser acessadas pela plataforma.

tratamento desses dados (para que e como esses dados serão usados). Especialmente quando os dados são armazenados em meio digital a possibilidade de desvio de finalidade no tratamento e a vulnerabilidade que a agregação dessas informações representa são questões a serem pensadas seriamente[52].

Se de um lado a informatização e digitalização da vida representam uma facilidade, uma ampliação de poder pessoal, ao passo que todos passam a ter voz, a serem produtores de conteúdo e influenciadores em potencial, por outro, enreda os sujeitos numa trama de vigilância e vulnerabilidade crescente e sem precedentes. Na contemporaneidade a exposição aos riscos inerentes à essa interação é irresistível, ao passo que as atividades mais corriqueiras são atravessadas pelo fornecimento de dados e pela automatização, pela intermediação de plataformas. Como mencionado por Zygmunt Bauman, em entrevista no documentário "*Everything's under control"* (2015), na sociedade informacional a postagem acontece para que a existência e o pertencimento se concretizem, e assim muitos dados são entregues de maneira voluntária para as plataformas. Os seus criadores e operadores exploram inferências de traços psicológicos para tornar os usuários mais vulneráveis e modular seus comportamentos.

A extração de dados se dá ainda pela imposição de rotinas com a inexistência de alternativas: transações bancárias, cumprimento de obrigações legais como a de declarar imposto de renda, a oferta e os processos seletivos para emprego, o acesso a vagas em universidades (pelo Sistema de Seleção Unificada – SISU), a contratação de serviços, o acesso a serviços públicos, a compra de passagens, o embarque e desembarque em aeroportos e rodoviárias, todas as atividades mencionadas são intermediadas por plataformas digitais. A transformação digital é uma realidade que empurra todos para a digitalização da vida. Nesse contexto, o mundo foi convertido em um grande banco de dados, em um imenso sistema de informação. Se por um lado esse fluxo contínuo e crescente de dados representa progresso e poder, por outro, também apresenta um potencial nocivo que pode passar despercebido para a maioria das pessoas. A nocividade se dá pela violação à própria dignidade da pessoa humana,

[52] Em sociedades que entendem a disparidade de poder entre os indivíduos e as organizações / pessoas que possuem o conhecimento de manejar dados pessoais, o temor quanto a postagens e manifestações usando redes sociais e outras plataformas digitais prevalece. Um exemplo é a forma de protesto e de manifestação de indignação que tem ocorrido em Hong Kong, contra o domínio da China: a *Lennon Wall.* Os manifestantes deixam suas opiniões e clamores registrados em *post-its* nas paredes de espaços públicos, por temor de serem identificados e sofrerem retaliações por isso. A contrário senso, a sensação predominante na sociedade brasileira na contemporaneidade é a de que as redes sociais e a internet são terra de ninguém, e espaço público em que a "livre manifestação" de opinião tem ultrapassado a linha tênue para desembocar numa efetiva apologia à violência, como ocorreu recentemente durante o período de eleições presidenciais, nas ações de 08 de janeiro de 2023 (através das postagens de vídeos e fotos feitas pelos próprios manifestantes, foi possível a identificação de envolvidos nos atos de vandalismo ocorridos nas dependências de sedes de órgãos federais).

pela anulação de qualquer resquício de autonomia e de possibilidade de autoconstrução e autorrepresentação de quem se é[53], de maneira irreversível com a capacidade de armazenamento e de processamento existente desde o *big data*.

O fornecimento de dados decorre, ainda que de maneira involuntária, pela simples interação com plataformas, e pelo simples uso de algum dispositivo "inteligente" (ao usar o *smartphone,* que tem censor de localização, de proximidade com outros dispositivos *smart* e de aceleração são produzidas informações sobre locais visitados, jeito de andar, eventuais companhias ou proximidade de outros dispositivos; usando *smartwatch* informações referentes à saúde e hábitos de vida, horários de despertar e de dormir, quando e se faz exercícios físicos, que tipo de exercício , presença de hipertensão ou hipotensão, incidência de ronco, entre outras). Vale destacar que esses dados fornecem subsídios quanto ao estado emocional dos indivíduos, sobre a sua história de vida e suas tendências, tornando-os vulneráveis e traçando uma leitura dos sentimentos manifestados, bem como eles viabilizam determinadas formas de interação e buscas específicas. Assim, os indivíduos rendidos, "mapeados", tornam-se mais facilmente manipuláveis, de modo silencioso, a partir de estímulos e *feedbacks* com potencial para modular o comportamento.

Sob a égide da sociedade informacional e da vigilância, no âmbito de uma economia em rede, o fenômeno da monetização de dados é a regra. Ela constitui o serviço ou produto, da mesma maneira que os dados gerados também constituem meios de criação de novos bens e serviços. Os seres são a todo momento, com base nos dados extraídos, alvos de decisões automatizadas de classificação, fundadas no corpo digital. E é esse corpo digital que os define, que fala por eles na sociedade informacional, que diz quem são antes que possam se manifestar conscientemente. Nesse contexto, a relação entre usuários e plataformas, se estabelece com base em uma assimetria de poder. Esse desequilíbrio é pautado tanto em questões técnicas, quanto em questões culturais e mesmo comportamentais. A assimetria de poder é agravada por componentes e derivados como o *big data*, que possibilita a agregação de grande monta informacional para os agentes de tratamento, vulnerando ainda mais os titulares de dados. Os

[53] Os documentários referenciados nessa tese destacam como a vigilância e a personalização impactam nos processos de formação de vontade e no comportamento dos indivíduos. Em "*Everything's under control*" (2015), Werner Boote apresenta um panorama do quanto perdemos privacidade al longo dos anos e o quanto isso viola nossos direitos da personalidade de maneira sutil, demonstrando que o mundo é orientado por dados e as economias baseadas na contemporaneidade na sua exploração. Em "*Privacidade Hackeada*" (2019) pode-se perceber o quanto esses dados podem ser usados para modulação comportamental, inclusive a ponto de direcionar eleições, colocando em risco a própria democracia. Em "*O dilema das redes*" (2020) podemos entender o quanto os algoritmos são programados para o engajamento, tendo como centro a manutenção do usuário em constante interação com as redes sociais, não importando o efeito disso para seu bem-estar (inclusive com a utilização de conteúdos que venham a engajar pelo ódio e pela disseminação de desinformação).

demais componentes e derivados das plataformas definidos nesta seção contribuem para o incremento dessa assimetria, como a IA, perfilamento, a internet das Coisas (*internet of things – IoT*), os *filtros bolha*, as câmaras de eco, o emprego de *dark patterns* (padrões obscuros), entre outros. O cenário narrado tende a se tornar ainda mais complexo, quando se tem em consideração a evolução tecnológica, o crescente uso de IA generativa de conteúdo de imagem e texto, cujos *outputs* são de difícil detecção, assim como pela possibilidade de uma integração ainda mais profunda entre o digital e o material, caso sistemas de imersão como o Metaverso[54] sejam concretizados e ganhem escalabilidade.

Na próxima seção abordam-se os efeitos da sociedade informacional para a soberania, para a regulação e para a instituição de políticas públicas para privacidade na era do capitalismo de plataforma e da sociedade informacional.

2.4 Fluxos transnacionais de dados e a mitigação da soberania na regulação

Esta seção argumenta que a porosidade das fronteiras comunicacionais e a intermediação das mais variadas relações humanas por plataformas reflete uma modificação na dinâmica do poder econômico e político. As grandes empresas agora exercem poder em maior paridade com os Estados nacionais, influenciando no exercício da soberania legislativa através do *lobby* em organizações internacionais. A configuração de exercício de uma soberania mitigada é justificada pela necessidade de convergência regulatória para lidar com problemas transnacionais. Essa nova dinâmica de poder caminha para o que Anne-Marie Slaughter (2004) denomina de uma nova ordem mundial, em que os Estados nacionais e as organizações privadas interagiriam abertamente em redes. Nessa teia de interações e de exercício de poder, os Estados nacionais passariam a exercer uma soberania desagregada[55] (SLAUGHTER, 2004, p. 266-271),

[54] O Metaverso, em que tantas empresas estão investindo para a viabilização do que seria uma evolução da internet, por tratar-se de ambiente em nuvem mais integrado e interativo representa um alto risco para a proteção de dados pessoais (VALADARES, 2022). O Metaverso não possui conceito jurídico, mas as pesquisas para a sua concepção e concretização já apontam elementos que o caracterizarão. Todas as interações nessa realidade paralela são registradas nos mínimos detalhes, gostos, preferências e sentimentos dos sujeitos, inclusive, de forma que o debate acerca da formação de subjetividades digitais se torna mais acirrado. Trata-se de sistema bastante sofisticado de imersão, interatividade e colaboração, em que poderemos executar quase todas as atividades intersubjetivas de forma remota, através de avatares. O panorama que o Metaverso anuncia torna flagrante o desafio de se controlar o tratamento de dados pessoais, sobretudo a sua utilização para mapear e manipular predileções e predisposições.

[55] "[...] The new model advanced here assumes disaggregated states in which national government officials interact intensively with one another and adopt codes of best practices and agree on coordinated solutions to common problems—agreements that have no legal force but that can be directly implemented by the officials who negotiated them. At the same time, in this new model, states still acting as unitary actors will realize that some problems cannot be effectively addressed without delegating actual sovereign power to a limited number of supranational government officials, such as judges and arbitrators in the WTO, NAFTA, and the ICC. In such

exercida por organismos internos para assuntos específicos, em um ambiente de governança e políticas públicas globais[56] para endereçar problemas supranacionais. Em sentido similar, Luciano Floridi (2020, p. 375-377) propõe a reconfiguração do exercício da soberania como poder não rival, dentro de uma rede conectada de agentes, de maneira que facetas de soberania sejam exercidas transnacionalmente, nacionalmente ou regionalmente (por exemplo, soberania monetária, soberania tributária, soberania digital, soberania regulatória etc.). Essa reconfiguração em rede para exercício de controle soberano seria legitimada de maneira hierárquica e distribuída em nós de conexão da rede (FLORIDI, 2020, p. 377).

O Direito, enquanto mecanismo de modulação comportamental, promove a ideia de segurança jurídica, de extrema relevância para a manutenção da vida em sociedade sob a égide do Estado de Direito (MELLO, 2019). Os sistemas jurídicos são construídos com normas pautadas no intuito de contingenciamento de riscos avaliados como críticos para a sustentabilidade da vida em comum, caso se concretizem corriqueiramente. Assim, a identificação dos riscos se traduz em tutela pelo direito a determinados bens jurídicos tidos como fundamentais para que o sistema siga funcionando como processo de adaptação social, contribuindo para a modulação comportamental que possibilite a convivência intersubjetiva (MELLO, 2019, p. 51). E enquanto instrumento de modulação comportamental, o direito também opera com base em dominação, no sentido de buscar anular ou ocluir a diferença que cria ruídos.

Entretanto, a existência de norma, por si só, não tem o condão de modificar a realidade fática, caso não existam mecanismos para a sua concretização. A partir do suporte normativo, os Estados nacionais atuam na concretização das tutelas previstas na norma ao instituir políticas públicas, como ações coordenadas em escala ampla para atuar sobre problemas complexos (BUCCI, 2019). Assim, sempre que se fala na atuação estatal para fomento de determinado comportamento e para a resolução de problemas complexos que impactam a vida em sociedade se está diante de temas afetos às políticas públicas.

No mundo globalizado a soberania, antes concebida como um poder sólido, passa por progressivas transformações, resultando no que Gabriel Méndez Hincapíe e Ricardo Sanín-

cases, the international agreements negotiated will be more immediately and automatically effective than the majority of agreements negotiated in the old system because they will be directly enforced through vertical government networks." (SLAUGHTER, 2004, p. 263).

[56] Com a proposta de conter a da ameaça de direitos fundamentais ante os fenômenos decorrentes da sociedade informacional, interessante a proposta formulada na tese "CASTELOS ALGORÍTMICOS DE PODER: enclausuramento tecnofeudal dos direitos humanos / fundamentais?", de autoria de Meire Aparecida Furbino Marques. A tese defendida na PUC Minas em 2022 propõe uma Declaração de Direitos Humanos Global aplicável no ciberespaço.

Restrepo (2012, p. 100) designam de soberania porosa. Essa nova manifestação da soberania consiste, para os autores, na transformação da soberania a favor dos métodos que acompanham a expansão do império do capital, como reflexo da manutenção do domínio:

> [...] Em geral, se trata de novas políticas de segurança que determinam usos e âmbitos inéditos de aplicação da força em direta consonância com a defesa dos interesses de empresas multinacionais que favorecem a dependência total de qualquer forma de vida ao mercado global. [...] (HINCAPÍE, SANÍN-RESTREPO, 2012, p. 100).

Na sociedade informacional, a "comoditização" da informação acontece como efeito da modificação do capitalismo, que passa a trabalhar com a espoliação da experiência humana para gerar a certeza de mercados futuros, a partir da mineração de dados e do perfilamento, na leitura profunda e detalhada do comportamento humano para fins de, a partir dos perfis traçados, predizer intenções e tendências. É a partir dessa constatação que Shoshana Zuboff (2019, p. 18-20) constrói a sua visão de Capitalismo de Vigilância, e dispõe o quanto essa modalidade de capitalismo gera uma nova espécie de poder, a que a autora denomina de "instrumentarismo" (poder instrumentário), por utilizar o conhecimento extraído dos dados pessoais para modular o comportamento das pessoas em interação com plataformas.

Esse poder instrumentário atua de maneira sutil e é imperceptível para a maioria das pessoas que tem os seus processos de tomada de decisão moldados a partir de estímulos e *feedbacks*, de propagandas assertivas e de exposição a determinados conteúdos, sempre em prol do interesse de terceiros, com finalidades que vão muito além do "mero" estímulo ao consumo de determinados bens e serviços[57]. É importante reforçar que a política de distanciamento social, adotada com a finalidade de contingenciar o avanço da pandemia da COVID-19, acelerou os riscos inerentes à interação com plataformas e aumentou o poder de empresas que já contavam com serviços de intermediação dessa interação remota. Isso porque a rotina profissional e acadêmica da maioria das pessoas passou a ser necessariamente intermediada por essas tecnologias. Essa foi uma opção viável e necessária, mas que acabou por acirrar as

[57] Vale lembrar do escândalo da *Cambridge Analytica*, que foi retratado no documentário "Privacidade Hackeada" (2019), que denunciou como o *Facebook*, hoje denominado *Meta*, utilizou o perfilamento e o tratamento de dados pessoais para influenciar eleições ao redor do mundo, expondo eleitores indecisos a conteúdos minuciosamente escolhidos para estimular um determinado comportamento, desejado por quem contratava a rede social para essa finalidade. O conhecimento dos fatos chegou a ser alvo de investigações pelo *Office of Australian Information Commissioner – OAIC*, autoridade de privacidade australiana, ao passo que dados de australianos foram coletados e utilizados com desvio de finalidade, violando os *Australian Privacy Principles – APP*, resultando em interferência na privacidade dos titulares desses dados. Até o presente momento o Facebook segue aplicando a tática de protelação do feito judicial, tentando evitar a submissão à jurisdição australiana, em flagrante exemplo dos desafios para a realização do reforço de políticas públicas para a promoção de direitos afetados pelo avanço tecnológico, como a privacidade e a proteção de dados. O caso será analisado com maior vagar no capítulo dedicado à análise da política pública de privacidade australiana (ver decisões: *Australian Information Commission v Facebook Inc* [2020] FCA 531; *Australian Information Commissioner v Facebook Inc* [2020] FCA 1307; *Facebook Inc v Australian Information Commissioner* [2022] FCAFC 9).

disparidades de poder e a exclusão de uma enorme gama de pessoas (em especial no Brasil, país que ainda apresenta elevado grau de exclusão digital[58]).

A crescente interação com plataformas e a digitalização da vida culminou no avanço da criminalidade digital e na proliferação de incidentes de segurança da informação. De outro lado, o uso da tecnologia de rastreamento e o compartilhamento de dados pessoais por empresas ao redor do mundo com os Estados, para fins de mapear o alastramento da contaminação, também reacendeu o debate sobre a necessidade de promover a proteção de dados e para a urgência de imposição de limites no processamento de informações que caracterizem dados pessoais. A pandemia evidenciou os riscos inerentes ao tratamento de dados pessoais, independentemente do meio em que eles aconteçam.

Ante a constatação dos riscos inerentes ao tratamento de dados pessoais de maneira indiscriminada, inicia-se movimento internacional em organismos como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e a União Europeia (UE), em prol do disciplinamento do processamento de dados pessoais, que é progressivamente incorporado aos sistemas jurídicos nacionais, de forma mais intensa nos últimos anos, como marca do fenômeno das soberanias porosas (HINCAPÍE, SANIN-RESTREPO, 2012). E a crescente defesa da necessidade de uma convergência regulatória para que haja efetividade das normas estabelecidas em relação às plataformas, seus componentes e derivados, desencadeou um processo de maturação de normas nacionais bastante inspiradas em *soft laws* gestadas no âmbito de organismos internacionais.

A soberania no contexto da sociedade informacional deixa de expressar o exercício de um poder sólido sobre dado território, sendo reduzida a um poder cada vez mais paritário ao dos particulares, fazendo com que o Estado nacional apresente a tendência de ser mais um negociador de interesses do que um ente soberano no que diz respeito à instituição de normas num sistema jurídico. Sabino Cassese (2012, p. 605-606) esclarece tendências do direito público à luz das transformações promovidas pela globalização, apontando essa tendência de diminuição do poder do Estado nacional e de transformação da soberania (com considerável declínio do seu exercício enquanto poder independente). Cassese[59] (2012) destaca que o mais

[58] Em razão da pré-existente exclusão social, a pandemia acabou por estabelecer uma disparidade abissal, inclusive no que tange o acesso à educação, já que muitas crianças e adolescentes ficaram totalmente alijados do acesso às aulas *on-line*, tanto por não disporem de dispositivos para acesso à Internet, quanto, para as que possuem celular ou outro dispositivo, por uma conexão precária (falta de acesso à conexão de banda larga).

[59] "*These are not only arenas in which contending forces operate, but also sets of organizations claiming control not over territories and people, but over functions."* (CASSESE, 2012, p. 605). Conforme o autor, existe uma sobreposição de exercício de poder, com os Estados Nacionais concorrendo com organizações internacionais pelo exercício de determinadas funções, tipicamente concebidas como de natureza estatal. Como consequência, o

importante reflexo do contexto global é a inexistência de uma delimitação clara quanto ao espaço e à política, com o crescimento de um espaço global (ao que se prefere a interpretação como um espaço transnacional, à medida que existem nações excluídas desse processo de múltipla e recíproca influência) e de uma política global (quanto ao termo vale a mesma ressalva, quanto a efetiva constatação de uma política transnacional).

Nesse sentido, existe uma desnacionalização do direito e da função regulatória, com uma progressiva sobreposição de exercício de poder e da incapacidade de controle pelo Estado nacional, a um só tempo regulador e regulado em muitas searas, como é o caso da proteção de dados. A transnacionalização marca, ainda, a existência de uma zona cinzenta entre as definições de público e privado, de maneira que o poder é exercido de forma bastante incidente por organizações híbridas ou privadas. Todo esse cenário conduz para uma dependência dos Estados da colaboração com a sociedade civil e com o mercado para a condução e efetividade das políticas públicas pertinentes a demandas oriundas das novas tecnologias.

O contexto de modificação na concepção e na expressão da soberania se deve também em grande parte pela maneira com que, nesse contexto global, a "nova economia", orientada por dados, repleta de bens não-rivais e dependente da fidelização do consumidor, da conformidade com *standards* instituídos internacionalmente e da criação de mercados futuros se estrutura em um contexto internacional. Conforme Cíntia Rosa Pereira de Lima (2020, p. 43), entre as características dessa "nova economia",

> [...] pode-se dizer que é *informacional*, porque a produtividade e competitividade dependem da capacidade de gerar, processar e aplicar de maneira eficiente as informações baseadas no conhecimento científico e tecnológico. É *global* porque a produção, a distribuição e o consumo são organizados em nível global e com a interligação entre vários agentes da economia. É *interconectada* ("*networked"*, na expressão de Manuel Castells) porque as novas condições socioeconômicas impõem a interconexão em redes entre as empresas. Quanto mais sólida for tal *network*, mais competitiva a produção desses agentes econômicos será.

Trata-se de resultado da Quarta Revolução Industrial[60], que com os avanços tecnológicos permite uma expansão de mercados, de maneira que, sendo os dados subsídios

---

fenômeno da desnacionalização do direito acaba por incidir e por refletir-se na incorporação crescente de diretrizes advindas desses organismos internacionais.

[60] Cíntia Rosa Pereira de Lima (2020, p. 43) esclarece que os economistas destacavam três períodos de revoluções que marcaram a produção na história. A Primeira Revolução Industrial seria originada na utilização da máquina a vapor como força motriz para otimizar a produção ao final do Século XVIII, até as últimas décadas do Século XIX. A Segunda Revolução Industrial, gerada pela substituição do vapor por motores movidos à combustão e elétricos no final do Século XIX até o fim da 2ª Guerra Mundial no Século XX. A Terceira Revolução Industrial seria fruto da utilização de energia nuclear. Entretanto, em meados de 1980, com o desenvolvimento da Tecnologia da Informação, e a crescente presença da ciência computacional na produção, contataram uma Quarta Revolução Industrial. No mesmo sentido, o professor Nívio Ziviani, em palestra (UFMG Talks – 2019 – disponível o Youtube) destaca que a importância dessa revolução se deve à IA, que permite dar aos computadores aprenderem

para a informação, principal *commodity*, e havendo a capacidade de armazenamento e de processamento se espraiado para além dos limites físicos do território nacional, os "problemas" advindos dessa realidade passam a ser transnacionais. Vale reforçar: na sociedade informacional os tratamentos de dados, inclusive dados pessoais, implicam em grande maioria o fluxo transfronteiriço desses dados. Dessa forma, a porosidade da soberania, apontada, entre outros indicadores pela diminuição de um exercício legislativo genuinamente autoral decorre em parte da necessidade de uma convergência regulatória para a normatização de temas afetos às novas tecnologias. Decorre, igualmente, da interconectividade da economia e do modelo de desenvolvimento dependente[61], que demanda a adaptabilidade do mercado interno e a sua internacionalização pela integração em redes de conexão multicontinentais.

Independentemente das causas que originam a porosidade da soberania, isto é, a sua modificação, e a mitigação significativa do poder estatal no contexto da sociedade informacional, com marcante ascensão do poder econômico das plataformas, reverberando em exercício de poder político através da inserção de seus interesses nas pautas de organismos internacionais, fato é que a soberania possui uma reconfiguração. E, assim como a reconfiguração da soberania, que afeta os Estados nacionais, é reflexo do papel central que a informação tem na contemporaneidade, dando poder a quem tem a capacidade e o conhecimento para efetuar mais tratamentos de dados, a reconfiguração da autonomia, que afeta os indivíduos, também deriva da divisão do aprendizado (ZUBOFF, 2019) e do conhecimento, já mencionadas. Antes as origens do desenvolvimento dependente eram relacionadas com processos históricos que levaram a uma divisão internacional do trabalho. Na sociedade informacional essa dependência é lastreada pelo controle do aprendizado, distinguindo quem vai meramente operacionalizar plataformas, seus componentes e derivados e quem tem a capacidade de programar e inovar na seara do processamento de informações e criação de estruturas digitais.

Apesar de o poder econômico das plataformas ter reverberado em poder político, a partir da sua influência na conformação dos sistemas jurídicos nacionais, essa manifestação de poder ainda precisa da estrutura do Estado nacional para alcançar seus objetivos. Conforme

---

com os dados, sem serem explicitamente programados quanto à sua operação. Os dados disponíveis em grande quantidade e o aumento da capacidade de armazenamento desses dados e de processamento, com o *big data*, impacta na característica informacional da economia contemporânea.

[61] Sob a perspectiva da vertente da Teoria do Desenvolvimento Dependente-Associado, desenvolvido por Fernando Henrique Cardoso e Enzo Faletto. Vivemos numa modalidade de Neoliberalismo Globalista, marcado pela abertura da economia ao mercado mundial e pela redução do Estado e reconfiguração do seu papel como negociador de interesses. Para uma visão geral do tema recomenda-se a leitura do artigo "As três tipologias políticas do desenvolvimento-dependente na América Latina: contribuições para um debate contemporâneo" de Bernardo Salgado Rodrigues, referenciado nesta tese.

demonstrado por Naomi Klein[62] (2009) e por escândalos como as denúncias promovidas por Edward Snowden (a partir de 2013), sobre a vigilância intrusiva e desarrazoada de órgãos de inteligência estatal, os Estados em suas atividades de promoção da segurança nacional se valem de informações obtidas pelo compartilhamento de grandes empresas de tecnologia, assim como utilizam ferramentas criadas e operadas por essas empresas privadas. Existe uma retroalimentação de interesses nessa maior paridade de poder entre Estado e organizações privadas. Se de um lado o Estado perde poder, de outro, ele impõe ônus aos particulares que antes eram tipicamente suportados somente por ele na seara da regulação. Por meio dessa paridade de poder se opera, ainda, a virada no modelo regulatório de "comando e controle" para de "regulação responsiva", impondo a participação do particular na fiscalização e no fomento de cultura dos valores que se pretende implementar. O particular se vê compelido a atuar na fiscalização e na proatividade como forma de contingenciar e mitigar riscos de sofrer penalidades que afetem seus interesses (perda de capital reputacional que impacta em prejuízo à fidelização, perdas financeiras pelo pagamento de multas, entre outros).

Quanto à necessidade de fiscalização mútua e de fomento à cooperação por meio de estratégias de estímulo à responsividade, é preciso ter em mente que a sociedade de vigilância tem sua origem em colaborações entre instituições privadas e públicas (VÉLIZ, 2021, p. 68-69), e permanece[63] até hoje, ao passo que a maioria dos Estados nacionais não tem experiência e expertise para desenvolver ferramentas de vigilância e *hackeamento*, empregadas em diversa atividades estatais atinentes à segurança pública e inteligência de Estado. A parceria entre instituições públicas e privadas para extrativismo de dados pessoais tem como raiz além do modelo de desenvolvimento dependente, o estímulo à racionalidade "gerencialista" com foco na eficiência, entendida como diminuição de custos, como métrica de sucesso, e na automatização de tarefas públicas[64] (com a adoção de tecnologias que são desenvolvidas,

---

[62] Klein menciona que o 11 de setembro foi o IPO (*Inicial Public Offering)* – oferta pública inicial - de uma era de simbiose entre a nova economia e as privatizações com o emprego da vigilância e do controle como necessários e aceitáveis em nome da guerra contra o terror. E o Iraque teria sido o primeiro laboratório dessa nova forma de retroalimentação de interesses entre Estado e grandes empresas privadas.

[63] "[...] Países em todo o mundo utilizam os gigantes da tecnologia para fins de vigilância. Palantir, Amazon e Microsoft, por exemplo, forneceram ferramentas que ajudaram a administração Trump na vigilância, detenção e deportação de imigrantes – políticas que foram excepcionalmente controversas devido á separação em massa de crianças de seus pais. Shoppings nos Estados Unidos são conhecidos por capturarem placas de carros e adicionarem essas imagens às bases de dados utilizadas pelas agências de polícia. As grandes empresas às vezes orientam a polícia sobre como acessar e utilizar os dados de seus clientes. [...]" (VÉLIZ, 2021, p. 69).

[64] "[...] Unlike the classical liberal state, neoliberal governance can be interventionist, leveraging law to enhance efficiency in institutions, minimize transaction costs, make decisions based on cost-benefit analysis, and use ever-growing information databases to deliver so-called "smart" forms of governance. This type of Governance relies on mass quantification, datafying as much about a population as possible, and using that data to model potential future outcomes about who or what poses risks." (WALDMAN, 2019, p. 61).

fornecidas e monitoradas por empresas privadas) como sinônimo de neutralidade e de entregas mais impessoais, rápidas e eficientes pelo Estado, e, portanto, como instrumentos de boa governança (WALDMAN, 2019, p. 61).

Ademais, os modelos regulatórios clássicos como o de "comando e controle", além de estarem defasados pela incapacidade do Estado de conduzir a fiscalização e a aplicação de sanções sozinho, sem a cooperação de organizações privadas, segue sendo pautado no objetivo de contingenciar riscos que se mostram como insuportáveis para a segurança jurídica e para continuidade da vida em sociedade. Ou seja, ocorre não com o objetivo principal de fomentar valores e contingenciar danos aos titulares de direitos, mas sim com o objetivo de assegurar a continuidade das relações interpessoais, necessárias para o funcionamento da economia e das relações comerciais. Neste cenário, somente uma estratégia regulatória que aposte nessa mesma cooperação em alguma medida entre público e privado pode ser frutífera.

Como demonstrado, na sociedade informacional os detentores de conhecimento sobre como transformar dados em informações para a criação de mercados certos e para a modulação comportamental de indivíduos e Estados detém o poder. A divisão do conhecimento gerada tanto pela formação de bolhas informacionais, quanto pela assimetria de conhecimento e percepção dos *nudges* que influenciam a autodeterminação coloca de um lado as pessoas naturais na condição de terem a sua autonomia relativizada, e de outro os Estados de terem o poder relativo à soberania mitigado. A complexidade das questões envolvidas na comoditização dos dados pessoais é agravada pelo fato de os agentes de tratamento de dados operarem de maneira transfronteiriça, gerando massivos fluxos de dados também transfronteiriços.

O intricamento das questões emergentes da sociedade informacional, da plataformização e da ubiquidade computacional ilustra os desafios enfrentados pela regulação das novas tecnologias, e o quanto o titular de dados é a parte mais fraca nessa rede de relações de poder. Sendo assim, a ideia de empoderamento efetivo desse titular de dados e a proteção dos seus interesses devem ser centrais na regulação da privacidade e da proteção de dados para evitar a sua objetificação. Essa vertente de proteção do indivíduo é utilizada como parâmetro para a efetividade das políticas públicas analisadas nos capítulos posteriores.

O próximo capítulo é dedicado à análise do desenvolvimento da regulação da privacidade e da proteção de dados em âmbito internacional. Busca-se fazer um parâmetro entre as normas, demonstrando a identificação dessa crescente influência das organizações internacionais na regulação da proteção de dados no âmbito dos Estados nacionais. Essa constatação é importante para a tese por destacar a similaridade das normas em termos

principiológicos, indicando que a disparidade de resultados em termos de proteção efetiva ao titular de dados está atrelada aos mecanismos de *enforcement* adotados.

3 PROTEÇÃO DE DADOS: busca de convergência regulatória na era do capitalismo de vigilância e de plataforma

Este capítulo argumenta que, apesar de a proteção de dados e a autodeterminação informativa enquanto direitos autónomos serem importantes e necessários para a proteção dos direitos de personalidade, a sua regulação constitui um desafio para o Estado nacional por inúmeras razões: o poder massivo detido pelas plataformas; a lógica de funcionamento das plataformas, que implica fluxos de dados transfronteiriços (as plataformas, na maioria das vezes, têm negócio físico num país mas operam em muitos outros, recorrendo a uma cadeia de fornecedores mundialmente disseminada desafiando a lógica da regulação nacional e da soberania enquanto poder exercido sobre um território nacional); a eficácia da regulação exige convergência regulatória e negociação entre Estados nacionais (daí que muitos Estados tendam a adotar modelos regulatórios criados por organismos internacionais e apresentados como as "melhores práticas"); as organizações internacionais que são o campo para o desenvolvimento deste tipo de "regulação convergente" são o ambiente onde as plataformas também exercem o seu poder, através do lobby; a adopção de modelos sem uma reflexão profunda sobre estratégias de *enforcement* resulta em inefetividade; os entes governamentais também são regulados no campo da proteção de dados.

Neste capítulo, esses desafios são tratados, mostrando como a convergência regulatória resulta na adoção de padrões pré-concebidos, explorando uma linha do tempo das normas de privacidade e suas influências de *soft law* de forma a tornar as estratégias de *enforcement* um diferencial importante para a efetividade. Ademais, o reconhecimento da deficiência do Estado deve levar a um regime regulatório cooperativo, apostando no estímulo à responsividade e à transparência para moldar a cultura organizacional e social.

3.1 Da Privacidade à proteção de dados como direito autônomo no mundo: repercussões da sociedade informacional e conectada em rede

Em perspectiva histórica, surge inicialmente a tutela da privacidade (RODOTÀ, 2008), como um direito estático e negativo do indivíduo de ser deixado em paz, de ser deixado só. Sua origem remonta a um contexto de pós-guerras, tendo como marco a *Declaração Universal dos Direitos Humanos*, no seu artigo 12º: “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei”

(ONU, 1948). Em 1950, a *Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais*, do Conselho da Europa[65], remetendo à *Declaração Universal dos Direitos do Homem*, no artigo 8º consagra o direito ao respeito pela vida privada e familiar[66]. A proteção à privacidade segue sendo o foco nas normas de Estados nacionais da década de 1970 (SAMPAIO, 1998; RODOTÀ, 2008).

Em 1980 a OCDE[67] publica um guia com *Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais*, aplicáveis aos fluxos de dados registrados em meio físico ou digital (SAMPAIO, 1998; RODOTÁ, 2008; DE LIMA, 2020). Em que pese este guia ter influenciado fortemente muitas leis de privacidade ao redor do mundo, inclusive o *Privacy Act 1988* (Cth)*[68]*, ele tem natureza de *soft law*, de mera recomendação, sem força cogente. No ano seguinte, 1981, o Conselho da Europa publica a *Convenção 108 para a Proteção de Indivíduos com relação ao Processamento Automático de Dados Pessoais*. Esta *Convenção* figura como primeiro instrumento internacional juridicamente vinculativo (para os signatários e com efeitos nos setores público e privado) adotado no domínio da proteção de dados. O propósito alegado da *Convenção 108*[69] era o de garantir a todas as pessoas singulares o respeito aos seus direitos e liberdades fundamentais, com especial ênfase ao direito à vida privada, em face ao tratamento automatizado dos dados de caráter pessoal. Mesmo sendo o primeiro documento que utiliza a expressão "proteção de dados pessoais", o foco da tutela prevista era somente o tratamento automatizado dos dados, não compreendendo a amplitude do que hoje se entende por proteção de dados pessoais. A *Convenção 108* trabalhava com a perspectiva da garantia pelos membros signatários do documento de um "nível adequado de proteção" aos dados compartilhados, para que pudesse seguir preconizando o livre fluxo desses dados.

---

[65] Necessário elucidar que "Conselho da Europa" não se confunde com "Conselho Europeu". O primeiro é uma organização internacional de defesa dos direitos humanos, da democracia e do Estado de Direito, fundado em 1949, enquanto o segundo é uma instituição da União Europeia, fundado em 1974.

[66] ARTIGO 8º **Direito ao respeito pela vida privada e familiar** 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros. (CONSELHO DA EUROPA, 1950).

[67] Em inglês a sigla é OECD – Organisation for Economic Co-operation and Development.

[68] Trata-se da Lei Australiana de privacidade. No sistema jurídico australiano todas as normas de aplicabilidade nacional são referenciadas com o ano e com a sigla *Cth*, para indicar a referência ao *Commonwealth.*

[69] Vide redação do ***Article 1 – Object and purpose:*** The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Outra importante norma internacional é a *Diretiva 46 de 1995* do Conselho Europeu (46/95/CE), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. O documento traçava diretrizes gerais cuja adoção pelos Estados-membros da União Europeia era considerada desejável para que "as diferenças entre os Estados-membros quanto ao nível de proteção dos direitos e liberdades das pessoas, nomeadamente o direito à vida privada, no domínio do tratamento de dados pessoais" (EU, 1995, n. 7) não constituíssem um obstáculo para as atividades econômicas e escala comunitária. A *Diretiva 46/95* já trabalha com uma linguagem de promoção da harmonização das leis dos Estados-membros num nível mínimo, numa perspectiva de "proteção equivalente" (ALLARS, 2014, p. 109). Entretanto, o texto normativo em referência deixava os Estados-membros livres para a elaboração de leis nacionais que estabelecem maiores restrições em relação ao mínimo estabelecido no documento.

A *Carta da EU,* de 2000, é o primeiro documento a distinguir o direito de proteção à vida privada e familiar[70], prevista no artigo 7º, do direito de proteção dos dados pessoais[71], previsto no artigo 8º. Ambos os direitos mencionados são incluídos no Capítulo II pertinente às Liberdades, assim como os direitos de contrair casamento e de constituir família, de liberdade de pensamento, de consciência e de religião, de expressão e de informação, entre outros, todos direitos ligados à autonomia e a autoconstrução do sujeito. O mencionado diploma é considerado o marco legal da proteção de dados como direito autônomo (RODOTÀ, 2008, p. 17).

Em 2004, o *Asia-Pacific Economic Cooperation – APEC*[72], fórum econômico para facilitação de comércio e investimentos, estabelece o seu *APEC Privacy Framework*, contendo

[70] "*Artigo 7º* **Respeito pela vida privada e familiar** Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações." (2000/C 164/01).

[71] "*Artigo 8º* **Protecção de dados pessoais** 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente." (2000/C 164/01).

[72] Atualmente o APEC tem como membros Austrália, Nova Zelândia, Indonésia, Papua Nova Guiné, Brunei Darussalam, Filipinas, Hong Kong, Taipei, Japão, Coréia do Sul, Singapura, Malásia, Tailândia, Vietnã, China, Rússia, Canadá, Estados Unidos, México, Peru e Chile. Vide informações contidas na página do APEC: https://www.apec.org/About-Us/About-APEC/Member-Economies. Acesso em 25 Jan. 2023.

nove princípios[73] que poderiam ser voluntariamente adotados pelos seus Estado-membros[74], com flexibilidade para o detalhamento dos mecanismos de implementação. Os princípios do APEC para a privacidade são bastante semelhantes com os contidos no *Guia da OCDE* de 1980. O documento tem o claro objetivo de encorajar uma convergência mínima nos parâmetros para lidar com a privacidade de dados, a fim de evitar a criação de barreiras "desnecessárias" para o fluxo de informações entre os países membro, além de fomentar o desenvolvimento de um ambiente negocial cooperativo a partir do mútuo reconhecimento de leis de privacidade entre os membros. Os parâmetros inseridos no documento permitem a adoção de políticas divergentes acerca da privacidade, de maneira que abre margem para a implementação de um nível mínimo de proteção para os dados pessoais muito incipiente e inseguro[75] para os interesses dos titulares.

Em 2010, o APEC iniciou um acordo multilateral abordando fluxos transfronteiriços de dados, o *APEC Cross-Border Privacy Enforcement Arrangement – CPEA*, que resultou no *APEC Cross-Border Privacy Rules (CBPR)*, que contém um *check list* a ser aplicado pelas organizações das economias membro aos destinatários de dados que forem ser compartilhados para checagem acerca da conformidade com os princípios de privacidade do APEC (ALLARS, 2014, p. 114-115). Este *Framework* raramente é mencionado em obras centradas na proteção de dados pessoais, mas é relevante para a tese ao passo que influenciou o panorama da privacidade na Austrália, que é um dos membros fundadores do APEC, estando vinculada ao bloco desde o seu início em 1989 e membro da OCDE desde 1971 (GREENLEAF, 2009;

---

[73] Os princípios contidos no *APEC Privacy Framework* são: prevenção de danos ao titular de dados; fornecimento de aviso prévio quanto a coleta de dados; limitação na coleta de dados pessoais; limitação do uso de dados pessoais (dados pessoais devem ser usados somente para cumprir com o propósito da coleta e outros compatíveis com o propósitos relatados para a coleta, a limitação não ocorre quando o tratamento diverso é feito com o consentimento do titular, quando necessário para o fornecimento de um produto ou serviço para o titular, em decorrência de lei ou outro instrumento legal); escolha (quando apropriado, os indivíduos devem ser providos com claro, proeminente, de fácil entendimento, e acessível mecanismo para escolher sobre a coleta, divulgação e uso dos seus dados pessoais; isso pode não ser apropriado quando os controladores de dados estão coletando dados pessoais disponíveis publicamente); integridade dos dados pessoais (as informações pessoais devem ser mantidas acuradas, completas e atualizadas para o propósito de uso); garantias de segurança (medidas de segurança devem ser tomadas para proteger informações pessoais); acesso e correção (os titulares devem ser informados e ter acesso às informações a eles relativas, assim como devem poder retificar informações, quando necessário); prestação de contas através de um modelo regulatório. *Tradução nossa.*

[74] Conforme ressalta Chris Pounder (2007, p.2) em artigo que critica a vacuidão e ambiguidade do modelo proposto pelo APEC, a China já indicou que não se compromete com a implementação de medidas legislativas ou administrativas para aderir aos princípios do modelo.

[75] A esse respeito, colaciono observação de Chris Pounder (2007, p. 2): "Caution needs to be exercised when discussing the likely deficiencies in the APEC Privacy Framework. The Framework's principles were drafted in order to get agreementsbetween diplomats – and diplomatic agreements tend to fudge important issues. The result is that the principles are ambiguous as to their effect and are capable of a vast number of interpretations and implementations. It is possible that an APEC member state, for example, Australia or New Zealand, could develop rules compliant with European Directive standards. But other member states could use the Framework's flexibility to implement a minimalist approach to privacy compliance that falls very far short of what would be deemed "an adequate level of protection"."

ALLARS, 2014; APEC, 2023). Relevante esclarecer que a *soft law* do APEC aborda a proteção à privacidade, sem estabelecer uma distinção da proteção de dados pessoais como direito autônomo.

Como intermediária na escala de contextualização histórica está a autodeterminação informativa (VALADARES, 2021), que tem como origem a necessidade de ampliação dos poderes do titular de dados pessoais para que possa se opor a tratamentos indevidos, e diz respeito à prerrogativa de acesso aos dados que estejam em processamento e de determinação por parte do titular em relação aos tratamentos realizados. Ou seja, consiste no poder de saber se o dado pessoal está em tratamento, de ter transparência quanto à finalidade de tratamento e limites desse tratamento, assim como de eventualmente se opor a esse processamento, quando julgar ilegítimo, além de requerer o apagamento desses dados. Tem como marco temporal decisão histórica da Corte Constitucional Alemã de 1983, que reconheceu a autodeterminação informativa como "o direito de manter o controle sobre as próprias informações e de determinar a maneira de construir a própria esfera particular" (RODOTÀ, 2008, p. 15; VALADARES, 2021). A autodeterminação informativa é tida como medida imprescindível para a autonomia do indivíduo na sociedade informacional (CASTELLS, 2013, p.56-57). Da mesma forma, revela-se crucial para a efetividade da política pública de proteção de dados pessoais (VALADARES, 2021) no sentido de proteger direitos da personalidade.

O *General Data Protection Regulation (GDPR) (REGULATION (EU) 2016/679),* norma de proteção de dados da União Europeia (UE) que tem sido usada como referência em termos de proteção de dados e que influenciou fortemente a LGPD (IRAMINA, 2020, p. 92; DEMETZOU, ZANFIR-FORTUNA, VALE, 2023, p. 8), é publicada em 2016, entrando em vigor em 2018. O *GDPR* mantém princípios e o sentido geral da *Diretiva 46 de 1995* no que diz respeito ao seu teor, mas a revoga. Uma diferença marcante é que o *GDPR* é imposto a todos os tratamentos de dados realizados por controladores e operadores que estejam inseridos na UE, independentemente de o tratamento do dado em si ocorrer ou não na União Europeia. Existe, assim, a aplicabilidade obrigatória por todos os membros da UE, diferentemente do que ocorria com a *Diretiva 46 de 1995* (BIONI, ZANATTA, 2021, p. 83). Outro aspecto bastante relevante é a previsão de eficácia extraterritorial[76], ao passo que o processamento de dados de

[76] Vide a redação do item 23 do preâmbulo do *GDPR:* "In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a

titulares que estejam na UE, ainda que realizado por controladores ou operadores fora da UE devem se submeter às exigências do *GDPR*. Essa previsão impulsionou um espraiamento das normas de proteção de dados ao redor do mundo, especialmente em países que mantém intensa relação comercial com a UE, assim como operou uma modificação na apresentação de bens e serviços não-rivais oferecidos *on-line* (sempre com *banner* de *cookies*, e documentos como Termos de Uso e Políticas de Privacidade). Como meio de demonstrar o "nível de proteção equivalente" ao fixado pelo *GDPR* muitas dessas normas acabaram se espelhando na estrutura e conteúdo da norma europeia. Necessário frisar, ainda, que a atuação da Autoridade Nacional de Proteção de Dados brasileira (ANPD) se valeu bastante de como o *GDPR* tem sido aplicado e interpretado para fixar orientações sobre a aplicação da LGPD (vide publicações dos *Guias Orientativos de Tratamento de Dados Pessoais pelo Poder Público* e *de Agentes de Tratamento e Encarregado*, disponíveis no site da ANPD[77], por exemplo).

Cumpre destacar que as normas resultantes dessa influência de *soft laws* possuem cunho principiológico e contam com a redação em cláusulas abertas à interpretação, demandando a atuação de autoridades no sentido de emitir orientações e enunciados para a interpretação e aplicação das normas, que gravitam em torno de um mesmo eixo fundamental de princípios, conforme demonstrado na tabela disposta no final desta seção. Sendo assim, no que tange a orientação geral da proteção estabelecida no plano normativo, não existe diferença substancial entre elas. A diferença em termos de efetividade da proteção estabelecida ocorre, em verdade, como fruto das estratégias de *enforcement*, ou seja, da estrutura e das medidas disponíveis para o titular de dados para fazer valer seus direitos, bem como das medidas de fiscalização e de reforço negativo, de aplicação gradativa de punições quando os desvios são encontrados que estejam em funcionamento.

---

currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union. In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.". Assim como redação do artigo 3 do *GDPR*: **Territorial scope** 1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2.This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. 3.This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

[77] Disponíveis em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em 10 Jul. 2023.

Em que pese as normas mencionadas sempre utilizarem o discurso de proteção ao indivíduo, do titular como centro da tutela estabelecida e da tecnologia como colocada à serviço da humanidade e do seu melhor interesse, também não se furtam de referendar a necessidade de convergência regulatória para que a incerteza e a iniquidade de níveis de proteção não figurem como obstáculos à livre circulação dos dados pessoais entre diferentes Estados nacionais. Em documentos oriundos de blocos econômicos como o APEC e a UE (*GDPR*), resta evidente que os sistemas de proteção de dados pessoais concebidos são em verdade vocacionados ao estabelecimento de um nível abstrato de proteção aos dados pessoais, sendo normas de segurança informacional, e não de soberania informacional para os titulares. A real preocupação por trás desses documentos parece ser a de assegurar a continuidade dos tratamentos de dados ao estabelecer standards de segurança com intuito de fomentar a livre circulação desses dados, vide à título de exemplo, o item 3 do artigo 1 do *GDPR*: "3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.*"* (GDPR, 2016).

É no contexto de sociedade informacional, marcado pela vida conectada que são acirradas discussões que culminam no movimento de normatização da proteção de dados pessoais. A proteção de dados pessoais como direito autônomo é reflexo de um amadurecimento da ideia de privacidade, contemplando um adicional, de tutelar os dados pessoais em movimento. Daí se dizer que se trata de tutela dinâmica, já que não diz somente respeito à proteção da inteligência do dado, mas de como essa informação será empregada, pensando em uma limitação finalística. A demanda por uma tutela dinâmica tem início na década de 1950 com o surgimento da Internet, mas a inclusão desse direito em normas nacionais começa a ser observada com maior ênfase a partir da década de 1990, com a popularização e escalabilidade da rede mundial de computadores (RODOTÀ, 2008; DE LIMA, 2020). Tem-se, assim, que a proteção de dados pessoais consiste no direito do titular de não ser simplificado, objetivado, e avaliado fora de contexto, de poder proteger e dispor do seu corpo digital, obstando que outros o façam ilegitimamente.

Ante o reconhecimento do potencial risco de violação da autodeterminação e da autonomia dos sujeitos, com base no cenário de inovações tecnológicas e de mescla entre as realidades digital e material, cresce movimento internacional pela regulação do tratamento de dados pessoais. Esse movimento é iniciado em organismos internacionais, conforme demonstrado. Sendo progressivamente incorporados nos sistemas jurídicos nacionais, em uma

mescla de impulso por meio da efetiva normatização, e de avanço interpretativo da jurisprudência.

É notável que o caminho da privacidade até a derivação do direito à proteção de dados pessoais possui íntima relação com o avanço da informática e das novas tecnologias como a IA e o *big data*, que implicam a possibilidade de tratamentos massivos de dados, a partir do aumento na capacidade técnica de armazenamento. Tem relação próxima com a popularização e escalabilidade da internet, que permite o estreitamento das barreiras territoriais e comunicacionais, impulsionando a interconexão e a realização de transações entre pessoas comuns para além das fronteiras do Estado nacional. Os fluxos de dados foram se tornando progressivamente transfronteiriços, fazendo com que a contenção de potenciais efeitos nocivos à dignidade humana fossem alçados ao patamar de problema transnacional.

O quadro abaixo demonstra a similaridade do conteúdo principiológico das normas de proteção de dados mencionadas. A existência de princípios basilares abordados de alguma maneira em todas as normas demonstra a convergência normativa se materializando, e reforça o argumento da tese de que as estratégias de *enforcement* desempenham papel relevante para a efetividade da norma, da regulação. Dito de outra forma, a qualidade do *enforcement* determinará o quanto a norma se realizará na vida prática.

Tabela 1- Princípios basilares nas normas de proteção de dados mencionadas

Princípios Basilares	**OCDE *Guidelines***	**Convenção 108**	**Diretiva 46/95/CE**	***Privacy Act 1988* (Cth) – *Australian Privacy Principles - APP* (2014)**	***APEC Privacy Framework (2004)***	**GDPR**	**LGPD**
A coleta de informações pessoais deve ocorrer por meios justos e legais	Princípio da limitação de coleta – Art. 7	Princípio da qualidade dos dados – Art. 5, (a)	Qualidade dos dados – Art. 6, (a)	APP 3 – Critérios para coleta de informações pessoais; APP 4 – tratamento de informações pessoais não solicitadas	Notificação – Art. 15; Limitação de coleta – Art. 18	Princípio da licitude, lealdade e transparência – Art. 5, 1 (a)	Coleta somente nas hipóteses dos Arts. 7 e 11 (dados pessoais sensíveis) – Bases legais para tratamento; Princípio da não discriminação – Art. 6, IX
A quantidade de informações pessoais deve ser limitada ao que for	Princípio da limitação de coleta – Art. 7	Princípio da qualidade dos dados – Art. 5, (c)	Qualidade dos dados – Art. 6, (c)	APP 3 – Critérios para coleta de informações pessoais	Limitação de coleta – Art. 18	Princípio da minimização dos dados – Art. 5, 1 (c)	Princípios da adequação e da necessidade – Art. 6, II e III

necessário para atingir a finalidade para a qual os dados foram coletados							
A coleta de informações pessoais deve ocorrer para finalidades específicas e o processamento deve ser compatível com essas finalidades	Princípio da especificação de finalidade – Art. 9; Princípio da limitação de uso – Art. 10	Princípio da qualidade dos dados – Art. 5, (b)	Qualidade dos dados – Art. 6, (b)	APP 6 – Uso e divulgação de informações pessoais	Notificação – Art. 15; Escolha – Art. 20; Uso de informações pessoais – Art. 19	Princípio da limitação das finalidades – Art. 5 (b); Princípio da limitação da conservação – Art. 5, 1 (e)	Princípio da finalidade – Art. 6, I
O tratamento de informações pessoais para finalidades secundárias somente pode ocorrer mediante consentimento do titular, autorização legal ou decisão de autoridade competente	Princípio da especificação de finalidade – Art. 9; Princípio da limitação de uso – Art. 10	Implícito no Princípio da qualidade dos dados – Art. 5, (a) e (b)	Implícito no Princípio da qualidade dos dados – Art. 6, (a) e (b); Critérios para processamento legítimo de dados – Art. 7	APP 6 – Uso e divulgação de informações pessoais	Uso de informações pessoais – Art. 19	Princípio da limitação das finalidades – Art. 5, 1(b); Princípio da limitação da conservação – Art. 5, 1(e)	Bases legais de tratamento – Arts. 7 e 11 (dados pessoais sensíveis)
As informações pessoais devem ser relevantes, precisas e completas para as finalidades de tratamento	Princípio da qualidade dos dados – Art. 8	Princípio da qualidade dos dados – Art. 5, (c) e (d)	Qualidade dos dados – Art. 6, (d)	APP 10 – Qualidade das informações pessoais	Integridade das informações pessoais – Art. 21	Princípio da exatidão – Art. 5, (d); Princípio da integridade e confidencialidade – Art. 5,1 (f)	Princípio da qualidade dos dados – Art.6, V
Devem ser adotadas medidas de segurança para proteger as	Princípio das proteções de segurança – Art. 11	Segurança de dados – Art. 7	Segurança no processamento dos dados – Art. 17	APP 8 – compartilhamento transfronteiriço de informações pessoais; APP 9	Salvaguardas de segurança – Art. 22	Princípio da integridade e confidencialidade – Art. 5, 1(f)	Princípios da segurança e da prevenção – Art. 6, VII e VIII

informações pessoais				– limitação da adoção, uso e compartilhamento de identificadores governamentais; APP 11 – Segurança das informações pessoais			
As pessoas devem ter acesso a informações a elas relativas, assim como poder requerer essas informações e retificá-las quando necessário	Princípio da abertura – Art. 12; Princípio da participação individual – Art. 13	Salvaguardas adicionais – Art. 8	Direito de Acesso – Art. 12	APP 1 - Abertura e transparência no manejo das informações pessoais; APP 5 – Notificação quanto a coleta de informações pessoais; APP 12 – Acesso às informações pessoais em tratamento; APP13 – Correção das informações pessoais	Acesso e correção – Art. 23	Princípio da licitude, lealdade e transparência – Art. 5, 1 (a); Direitos do titular dos dados – Arts. 12 ao 23	Princípio da transparência – Art. 6, VI; Direitos do titular – Art. 18, I, II, III e VIII
Os agentes de tratamento de informações pessoais devem ser responsáveis pelo cumprimento dos princípios contidos na norma	Princípio da responsabilidade e prestação de contas – Art. 14	Implícito no Art.1	Implícito na obrigação de notificação à autoridade competente – Arts. 18, 19, 20 e 21	APPs 1 ao 13	Responsabilidade de prestação de contas – Art. 26	Princípio da responsabilidade – Art. 5, 2	Princípio da responsabilização e prestação de contas – Art. 6, X

A próxima seção é dedicada à propositura de reflexões acerca das causas e efeitos dessa convergência regulatória.

3.2 Convergência regulatória da privacidade e da proteção de dados: emulação e a emergência das estratégias de *enforcement* como diferencial

O caminho percorrido até a derivação da privacidade em proteção de dados pessoais como direito autônomo está ligado com o desenvolvimento da tecnologia e a sua ubiquidade, sendo incorporada na vida cotidiana dos sujeitos. Existe uma linha cada vez mais tênue que separa a realidade dita digital e a material. Privacidade, autodeterminação informativa e proteção de dados pessoais são direitos diversos, cuja efetivação seria imprescindível para um reforço mútuo no contexto da sociedade informacional em sentido de promover a dignidade da pessoa humana, a partir da preservação do corpo digital e de aspectos morais da personalidade. A necessidade de proteção da personalidade é a grande justificativa para a derivação da proteção de dados em direito autônomo como frisado, bem como para o seu espraiamento nos sistemas jurídicos no mundo. A efetiva proteção do corpo digital de fato demandaria a convergência regulatória, ao passo que o fluxo de dados na sociedade informacional ocorre em grande parte de maneira transfronteiriça. Nota-se que os servidores e bases de dados das principais plataformas que prestam serviços em ambiente digital, como o *Google*, a *Meta*, a *Microsoft*, a *Apple*, entre outras, são situados em territórios nacionais restritos, prejudicando a aplicabilidade prática de normas nacionais, mesmo diante da corrente previsão de aplicação extraterritorial. Os riscos para a personalidade e mesmo para a segurança de coletividades são mais do que evidentes e bastante difundidos em livros que abordam o tema do incremento da vigilância e da sua naturalização sob discursos como a necessidade de combater o terrorismo, de preservar a democracia, de manter a segurança, de medir produtividade, de melhorar performance etc.

Muitos autores argumentam que o evento histórico que contribuiu sobremaneira para a naturalização da vigilância por parte das agências estatais foi o ataque às Torres Gêmeas em Nova Iorque, conhecido como o 11/09/2001 (RODOTÀ, 2008; KLEIN, 2015; ZUBOFF, 2020; VÉLIZ, 2021). Muitos Estados nacionais aprovaram leis permitindo a prática de vigilância sob a justificativa de que essa seria a única forma de combater o terrorismo, de manter a paz mundial e a segurança, após o mencionado episódio. E muitos projetos de normas relativas à proteção de dados pessoais foram interrompidos e os debates sobre o tema prejudicados em face do temor da "ameaça terrorista". Para que a vigilância estatal fosse efetiva, e o combate à "ameaça terrorista" se concretizasse, ocorreram muitas alianças entre agências governamentais de segurança e empresas privadas que atuam na sociedade informacional fornecendo serviços e produtos tecnológicos de propósitos variados (reconhecimento facial, identificação de riscos, interação remota, mapeamento de territórios, entre outros). Autoras como Véliz (2021) e Zuboff

(2019) argumentam que essas associações entre Estado e entidades privadas resultaram num afrouxamento da perspectiva de regulação das atividades dos particulares na seara do processamento de dados, especialmente de dados pessoais. E essa união entre governos e empresas privadas torna o desafio de regular o fluxo de dados ainda maior, por demandar que entidades públicas e privadas sejam reguladas a um só tempo, além do estabelecimento de ambiente regulatório em que todos os regulados tenham que exercer a supervisão sobre as práticas dos seus parceiros comerciais.

Sampaio (1998) apresenta uma visão de que o espraiamento de normas versando sobre privacidade é fruto do amadurecimento progressivo das discussões em âmbito internacional, e de como os Estados nacionais se utilizam da emulação enquanto aproveitamento de experiências de outros para caminhar em sentido de melhoramento contínuo. A emulação parece ser causa plausível não só para a convergência regulatória, como para a inovação nos sistemas jurídicos locais a partir de atividade não autoral dos Estados, ou seja, pela adesão à preceitos de normas internacionais ou de outros Estados nacionais. E essa adesão por emulação é motivada pela constatação da demanda atinente à convergência regulatória, ao passo que o problema oriundo dos fluxos transfronteiriços de dados em meio à intermediação por plataformas se tornou transnacional, quanto para pertencimento, para continuidade de relações travadas na economia em rede, pela ostentação de medidas normativas que demonstrem um nível de proteção adequado ao tratamento de dados pessoais.

Em que pese se reconheça a emulação e a razoabilidade do argumento em prol da convergência regulatória, não se pode olvidar que a urgência pela proteção de dados como direito autônomo foi fomentada necessidade das grandes corporações que lidam com os dados pessoais como insumos de assegurar a continuidade do fluxo desses dados. A esse respeito Rodotà (2008, p. 54) menciona a importância da IBM na regulação do uso de dados na Suécia. A maneira com que a proteção de dados é abordada, como resultado do impacto do *lobby* no processo de aprovação das normas organismos internacionais, acaba por ocasionar a possibilidade de haver conformidade de fachada, a criação de documentações e certificações que atestem a segurança informacional e o compromisso com os direitos do titular sem que, de fato, se note uma preocupação real com a promoção desses direitos.

Relatório[78] elaborado e publicado pelo *Corporate europeu Observatory Lobby Control e.V. Brussels and Cologne*, de 2021 (BANK, DUFFY, LEYENDECKER, SILVA, 2021), demonstra com dados quantitativos o poder político que as plataformas digitais exercem por

[78] Disponível em: https://corporateeurope.org/en/2021/08/lobby-network-big-techs-web-influence-eu. Acesso em 10 Dez. 2022.

intermédio do *lobby* nos processos de elaboração de políticas. O relatório traz análises atinentes ao processo de elaboração e aprovação do *Digital Services Act – DAS* e do *Digital Markets Act – DMA*, normas visam regular a atuação de plataformas digitais, através da criação de um espaço digital em que os direitos fundamentais dos usuários sejam protegidos e do estabelecimento, ao mesmo tempo, de um ambiente propício à inovação, ao crescimento e à competitividade no mercado europeu e global. Os resultados encontrados quanto ao mapeamento do *lobby* nos processos de elaboração de políticas da União Europeia chamam atenção, apesar de somente reforçarem uma percepção existente sobre o domínio das plataformas, especialmente as de propriedade de *big techs* já mencionadas neste tese:

> […] Together, they spend over € 97 million annually lobbying the EU institutions. This makes tech the biggest lobby sector in the EU by spending, ahead of pharma, fossil fuels, finance, or chemicals; in spite of the varied number of players, this universe is dominated by a handful of firms. Just ten companies are responsible for almost a third of the total tech lobby spend: Vodafone (€ 1,750,000), IBM (€ 1.750.000), QUALCOMM (€ 1.750.000), Intel (€ 1,750,000), Amazon (€ 2,750,000), Huawei (€ 3,000,000), Apple (€ 3,500,000), Microsoft (€ 5,250,000), Facebook (€ 5,550,000) and with the highest budget, Google (€ 5,750,000); out of all the companies lobbying the EU on digital policy, 20 per cent are US based, though this number is likely even higher. […] More than 140 lobbyists work for the largest ten digital firms day to day in Brussels and spend more than € 32 million on making their voice heard; Big Tech companies don't just lobby on their own behalf; they also employ an extensive network of lobby groups, consultancies, and law firms representing their interests, not to mention a large number of think tanks and other groups financed by them. The business associations lobbying on behalf of Big Tech alone have a lobbying budget that far surpasses that of the bottom 75 per cent of the companies in the digital industry. (BANK, DUFFY, LEYENDECKER; SILVA, 2021, p. 6)

O mencionado relatório deixa evidente um dos desafios da atividade regulatória que impacte as plataformas, que extrapolam as variáveis imanentes à sociedade informacional: os reguladores têm que enfrentar enorme pressão por parte das plataformas digitais, especialmente das *big techs*, que utilizam o domínio oriundo da divisão do aprendizado e do conhecimento (que lhes assegura concentração de poder econômico financeiro) como ameaça para mobilizar a opinião pública e neutralizar intenções regulatórias que desafiem em demasia os seus interesses. Outra estratégia é a adoção do discurso de que qualquer medida que venha a impactar no *modus operandi* das plataformas acarretaria risco de desencorajamento de investidores no país, ou mesmo no encerramento de atividades de certas plataformas no território em que a regulação tenha aplicabilidade.

No Brasil durante discussões travadas em 2023 sobre o Projeto de Lei (PL) nº2630/2020, apelidado de PL das *fake news*, cujo trâmite visa a instituição de uma lei de liberdade, responsabilidade e transparência na Internet, que seria (conforme debate predominante até 2022) aplicável a redes sociais, serviços de mensagem instantânea e buscadores, *Google* e *Telegram* foram advertidos por explicitamente travarem campanha contra o projeto de lei. O

Google pela disponibilização da seguinte frase na página de busca "O PL das *fake news* pode aumentar a confusão sobre o que é verdade ou mentira no Brasil", e o *Telegram* por envio de uma mensagem de texto aos usuários enfatizando que a democracia estaria sob ataque no Brasil e que o PL das *fake news* daria poder de censura ao governo[79]. No mesmo sentido, Zuboff (2019) argumenta como o *lobby* é instrumento de exercício de poder capilarizado pelas plataformas. Isso porque é exercido não somente em ambientes de elaboração de políticas públicas, mas busca assegurar influência pela formação de alianças com políticos (através do financiamento de campanhas), pelo fomento de estudos acadêmicos, com o financiamento de pesquisas, para reforçar os argumentos convenientes aos seus interesses, e pela mobilização direta da opinião pública com a disseminação de desinformação e o impulsionamento de resultados de pesquisas que apresentem resultados favoráveis aos seus interesses, como uso de argumento de autoridade.

Mesmo sendo evidente que os sistemas de proteção de dados pessoais, enquanto resultantes do cenário demonstrado, são até certo ponto ficcionais, por não possuírem a real vocação de promover a tutela da autonomia e da autodeterminação informativa, consequentemente não sendo aptos a assegurar a dignidade da pessoa humana, tampouco a proteger o corpo digital, há que se ter em conta que eles constituem, no dizer de Bethânia Assy[80] (2019), a um só tempo uma promessa e uma efetivação normativa. E isso, do ponto de vista de *enforcement,* é de extrema importância por fornecer o potencial de os sujeitos reivindicarem esse direito, por criar uma causa de ação, permitindo que a partir de sucessivas reivindicações o panorama possa ser modificado progressivamente. Assim, a efetivação normativa rompe com a esfera do meramente simbólico, independentemente das razões que fomentaram a sua realização, dos verdadeiros porquês que jazem ocultos, dos poderes que estão encriptados na sua produção e dos efeitos veridicamente buscados de neutralizar a *potentia*, pela dominação ao estabelecer uma *potestas*. Vale ressaltar: uma vez que a normatização ocorre e que um direito é fixado no sistema legal, seu titular pode mover o sistema institucional para concretizá-lo. Notável, por conseguinte, que a efetivação normativa, embora não seja o único caminho possível, e por si só não tenha o condão de modificar de imediato a realidade, sempre carrega

[79] Vide reportagem, disponível em: https://tecnoblog.net/noticias/2023/05/09/telegram-publica-texto-preguicoso-contra-pl-das-fake-news/. Acesso em 25 Mai. 2023.

[80] Vide vídeo do Café Filosófico da CPFL, de 2019, em que Bethânia Assy ressalta essa importância da efetivação normativa, ainda que inefetiva em produzir os efeitos que supostamente intende gerar. Mesmo na negação total de direitos, o sujeito ainda tem o poder de reivindicá-los. Esse potencial da normatização o retira da esfera do que é meramente simbólico, pois empodera em alguma medida o titular de direitos. Disponível em: https://www.youtube.com/watch?v=T_eXibue6gM. Acesso em 05 Jan. 2021.

consigo a potência de modular a cultura vigente e transformar progressivamente a concretização da tutela assegurada em lei.

Cumpre ressaltar, ainda, que a simples denúncia quanto à inefetividade das políticas de proteção de dados, e quanto ao fato de elas serem resultados da atuação de organismos internacionais, influenciados pelo *lobby* das plataformas, que provocam a internalização de diretrizes e diretivas nos sistemas legais nacionais, não sendo fruto de exercício legislativo autoral, também não opera a mudança dos paradigmas existentes. Inegável o potencial de trazer luz o que segue encriptado, evitando a satisfação acrítica com a "inovação" normativa, entretanto a denúncia isolada não promove a transformação da realidade. Tampouco promove o melhoramento do que está posto, que é o subsídio com o qual se pode trabalhar para buscar proteção mais efetiva para os tratamentos de dados pessoais. Tendo em vista essa constatação e a vontade de contribuir de alguma maneira com o melhoramento da política pública de proteção de dados fez-se imperiosa a adoção de novo recorte para a tese, a partir da realização do estudo comparado entre os sistemas Australiano e Brasileiro de privacidade e proteção de dados, de forma a entender nuances na efetivação dos direitos que podem ser benéficas para o melhoramento de ambos os sistemas em estudo, especialmente no que tange as estratégias de *enforcement.*

Ademais, tendo em vista a noção adotada de política pública, entendida como uma ação governamental coordenada em escala ampla para atuar sobre problemas complexos (BUCCI, 2019), a abordagem de aspectos ontológicos da Política Nacional de Proteção de Dados Pessoais demanda a premissa de que a perspectiva adotada é a do Estado como centro emanador da regulação e condutor das estratégias para atingir os fins colocados como justificativa para a instituição da política. Dentro dessa perspectiva, ao lidar com a política pública de proteção de dados, a presente pesquisa se debruça sobre as estratégias fixadas na LGPD – suporte normativo da política pública que institui suas diretrizes e contornos gerais – para aplicação das suas exigências, cumuladas às efetivas ações por parte do Executivo nacional para estruturar o arcabouço institucional e funcional que viabilizem a fiscalização e reforço dos requerimentos impostos pela LGPD. Isso posto, e considerando que uma das causas existentes para o espraiamento de normas regulando o tratamento de dados pessoais é a necessidade de atender a um padrão fixado em âmbito internacional, para assim garantir a continuidade e a competitividade num mercado em rede, um dos efeitos dessa forma de instituição sem um genuíno e autêntico planejamento estatal é a fragilidade das estratégias de *enforcement* da política pública em comento. Esse efeito é constatado tanto pelo fato de ANPD, autoridade central para a concretização da política pública e para o seu melhoramento ter sido criada

vinculada à Presidência da República, quanto pela decorrência de não ter autonomia orçamentária, dado que a criação se deu sem aumento das despesas estatais[81]. A autonomia orçamentária da ANPD só veio a ser estabelecida em 2022, por meio da *Lei Federal nº. 14.460, de 25 de outubro de 2022*, derivada da aprovação da *Medida Provisória nº. 1.124/2022.*

Como destacado por Giovani Clark, Leonardo Alves Corrêa e Samuel Pontes do Nascimento (2019), o fator econômico atravessa e impacta na efetividade ou inefetividade de todas as políticas públicas, mesmo as mais específicas e aparentemente vocacionadas prioritariamente a uma repercussão social. Vale dizer, a efetividade das políticas públicas passa pelas estratégias de *enforcement*, que demandam gasto para a reunião e planejamento dos recursos necessários (pessoais, técnicos, tecnológico institucionais, entre outros). O menor investimento para a busca de efetividade das políticas públicas instituídas é fruto do momento econômico vivido pelo Brasil, de neoliberalismo de austeridade (CLARK[82], 2021), sendo ao mesmo tempo um indicador de que algumas medidas normativas têm sido adotadas mais para assegurar o pertencimento num panorama de relações transnacionais do que para a efetivação de direitos, cabendo aos pesquisadores do campo direito e políticas públicas sinalizar essa constatação e ir além pensando em modificar o que está posto para o melhoramento contínuo da política pública.

A próxima seção argumenta sobre os desafios de o Estado figurar como regulador e regulado, e ter recursos cada vez mais escassos, sendo incapaz de assumir o ônus da fiscalização e reforço das políticas públicas sozinho (modelo de comando e controle), e as repercussões disso na instituição de modelos regulatórios que apostam na cooperação entre Estado e particulares, como o que tem prevalecido no campo da proteção de dados pessoais.

3.3 Estado como regulador e regulado: elementos de regulação responsiva e a construção da cultura de privacidade e proteção de dados

A disputa por soberania de fato já não ocorre somente entre Estados nacionais. A disputa pelo poder de controle do digital é travada entre Estados e empresas de tecnologia, que operam em escala transnacional, como agentes de tratamento de dados pessoais. E o indivíduo, titular

[81] Essa vinculação e a ausência de aumento de despesas se encontravam na redação da LGPD que entrou em vigor em 2020. Durante o desenvolvimento da pesquisa utilizou-se a página de transparência da ANPD e da Presidência da República para endosso da premissa, constatando-se que as únicas despesas efetivadas para o funcionamento inicial da ANPD foram pertinentes ao pagamento de diárias para viagens dos seus agentes.

[82] Conforme curso "Direito e Políticas Públicas", ministrado pelo Prof. Giovani Clark no primeiro semestre de 2021 no Programa de Pós-graduação em Direito da PUC Minas.

de dados pessoais figura como massa de manobra, como fornecedor de matéria prima, alienado da possibilidade de escolha, que inexiste como pontua Floridi (2020). Em que pese a soberania digital de fato seja exercida pelas empresas, a soberania de direito segue nas mãos dos Estados nacionais, que passam a ser alvos do *lobby* das plataformas, ao passo que as regulações propostas podem impactar as suas operações (FLORIDI, 2020, p. 375-377). A sociedade informacional impulsionou a mudança nos papeis desempenhados pelo indivíduo e pelos Estados nacionais. O indivíduo passa de votante / consumidor, para o papel de seguidor/ usuário no novo modelo econômico informacional (FLORIDI, 2020, p. 375-377). E o Estado nacional deixa de exercer poder determinante, figurando mais como um negociador de interesses com as empresas transnacionais e com outros Estados e organismos internacionais.

Cumpre rememorar que o sentido de regulação empregado nesta tese é abrangente, referindo-se aos processos de estabelecimento de normas, assim como ao seu monitoramento e reforço, para efetiva aplicabilidade (BARAK-CORREN, KARIV-TEITELBAUM, 2021). Esta seção concentra-se na perspectiva da regulação promovida a partir do Estado no âmbito da política pública de proteção de dados. Essa opção metodológica não implica desconhecimento do crescente papel de atores não estatais no processo regulatório (AYRES, BRAITHWAITE, 1992; GRABOSKY, 2013), especialmente a partir da difusão da visão da governança como fator de eficiência. Muitas organizações privadas atuam no processo regulatório, a partir do estabelecimento de sistemas de integridade, com a instituição de programas de compliance e de governança de dados, contando com arcabouço de normas internas (políticas, processos e procedimentos orientados pela visão, missão e valores da organização, assim como pela busca pela conformidade com as normas estatais e com as "melhores práticas").

Feitos esses esclarecimentos, é interessante observar que a LGPD, suporte normativo da Política Nacional de Proteção de Dados Brasileira, institui um tipo de regulação pautada no estímulo à responsividade dos agentes de tratamento, à proatividade, e à escalabilidade de punições, partindo de medidas preventivas, em uma atuação também responsiva por parte da ANPD. Assim, tem-se que a perspectiva regulatória instituída pela LGPD e ratificada pela *Resolução CD/ANPD nº. 4, de 24 de fevereiro de 2023* é alinhada com a proposta da regulação responsiva, desenvolvida inicialmente por Ian Ayres e John Braithwaite (1992) (IRAMINA, 2020). O alinhamento com a regulação responsiva no sistema regulatório instituído pode ser percebida pelos seguintes indicadores: utilização de escalonamento das sanções previstas no art. 52 da LGPD *(*conforme art. 3º, §1º do *Regulamento de Dosimetria e Aplicação de Sanções Administrativas)*, com uma abordagem caso a caso (art. 5º do *Regulamento de Dosimetria e Aplicação e Sanções Administrativas)*; proposta de levar em conta a postura do agente de

tratamento na condução de eventual violação à LGPD*;* recompensar agentes de tratamento que proativamente busquem remediar violações detectadas; trabalhar com a ideia de relativização de sanções administrativas, caso o agente demonstre que as medidas de segurança da informação e de promoção de meios para que o titular exerça os seus direitos foram efetuadas de maneira alinhada com as melhores práticas, respeitado o estado da técnica; estimular a cooperação entre os envolvidos na cadeia de tratamento de dados pessoais (agentes de tratamento se fiscalizando mutuamente e exigindo garantias de adoção de medidas como meios de se resguardar). Todos os indicadores mencionados fazem parte de uma estratégia de persuasão, pela dissuasão à não conformidade.

A característica mais emblemática da regulação responsiva é a concepção da instituição de uma abordagem do *enforcement* através de uma pirâmide de escala punitiva, que visa adequar a ferramenta de aplicação da norma regulatória pelo regulador de acordo com o comportamento do regulado, partindo da base da pirâmide, pautada em ações dialógicas e menos drásticas, como forma de estimular a compreensão do interesse público por trás da norma e dissuadir comportamentos desviantes. Em linhas gerais, a abordagem inicial do regulador deve ser sempre no sentido de tentar a cooperação do regulado, antes de lançar mão de estratégias[83] punitivas. Essa concepção registrada inicialmente na obra *Responsive Regulation: transcending the deregulation debat,* de Ian Ayres e John Braithwaite (1992) e lastreada por estudos empíricos realizados por Peter Grabosky e John Braithwaite na análise dos regimes regulatórios na Austrália, entre os quais o registrado na obra *Of Manners Gentle: enforcement strategies of Australian business regulatory agencies* (GRABOSKY, BRAITHWAITE, 1986). A obra de 1986 conclui que a grande maioria das agência responsáveis pela aplicação de regulações na Austrália prefere compreender que sua principal função é a de educar e persuadir, evitando a adoção de posturas adversariais na abordagem dos regulados, mesmo considerando de vital importância a existência de poder para a instituição de punições, caso não possam obter a cooperação.

[83] "This conclusion is not grounded in any assumption that business people are cooperative in nature; rather, the payoffs in the regulation game make cooperation rational until the *Responsive Regulation* other player defects from cooperation. The motivational account of the firm is of a unitary actor concerned only with maximizing profit". (AYRES, BRAITHWAITE, 1992, p. 21-22).

Uma das críticas opostas à regulação responsiva é o fato de ela ter sido desenvolvida e aplicada inicialmente no âmbito de economias desenvolvidas. Entretanto, conforme assevera Braithwaite, é incorreto pensar que a regulação responsiva seja uma estratégia regulatória não aplicável a países com economias em desenvolvimento (BRAITHWAITE, 2006). O autor (BRAITHWAITE, 2006, p. 886) reforça que a abordagem da regulação responsiva pode ser de grande valia para economias em desenvolvimento que contem com menor capacidade de controle, justamente porque a regulação responsiva parte do pressuposto de que nenhum governo tem a capacidade de estabelecer efetivo *enforcement* para todas as leis. E lida com o estímulo à responsividade e com a repartição da função de fiscalizar como meios de otimizar os recursos existentes, podendo funcionar como instrumento de contingenciamento de escassez de recursos. Assim, em linhas gerais a responsividade é a linha condutora para a efetividade, consistindo, ainda, num ideal democrático (BRAITHWAITE, 2006, p. 889).

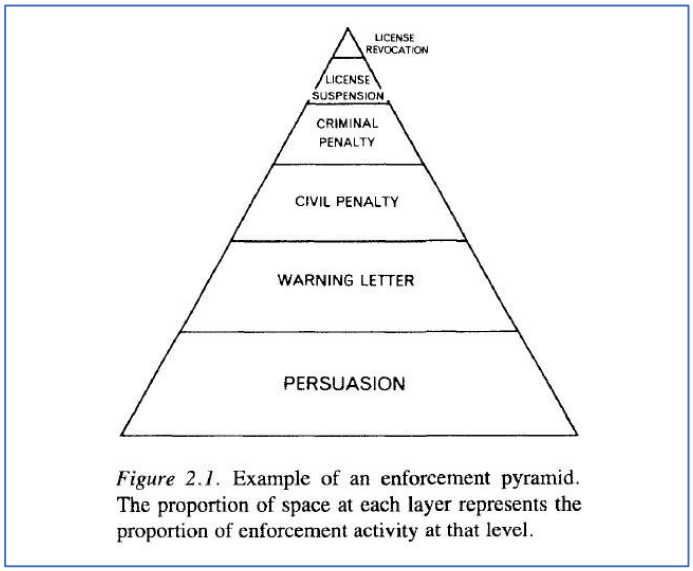

Figure 2.1. Example of an enforcement pyramid. The proportion of space at each layer represents the proportion of enforcement activity at that level.

Figura 1 – Fonte: AYRES; BRAITHWAITE (1992, p. 35)

Desde o avanço da internet e da facilidade e comunicação, os problemas que afetam os Estados nacionais passaram a ser recorrentes para uma larga gama de Estados, tendo natureza transnacional (SLAUGHTER, 2004). Dessa maneira, vive-se numa era de governança transnacional (BRAITHWAITE, 2006, p. 890), em que organizações internacionais que estabelecem relações de rede com uma diversidade de países são importante fonte regulatória e podem contribuir para a fiscalização e reforço de normas. Nesse cenário, a regulação responsiva mostra-se como um caminho para os países em desenvolvimento de suprir a baixa capacidade de intervenção explorando a formação de uma rede de governança com agentes não estatais, e se necessário, transnacionais, para o alcance dos objetivos regulatórios.

> The core idea of responsive regulation as a strategy actually has special salience for resource-poor states. This is the idea that no regulator has the resources to consistently enforce the law across the board and therefore limited enforcement resources need to be focused at the peak of an enforcement pyramid. Networking escalation is an interesting elaboration of how to make the most of limited regulatory capacity. (BRAITHWAITE, 2006, p. 896)

Impende destacar, que a regulação responsiva consiste numa metaestratégia, ou seja, numa estratégia para escolher estratégias de *enforcement*, conforme esclarece Braithwaite (2016)[84], que se pauta na máxima de dar preferência sempre a mecanismos de *enforcement* menos coercitivos num momento inicial, e eventualmente escalar para a aplicação de mecanismos mais coercitivos, até que a situação-problema seja solucionada. Assim, a regulação responsiva atua no contingenciamento de riscos e remediação de problemas que motivaram a regulação como o médico, que por tentativa e erro prescreve tratamentos a um paciente doente, até que esse encontre a cura. Como tal, demanda o melhoramento contínuo[85], a constante medição e busca por adoção de medidas de *enforcement* adequadas e mais efetivas para a obtenção dos resultados almejados. Embora nem a Autoridade Nacional de Proteção de Dados brasileira (ANPD), nem a autoridade de privacidade australiana (*Office of Australian Information Commissioner* – OAIC) adotem expressa e explicitamente a regulação responsiva, a sua forma de atuação é pautada nos elementos dessa modalidade de regime regulatório.

Numa realidade dinâmica e cambiante o contingenciamento de riscos fica cada vez mais difícil e exige maior atenção. No contexto da globalização e da permeabilidade de fronteiras comunicacionais e físicas os Estados nacionais passam a repartir os riscos com os particulares, atuando com relação a eles de forma responsiva e instituindo regimes regulatórios pensados para colocar os particulares na posição de colaboradores para o alcance o interesse público fomentado na norma reguladora. Ao mesmo tempo em que mudam a perspectiva da regulação, de comando e controle, para a cooperação e responsividade, os Estados admitem implicitamente a sua incapacidade de exercer a fiscalização e o controle sozinhos, e compelem os particulares a atuarem nessa seara. E essa instituição de uma rede de escalonamento de reforço à norma, ao lidar com problemas transnacionais, de maneira cada vez mais recorrente os Estados nacionais têm apostado na cooperação internacional, com entes estatais e não estatais fora do seu território, inovando a aparência da pirâmide de *enforcement*.

---

[84]"[...] Responsive regulation is a meta-strategy for arranging problem-solving strategies in a hierarchy of coerciveness and then implementing a presumptive preference for trying the less coercive solutions first, moving up the hierarchy of strategies until one of them succeeds in fixing the problem." (BRAITHWAITE, 2016, p. 1-2).

[85] "[...] Responsive regulation is regulation that expects and sometimes requires continuous improvement. That means continuous improvement in discovering lower cost ways to achieve regulatory outcomes and continuous improvement in achieving better outcomes." (BRAITHWAITE, 2016, p. 15).

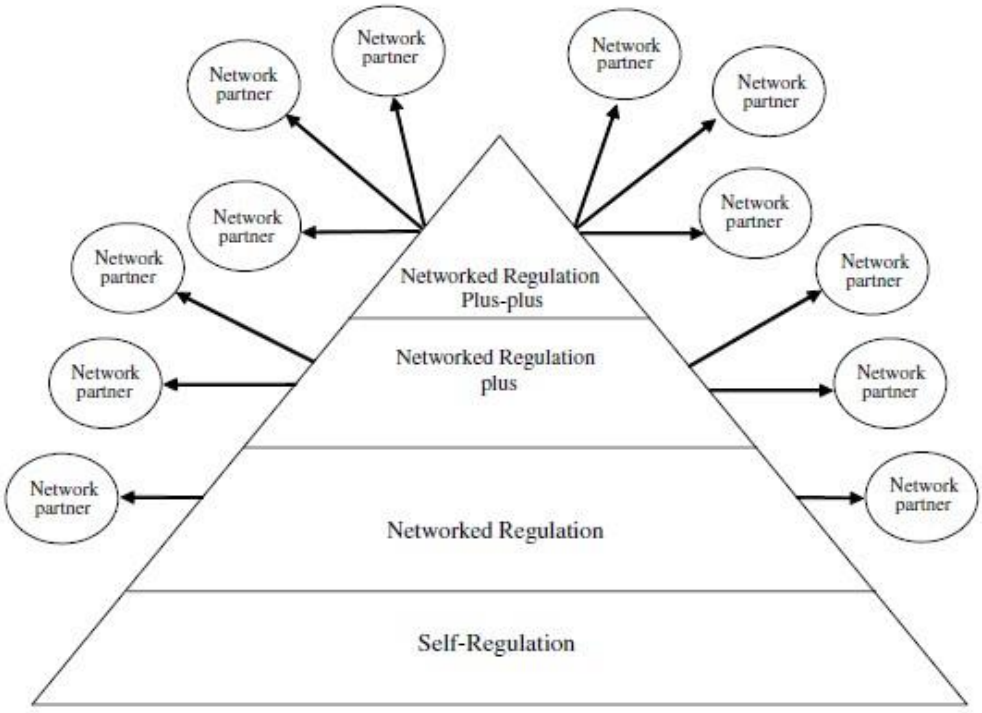

Figure 2. *A responsive regulatory pyramid for a developing economy to escalate the networking of regulatory governance.*

Figura 2- BRAITHWAITE, 2006, p. 890

A LGPD adota a estratégia de reforço à adoção de melhores práticas e instituição de programas de governança de dados pelos agentes de tratamento (arts. 50 e 51, LGPD*).* Aplicando a perspectiva da cooperação e do estímulo à responsividade, a LGPD institui um panorama regulatório em que cada agente de tratamento é corresponsável pelos tratamentos de dados pessoais feitos pelos seus parceiros comerciais, a partir da relação com eles firmada. Assim, cada agente de tratamento tem o dever de tomar medidas razoáveis para assegurar que seus parceiros estejam também em conformidade com a LGPD (seja pela prévia avaliação de riscos na parceria, pela condução de processos de *due diligence* – no caso de outras empresas – ou *background check* – no caso de parcerias com pessoas físicas – seja pela adoção de Acordos de Tratamentos de Dados, estabelecendo a responsabilidade de cada um no que tange o tratamento de dados pessoais e os deveres a fim de proteger os dados pessoais em tratamento, assim como prevendo a deleção após o esgotamento da finalidade de tratamento). Os agentes numa cadeia de tratamento possuem responsabilidade solidária perante o titular de dados, tendo direito de regresso em relação ao agente que tiver dado causa ao dano, se comprovarem não possuir responsabilidade no evento danoso e terem tomado todas as medidas administrativas e técnicas razoáveis para a atividade que desempenham (arts. 42-49, LGPD).

Ao delimitar conceitos basilares do sistema de proteção de dados que enuncia, a LGPD, no artigo 5º inclui as pessoas jurídicas de direito público como agentes de tratamento. Dessa forma, a Administração Pública, seja ela direta ou indireta também terá os processamentos de dados pessoais que fizer, que não estejam incluídos nas exceções previstas no artigo 4º da LGPD, submetidos às exigências e limitações que a proteção de dados pessoais impõe. A submissão às exigências da LGPD representa um desafio ainda maior para o Poder Público, responsável por fiscalizar e regular um segmento em que também figura como regulado. O controle dos agentes de tratamento de dados, tão enfatizado pela doutrina ao abordar a LGPD representa encargo desafiador para o Estado, ao passo que os próprios agentes estatais são alvo da viciação de vontade decorrente da interação com as plataformas, seus componentes e derivados (e da necessidade de adequação à LGPD), o que reverbera na construção da vontade administrativa. Soma-se a isso a dificuldade regulatória atinente à dinamicidade das novas tecnologias, que são meios de entrada para tratamento de dados, sem mencionar o fato de numa economia em rede, a maioria dos tratamentos de dados pessoais em meio digital ocorrer envolvendo fluxos transfronteiriços.

Ante o cenário exposto, é inegável a importância que os atores não estatais possuem na efetiva regulação de um setor, especialmente com o incremento da tecnologia que permite o encurtamento de distâncias comunicacionais e territoriais (GRABOSKY, 2013, p. 117). Entretanto, cumpre rememorar a retroalimentação entre lei e interesses de grandes empresas (o *lobby* de grandes empresas impulsiona a criação de leis que assegurem condições que são do seu interesse, e somente a partir da instituição de cobranças legais essas iniciativas de regulação privada são efetivadas – vale reforçar, a autorregulação privada não acontece espontaneamente a não ser que represente vantagem competitiva em alguma esfera – financeira, fidelização do cliente, reputacional, entre outras), num processo de captura da regulação, no dizer de Grabosky e Braithwaite (1986, p. 198).

Graças a essas ferramentas tecnológicas opiniões podem ser compartilhadas de maneira muito veloz e impactar na reputação e, consequentemente, na escolha das pessoas por um dado fornecedor ou outro. A preocupação com a reputação amplia, ainda, o poder de grandes empresas em relação a sua cadeia de fornecedores, no que tange à fixação de níveis de qualidade para produtos e serviços. O fator tecnológico, atrelado à conexão do mercado em rede, com fluxos comerciais transnacionais, cria um ecossistema de regulação mais complexo, por contar com esse significante papel desempenhado pelos atores não estatais na persuasão e na modulação comportamental recíprocas. Tendo em vista essa constatação, autores como Peter Grabosky e Neil Gunningham sugerem que a pirâmide de resposta regulatória de Ayres e

Braithwaite, bidimensional e centrada na ação estatal, estaria defasada, sendo mais acertado tratar de um panorama de resposta regulatória tridimensional, no formato de um tetraedro[86], para comportar as respostas desses atores não estatais (GRABOSKY, 2013, p. 120-121). O tipo de regulação proposta por Gunningham e Gabosky é denominada de *Smart Regulation* (BALDWIN; BLACK, 2008, p. 65), e, ao apostar numa resposta regulatória mais holística, enfrenta desafios como a necessidade de criar uma rede regulatória e um processo de coordenação de respostas através de diferentes identidades culturais e políticas, cuja execução não é fácil.

Em que pese a constatação de que de fato faz-se necessária uma rede de cooperação entre agentes estatais e não estatais, e em uma dimensão transnacional, entende-se que essa demanda é atendida como consequência do desenho de *enforcement* local e pelo compartilhamento de um problema comum entre os agentes transnacionais, não devendo ser formalmente instituída como estratégia de reforço à lei, pela dificuldade de o Estado controlar a existência de efetiva cooperação ou não por parte de entidades internacionais, não podendo contar com essa variável para o monitoramento e melhoramento da política pública de proteção de dados.

No contexto da sociedade informacional (DE LIMA, 2020; CASTELLS, 2013), a efetividade da regulação da proteção de dados como direito autônomo depende mais da qualidade dos mecanismos de *enforcement* disponíveis para a concretização do direito pelos titulares dos dados, do que da amplitude dos direitos incluídos na norma que dá início à regulação e sustenta a política pública. Para estimular a capacidade de resposta dos regulados e criar um ambiente cooperativo, determinadas características devem ser observadas nas estratégias de *enforcement*, como a transparência, uma abordagem dialógica por parte do regulador, a adoção de reforço liderada pelo regulador e o escalonamento progressivo das punições. Alguns elementos da regulação responsiva permitem que o Estado nacional, por meio da Autoridade de Proteção de Dados, operacionalize a política pública, compartilhando responsabilidades com partes privadas. Essa distribuição de responsabilidades é vital para a eficácia da política pública, pois o Estado atua como regulador e regulado no campo da proteção

[86] "[...] Unlike the Ayres-Braithwaite Pyramid, which is two dimensional, the tetrahedron is a three dimensional space. To the extent that a given regulatory instrument entails elements of state, self-regulatory, or third-party activity, it can be depicted as a form within the tetrahedron. Is vertical location within the tetrahedron will reflect the degree of coerciveness with which it impacts on the organizational life of the regulatee; its horizontal location will reflect its institutional (or interinstitutional hybrid) form. Theoretically, any regulatory instrument can be situated within the space, depending upon its institutional sponsor (or sponsors) and its coerciveness. Any location on or within the tetrahedron can be represented by precise co-ordinates, and is thus amenable to formal (i.e. quantitative) representation. This may one day permit more precise modelling of regulatory systems, as well as a more sophisticated degree of hypothesis testing and theory building." (GRABOSKY, 2013, p. 120).

de dados. Além disso, a existência de mecanismos disponíveis para que os titulares de dados busquem administrativamente a solução para a violação de seus direitos, sem custos, milita em favor da natureza democrática do direito à proteção de dados e de sua introjeção na cultura.

Na sociedade informacional, o aprimoramento dos sistemas jurídicos tende a ser cada vez mais orientado por diretrizes internacionais, *soft laws* definidas em instituições supranacionais. A ubiquidade computacional gerada pela Internet, com a dicotomia entre o digital e o material, rompe a distinção entre público e privado, bem como entre governo e sociedade, de tal forma que os problemas que emergem do contexto narrado somente serão contingenciados com a participação do Estado e da coletividade (empresas privadas e pessoas físicas, atores não estatais). O Estado não é mais o único repositório do poder de vigilância. Na verdade, ele se torna mais alvo do que executor de vigilância (observe o avanço das audiências virtuais, dos processos eletrônicos e de muitas outras execuções de serviços públicos intermediados por soluções tecnológicas, por plataformas digitais, muitas vezes não produzidas, nem mantidas pelo Estado ou por entidades públicas). As plataformas digitais que hospedam esses sistemas, por meio dos quais o Estado está atuando, têm acesso lícito ou ilícito aos dados produzidos.

Importante frisar que os elementos de regulação responsiva evidenciados nesta seção parecem ser dotados da vocação para conduzir a regulação do tratamento de dados pessoais e a política de proteção de dados para a efetividade, estabelecendo um sistema de proteção aos direitos do titular de dados pessoais. Sob a perspectiva da política pública, entende-se que a regulação responsiva é o caminho mais profícuo, num cenário em que os Estados nacionais têm poder relativizado, tendo que lidar com entes privados e forma mais paritária. No próximo capítulo, aborda-se com maior vagar aspectos normativos e práticos da regulação instituída a partir da LGPD, suporte normativo da Política Nacional de Proteção de Dados Pessoais brasileira.

4 PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL: da elaboração da LGPD à implementação da Política Nacional de Proteção de Dados

Este capítulo é dedicado a contextualizar a *Lei Geral de Proteção de Dados* brasileira (LGPD, *Lei Federal nº 13.709/2018*) como suporte normativo à Política Nacional de Proteção de Dados Pessoais brasileira. Argumenta-se sobre a existência de uma implementação em curso de uma política pública, tratatando-se das estratégias e especificidades do modelo brasileiro, muito inspirado no *General Data Protection Regulation - GDPR*, por um lado como resultado de um debate convergente transnacional (DONEDA, 2020), por outro como a incorporação de "melhores padrões" para alcançar o pertencimento e manter os negócios e a economia brasileiros competitivos em um mundo transnacional em rede (VALADARES, 2020).

Depois de explorar a estrutura projetada pela LGPD e como ela foi executada até o momento, o capítulo argumenta que apesar da aparente vocação da política pública estabelecida para promover os direitos da personalidade, a limitação no *enforcement* devido à forma como o Brasil tem desenvolvido essa política tende a resultar em inefetividade para esse fim, especialmente pelo predomínio da litigância judicial como principal meio disponível ao titular de dados para assegurar seu direito à proteção de dados. Esse argumento detalha como a defesa da proteção de dados, sob a perspectiva do titular de dados (titular também do corpo digital) se baseia na judicialização e como essa opção de efetivação do direito, apesar de válida, é elitista e excludente, transformando a proteção de dados e a autodeterminação informativa em direitos para determinadas pessoas e em proteção apenas aparente para outras.

Além disso, a LGPD, como maioria das normas no campo da proteção de dados, foca na segurança da informação para o estabelecimento de um standard mínimo para continuidade dos fluxos de dados. Esse enfoque pode induzir o cumprimento de procedimentos por parte dos agentes de tratamento de dados sem o compromisso com os direitos da personalidade e com a proteção do corpo digital. Isso é perigoso porque pode criar uma falsa compreensão da realidade que leva os indivíduos a se sentirem seguros e "anestesiados", tornando-se passíveis de manipulação, por reduzirem o nível de alerta quanto aos tratamentos dos seus dados. Prejudica, ainda, a intenção de educação para a promoção de uma cultura de privacidade e proteção de dados.

A análise é feita por meio do estudo da lei, das instituições envolvidas na política pública e das decisões judiciais tomadas pelo Supremo Tribunal Federal (STF) e pelo Superior Tribunal de Justiça (STJ), de 2020 (ano em que a LGPD entrou em vigor) a 2022, com base na LGPD. Neste ponto, impende destacar que um dos objetivos da pesquisa era a análise de

decisões administrativas proferidas pela ANPD. Entretanto, a Autoridade não proferiu nenhuma decisão em sede de Processo Administrativo no recorte temporal estabelecido[87].

Em virtude de limitações enfrentadas na execução da pesquisa, alguns pontos não foram abordados com a profundidade almejada. Entre as limitações, elenca-se a ausência de campo de análise robusto no Brasil, ao passo que a política pública de proteção de dados brasileira segue em fase de implementação, representando uma versão ainda imatura de ações desenhadas para o fortalecimento da cultura de privacidade e proteção de dados no país. Assim, utilizou-se de outras pesquisas para subsidiar os resultados. A tese se valeu da pesquisa *LGPD nos tribunais*, conduzida pelo IDP / CEDIS e pelo JusBrasil para observar as tendências da judicialização da proteção de dados com base em decisões de tribunais estaduais e de Cortes federais em primeira e segunda instância. Pela exiguidade do tempo, utilizou-se a pesquisa "*Privacy Culture"* (edições de 2021 e de 2022) para análise a do nível de adesão dos regulados às exigências da LGPD.

Importante enfatizar que a tese se debruça na investigação da regulação alinhada às Teorias do Interesse Público, que podem ser classificadas de acordo com a abordagem adotada para definir o conteúdo desse interesse público: abordagem econômica, abordagem social (ou orientada por valores), e abordagem de controle de riscos (WINDHOLZ, 2018, p. 36 - 42). Ademais, há que se ter em conta que a regulação proposta pela LGPD é justificada pelo alcance do interesse público tanto no sentido de promover valores, notadamente pela ênfase dada em princípios que devem orientar o tratamento de dados pessoais, assim como nos direitos fundamentais a serem promovidos, quanto no sentido de controlar riscos emergentes da sociedade informacional. Verifica-se com a possibilidade de requerimento por parte da ANPD de relatório de impacto à proteção de dados quando atividades de tratamento tiverem como base legal o legítimo interesse (art. 10, §3º, da LGPD), assim como na necessidade de avaliação de impacto para atividades de tratamento que representem maior probabilidade de ocorrência de uma violação e que tenham extensão maior, resultando em ampla repercussão de eventual violação à proteção de dados.

[87] Vide página da ANPD, abaixo do título "Decisões em Processos Sancionadores": https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em 20 Jan. 2023.

4.1 LGPD como suporte normativo da Política Nacional de Proteção de Dados Pessoais

O gérmen do direito à proteção de dados no sistema jurídico brasileiro remonta à década de 1970. Conforme elucidam Danilo Doneda e Rafael Zanatta[88] (2022, p. 42-44), foi durante a ditadura militar (1964-1984) que o movimento acadêmico em prol da constitucionalização da privacidade teve o seu fortalecimento, em face das sucessivas violações aos direitos fundamentais promovidas pelos militares no poder. Doneda e Zanatta relatam que um projeto apresentado pelo governo militar em 1975 para a instituição de um banco de dados nacional unificado – Registro Nacional de Pessoas Naturais – RENAPE – reunindo dados oriundos de diferentes bases, com as bases estaduais de Registro Geral, de Cadastros de Pessoas Físicas, a de inscrição no Instituto Nacional de Seguridade Social, em uma base com informações biométricas dos cidadãos, motivou a discussão acerca de boas práticas de proteção de dados. A proposta de instituição do RENAPE provocou a mobilização de diversos intelectuais e profissionais de empresas de tecnologia contra a sua aprovação e instituição (DONEDA, ZANATTA, 2022, p. 43). O fornecimento de dados por parte dos cidadãos seria instituído de maneira obrigatória, caso o RENAPE fosse aprovado.

A oposição de diversos ativistas ao RENAPE, como Maria Tereza Oliveira, Ethevaldo Siqueira e Renè Ariel Dotti, foi registrada em jornais de grande circulação como o *Estado de São Paulo,* em discursos públicos e em periódicos científicos especializados como a *Revista Dados,* e era centrada em argumentos sobre o potencial nocivo da constituição de um banco de dados dessa magnitude, não somente por ameaçar os cidadãos, no que tange a sua privacidade e liberdade, mas por ameaçar o próprio capitalismo, assim como o fato de que nenhum interesse público poderia justificar a sistemática violação da privacidade humana (DONEDA, ZANATTA, 2022, p. 42-43). Vale lembrar que a ameaça do comunismo foi o principal argumento que tentava legitimar o golpe de 1964 que levou o país à ditadura militar por vinte anos. Os ativistas invocavam o reconhecimento da vida privada como um direito humano na *Declaração Universal dos Direitos Humanos* e o fato de muitos países europeus como a Bélgica, a Itália, a Alemanha e Portugal terem rejeitado propostas similares à do RENAPE, por considerarem os riscos envolvidos para os direitos fundamentais.

Consoante destacam Doneda e Zanatta (2022, p. 42) as ideias elaboradas em oposição ao RENAPE traziam proposições bastante influenciadas pela *Lei de Proteção de Dados*

[88]DONEDA, Danilo; ZANATTA, Rafael. *Personality rights in Brazilian Data Protection Law: a historial perspective.* In.: ALBERS, Marion; SARLET, Ingo Wolfgang (Eds.). **Personality and Data Protection Rights on the Internet: Brazilian and German approaches.** Cham: Springer, 2022. Pp. 35-54.

Francesa, sendo que o primeiro projeto de lei brasileira de proteção de dados, datado de 1977 e proposto por José Faria Lima (Arena), se espelhava nas diretrizes contidas na lei francesa, inclusive com a proposta de criação de uma Autoridade Nacional de Proteção de Dados, seguindo o modelo da *Commission Nationale de 'lInformatique et des Libertés (CNIL).* No mesmo ano, o Senador Nelson Carneiro (MPB) foi autor de projeto de lei centrado na proteção de informação computacional. Entretanto, ambos os projetos foram rejeitados pelo Congresso Nacional.

A discussão sobre o direito de privacidade e a sua singular importância para o desenvolvimento do indivíduo se fortaleceu e na década de 1980 outros projetos de lei nesse sentido foram propostos (*Projeto de Lei nº. 4.646/1984*, de autoria de Cristina Tavares (PMDB), que previa o direito à privacidade a aos dados pessoais, e *Projeto de Lei nº. 4.766/1984*, de autoria de José Jorge (PDS), que previa o direito à privacidade e de acesso a informações) até o início da Constituinte em 1986, que resultou na consagração de diversos direitos da personalidade na *Constituição Federal* de 1988, como mencionado por Doneda e Zanatta (2022, p. 43). A *Constituição Federal* de 1988 trazia desde a sua promulgação o direito à intimidade e à vida privada (Art. 5º, X) como direito fundamental, além de contemplar direitos de acesso e correção de informações pessoais (*habeas data* – Art. 5º, LXXII) com o mesmo status de fundamentalidade.

No sistema jurídico brasileiro a tutela da privacidade encontra-se consignada no art. 5º, X e XII da Constituição Federal (BRASIL, 1988), quando trata da preservação da vida privada e do sigilo das comunicações como direitos fundamentais. Observa-se, assim, que a tutela da privacidade tem por objeto a integridade moral do titular, sua vida íntima, com foco no sigilo das informações pertinentes à sua esfera privada. A privacidade se comunica mais diretamente com a proteção à honra e à intimidade. Ocorre que essa proteção que diz respeito mais à intimidade, e é bastante ligada à noção de sigilo, torna-se insuficiente em face de toda uma representação de subjetividade pelo corpo digital no âmbito da sociedade informacional. As interações no andamento das relações de trabalho, de estudo e interpessoais são intermediadas por plataformas digitais e travadas de maneira remota. Tem-se toda uma rede de relacionamentos e de mecanismos para que se possa trabalhar, estudar, comprar e realizar uma larga monta de atividades cotidianas remotamente. Mais do que nunca há que se falar num sujeito digital, que possui um corpo digital, composto por todos os dados e informações extraídos da sua interação com as plataformas digitais.

Após o advento da *Constituição Federal* de 1988 diversas leis federais incrementaram a tutela da privacidade e da proteção de dados de maneira pulverizada[89] no sistema legal brasileiro, tais como o *Código de Defesa do Consumidor* (*Lei Federal nº. 8.078/1990*), da *Lei dos serviços de telecomunicações* (*Lei Federal nº. 9.472/1997*), da *Lei de Direitos Autorais* (*Lei Federal nº. 9.610/1998*), do *Código Civil* (*Lei Federal nº. 10.406/2002*), *Lei de Acesso à Informação* (*Lei Federal nº. 12.527/2011*), e do *Marco Civil da Internet*[90] (*Lei Federal nº. 12.965/2014*). Dessa forma, pode-se dizer que a LGPD teve o papel de harmonizar e compilar tutelas instituindo uma coerente efetivação normativa da proteção de dados no sistema legal brasileiro[91].

Merece destaque, consoante enfatizado por Doneda e Zanatta (2022, p. 49), o fato de o Brasil ter participado de Grupo de Trabalho no Mercosul (SGT13 – Comércio eletrônico e certificação digital), por cinco anos, preparando um documento com diretrizes a serem adotadas pelos países do bloco econômico, àquele tempo formado por Brasil, Paraguai, Argentina e Uruguai, atinentes à proteção de dados. O documento foi assinado por todos os membros em 2010 e seria avaliado posteriormente pelo comitê executivo do Mercosul antes de sua eventual promulgação. Mesmo que o documento não tenha sido avaliado para promulgação, tratou-se do primeiro documento endossado por autoridades brasileiras reconhecendo a necessidade de se estabelecer um panorama de proteção de dados pessoais coerente e coeso no sistema jurídico brasileiro (DONEDA, ZANATTA, 2022, p. 49).

A LGPD, suporte normativo da Política Pública de Proteção de Dados brasileira, resulta, assim, de longo período de negociações[92]. Em 2010 tem início o debate mais profícuo[93] com o

---

[89] Instituindo um sistema de proteção firmado como um *"patchwork model"*, nas palavras de Danilo Doneda e Rafael Zanatta (2022, p. 44).

[90] Laura Schertel Mendes e Danilo Doneda entendem que o Marco Civil da Internet afirma um "direito fundamental à proteção de dados" (tradução nossa), além de estabelecer o consentimento como base legal fundamental para a aplicação da lei (DONEDA, MENDES, 2014, p. 3-20). Ademais, o Marco Civil da Internet é uma lei autoral, por não encontrar leis similares no plano internacional e possui tratamento mais rigoroso para processamentos de informações dos usuários da internet, tendo como base legal única, ou seja, como situação em que esse processamento é presumidamente legítimo e legal, o consentimento, livre, expresso e informado do usuário (VALADARES, 2020, p. 115-150).

[91] Enfatizando esse papel que a LGPD desempenhou de dar corência ao microssistema regulatório da proteção de dados, vale a leitura da tese de Bernardo Grossi: "Foi exatamente a partir da LGPD que esse microuniverso regulatório recebeu uma sistematização mais clara e segura." (GROSSI, 2022, p. 80).

[92] A presente contextualização é realizada com subsídio em excelente e minuciosa pesquisa realizada pelo Observatório da Privacidade" da organização "Data Privacy BR". Para maiores informações sobre a trajetória de negociações, recomendo o acesso ao segmento "Memória da LGPD", linha do tempo montada pelo "Observatório da Privacidade" da organização "Data Privacy BR", devidamente referenciado. A linha do tempo conta com entrevistas a atores que tiveram papel relevante ao longo das tratativas que resultaram na LGPD. Disponível em: https://observatorioprivacidade.com.br/memorias/. Acesso em 28 Ago. 2022.

[93] Conforme registrado no "Memória LGPD", em entrevista com Rafael Zanatta, o primeiro projeto a respeito da proteção de dados de pessoas naturais remonta à 1978, em uma reação à projeto de lei que propunha Sistema

propósito de elaboração de projeto de lei sobre o tema, sendo colhidas sugestões por meio de blog mantido pelo Ministério da Justiça até 2011. O Anteprojeto sobre o qual se debruçava a consulta em comento foi escrito por Danilo Doneda[94], que coordenou os trabalhos da *Secretaria Nacional do Consumidor*, e Laura Schertel, membros da primeira formação do Conselho Nacional de Proteção de Dados e da Privacidade (CNPD), integrante da Autoridade Nacional de Proteção de Dados (ANPD). O primeiro Projeto de Lei que versa sobre o tema é datado de 2012 – *Projeto de Lei (PL) nº. 4060/2012*, proposto pelo Deputado Federal Milton Monti.

O escândalo a respeito das atividades de espionagem promovidas por agências internacionais[95] de segurança vem à luz em 2013, impulsionando os debates sobre o tratamento de dados pessoais e sobre os limites da vida privada e do espaço privado, sobretudo quando a internet é o ambiente de interação. Esse escândalo acaba por militar a favor da aprovação da *Lei Federal nº. 12.965, de 24 de abril de 2014 – Marco Civil da Internet*. E em 2014 o Senador Antônio Carlos Valadares apresenta o *Projeto de Lei do Senado - PLS nº. 131/2014*, fruto de discussões que tiveram lugar na *Comissão Parlamentar de Inquérito (CPI) da Espionagem*, e o Senador Vital do Rêgo apresentou *PLS nº. 181/2014*. O então Senador, Aloysio Nunes, foi designado relator de projetos que estavam em tramitação, ficando responsável por condensar as sugestões colhidas em consultas públicas e nos Projetos. Dessa forma, após um trabalho de análise crítica e compilação de informações, o Senador em questão apresentou *Projeto Substitutivo ao PLS 330/2013*, que foi aprovado na *Comissão de Ciência e Tecnologia*[96].

Enquanto avança a tramitação do *PLS nº. 330/2013*, o *PL nº. 4060/2012* não tem o mesmo trajeto na Câmara dos Deputados. Dilma Rousseff, em um dos seus últimos atos, enviou para a Câmara dos Deputados Anteprojeto de Lei, que contava com contribuições colhidas nas consultas públicas promovidas pelo Ministério da Justiça, em 12 de maio de 2016. O Anteprojeto passa a tramitar na Câmara, apensado ao *PL nº. 4060/2012* como *PL nº. 5276/2016* (após todas as contribuições colhidas em audiências públicas e reuniões com a organizações da

---

Nacional de Pessoas Naturais – RENAPE, na época do Governo Geisel. Essa tentativa restou fracassada e contava com o apoio de técnicos da IBM. As primeiras formulações após essa iniciativa começam por pressão internacional sobre o Brasil, a partir de meados de 2000, após a promulgação da lei de proteção de dados argentina, com o intuito de disciplinar o tratamento de dados pessoais, especialmente para uso no comércio eletrônico no âmbito do Mercosul.

[94] Em 04/12/2022 Danilo Doneda faleceu, momento em que já havia avançado nos registros da pesquisa. Seu trabalho foi de extrema relevância para a normatização da proteção de dados no Brasil, assim como a sua postura profissional e sua militância, que seguem inspirando os estudiosos da proteção de dados a lutarem pela efetividade desse direito.

[95] Com as denúncias realizadas por Edward Snowden, ex-administrador de sistemas da CIA e ex-analista da NSA.

[96] Vide reportagem contextualizando essa aprovação. Disponível em: https://www12.senado.leg.br/noticias/materias/2015/10/13/marco-regulatorio-para-protecao-de-dados-pessoais-e-aprovado-pela-cct-e-segue-para-tres-outras-comissoes. Acesso em 28 Ago. 2022.

sociedade civil, este é o *PL* que fornece o texto inicial da LGPD). Empresas e organizações da área de tecnologia e entidades da sociedade civil entram no debate, com pontos de vista divergentes e com movimentações em prol de sentidos diversos da lei. O Relator dos PLs na Câmara, Deputado Orlando Silva, conduz a tramitação de modo que eles passem por quatro Comissões, atraindo a aplicabilidade de norma regimental que autoriza a criação de Comissão Especial centrada no tema.

Assim, em 26 de outubro de 2016 é criada a *Comissão Especial de Proteção de Dados Pessoais*. Em 06 de dezembro de 2016 essa comissão promove a primeira audiência pública, contando com a participação de representantes da academia, de pessoas jurídicas de direitos público e privado, e da sociedade civil. Conforme descrito nos itens 14 a 16, do segmento "2016-2018: O Anteprojeto chega à Câmara", da linha do tempo "Memória da LGPD"[97],

> 14. Ao todo, a Comissão Especial organiza 11 audiências públicas e 2 seminários internacionais – a última delas no dia 12 de julho de 2017. Organizados por temas, esses encontros ajudam os atores envolvidos a depurar o entendimento sobre diversos conceitos ligados à Proteção de Dados.
> 15. Ao longo de 2016 e 2017, a proteção de dados pessoais é tema central de diversos outros eventos e seminários ao redor do Brasil, como o Workshop de Proteção de Direitos e Indústria de Dados Pessoais promovido pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC).
> 16. Também em 2017, o MCTIC inclui a necessidade da aprovação de uma lei de proteção de dados – assim como a criação ou identificação de um órgão responsável por aplicar a lei – dentro da Estratégia Brasileira para Transformação Digital. (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA).

Em que pese os encontros e audiências mencionados tenham contribuído para arrefecer a tensão de posicionamentos existente entre os diversos setores atuantes nas discussões sobre a regulação da proteção de dados pessoais, o tema não estava suficientemente maduro para a aprovação de um marco legal a respeito. Foi o escândalo da *Cambridge Analytica*[98], que veio à tona em março de 2018, somado ao interesse do governo brasileiro de que o Brasil ingressasse na Organização para Cooperação e Desenvolvimento Socioeconômico (OCDE), que fomentaram a urgência em aprovar o marco regulatório sobre o tratamento de dados pessoais no país. Os interesses econômicos e humanitários dos diversos setores que atuaram nas negociações sobre o teor da norma, geravam uma pressão pela aprovação da lei, mantendo o

---

[97] Disponível em: https://www.observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em 28 Ago. 2022.

[98] O escândalo revelou a utilização de dados de usuários do Facebook como subsídio para feedbacks assertivos disparados por empresa de Marketing com o intuito, bem-sucedido, de modular a vontade dos usuários em diversos processos eletivos aos redor do mundo. Por exemplo na eleição de Donald Trump, nos Estados Unidos, em referendos na Índia, e na saída do Reino Unido da União Europeia, evento conhecido como BREXIT. O documentário "Privacidade Hackeada" (2019) mostra com detalhes as nuances dessa vigilância empregada como meio de modular comportamentos dos usuários da rede social.

Brasil alinhado com tendências internacionais, que passavam a figurar como exigências no mercado global (conectado em rede).

O texto do *PL nº. 5276/2016* é aprovado com unanimidade na Câmara em 29 de maio de 2018, sendo remetido ao Senado em junho do mesmo ano, e aprovado sem modificações. Dessa forma, seguiu para a sanção do então presidente Michel Temer, que sanciona a LGPD em 14 de agosto de 2018, vetando, entretanto, algumas previsões essenciais para a efetividade do sistema de proteção estabelecido pela lei, como por exemplo a criação de uma Autoridade de Proteção de Dados dotada de autonomia técnica e orçamentária. O veto resultou em intenso debate sobre a natureza jurídica dessa autoridade e na criação da ANPD em 2020 (pela *Lei nº. 13.853/2019*), como órgão da Presidência da República, fato que militou em desfavor da efetividade da política pública de proteção de dados.

Por ter contado com diversas colaborações e ser fruto de intensas negociações, é creditada a *LGPD* a qualidade de ser fruto de processo multisetorial de negociações (BIONI, RIELLI, 2021; DONEDA ZANATTA, 2022). Há que se reconhecer que essa multisetorialidade e a multidisciplinaridade na abordagem da proteção de dados e das políticas públicas é desejável e necessária, por serem temas atinentes a uma diversidade de setores (públicos e privados) e por abrangerem atividades variadas. Na prática, são raras as atividades e ofícios que escapam à disciplina do tratamento de dados pessoais no âmbito da sociedade informacional. Imperioso, ainda, concordar com o fato de que a LGPD consagra uma tradição de normatização de direitos da personalidade existente no sistema legal brasileiro, conforme demonstrado, ao passo que reúne num único documento proteções que se encontravam pulverizadas, fragmentadas em uma série de leis federais. Fato também que a tradição jurídica brasileira é influenciada pelo Direito Europeu, de maneira que a forte influência do *GDPR* no texto final da LGPD não representa uma emulação excepcional (ou surpreendente).

Assim, a redação da LGPD acaba por refletir um espelhamento de standards consagrados no *GDPR*, em detrimento de exercício legislativo autoral. Isso ocorre por uma série de fatores já abordados na tese, entre os quais o fato e os fluxos de dados serem transfronteiriços, sendo a sua disciplina e a adoção de medidas para a efetividade de direitos dos titulares desses dados um problema transnacional, que resulta na necessidade de convergência regulatória entre os sistemas normativos dos Estados nacionais. É produto ainda da modificação ocorrida na soberania que passa a ser porosa, permeável à necessidade de pertencimento no mercado global, ligado em rede, para a continuidade das relações comerciais. E com as modificações de políticas econômicas num sentido de menor participação do Estado na economia, e de redução do tamanho da máquina pública, opera-se a diminuição do poder

efetivo do Estado, que também tem o exercício da sua soberania permeado pelo poder econômico e financeiro das grandes corporações e das plataformas.

A ligação crescente entre governos e grandes corporações resulta em desafios regulatórios ainda maiores para a proteção de dados. Estado e plataformas digitais privadas passam a ter paridade de poder. Se aquele detém o poder político, estas detêm o poder econômico e de dominação pela divisão do aprendizado e do conhecimento, influenciando decisivamente nos caminhos políticos dos Estados como meio de assegurar ambientes propícios para seus interesses.

4.1.1 Previsões e tutelas no plano normativo

A LGPD disciplina o tratamento de dados pessoais que não estejam inseridos nas exceções do art. 4º[99], em meios analógicos e digitais, com o objetivo de proteger direitos fundamentais e o livre desenvolvimento da personalidade, conforme previsto em seu art. 1º. Suas determinações devem ser observadas por pessoas jurídicas e naturais, de direito público e privado, que tratem dados pessoais na execução de suas atividades.

---

[99] "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público." (BRASIL, 2018). *Redação vigente em junho de 2023.*

O art. 5º da lei é dedicado a conceituar termos chave para a Política Nacional de Proteção de Dados Pessoais. Entende-se como dado pessoal a "informação relacionada à pessoa natural identificada ou identificável" (BRASIL, 2018). E estabelece a necessidade de observância de maior cuidado e cautela se o tratamento dos dados ocorrer em relação a dados pessoais sensíveis, que são dados que apresentam um potencial de colocar o titular em situação de vulnerabilidade a tratamentos discriminatórios (dados biométricos, sobre origem racial ou étnica, sobre convicção religiosa, opinião política, vinculação à sindicato ou organização de caráter religioso, filosófico ou político, referente à saúde ou vida sexual, por exemplo). A LGPD adota uma diferenciação entre agentes de tratamento, que são classificados em Controladores, caso possuam o poder de decidir sobre o tratamento de dados em análise, e Operadores, quando realizam um tratamento em nome do Controlador (e idealmente conforme as suas orientações). Tratamento de dados pessoais consiste em toda operação realizada com essas informações, conforme art. 5º, X (rol não exaustivo de exemplos de tratamentos, entre os quais constam o armazenamento e arquivamento).

O art. 2º traz os fundamentos da proteção de dados pessoais: respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico, tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas. O art. 3º trata dos requisitos para aplicabilidade das exigências da LGPD e prevê a possibilidade de aplicação extraterritorial, desde que alguma operação com dados ocorra em território nacional, ainda que o agente de tratamento não possua sede no Brasil.

O art. 6º traz princípios que devem orientar o tratamento de dados pessoais: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas. Trata-se de artigo de extrema relevância para a avaliação dos casos concretos, e juntamente com o art. 7º, que aborda as hipóteses que autorizam o tratamento de dados pessoais[100], e art. 11, que traz as hipóteses de

[100] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

autorização para o tratamento de dados pessoais sensíveis[101], compõe o cerne de valores que orientam a proteção de dados no sistema nacional. Essas hipóteses em que o tratamento de

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência
§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência
§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência
[101] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.
§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os

dados goza de presunção de legitimidade são abordadas pela doutrina como “bases legais” de tratamento de dados pessoais.

Quanto às bases legais de tratamento destaca-se que o consentimento é somente uma das hipóteses de autorização do tratamento, e deve ser obtido quanto a finalidades determinadas, de maneira inequívoca e informada, podendo ser revogado a qualquer tempo pelo titular. Em caso de revogação do consentimento, os tratamentos anteriores à revogação serão reputados legítimos. Qualquer alteração quanto às finalidades de tratamento, bem como sobre as operações a serem realizadas devem ser comunicadas ao titular. Bases legais como o legítimo interesse do controlador, ainda que atraia uma necessidade de realização de avaliação quanto aos impactos à privacidade (*Privacy Impact Assessment – PIA)*, seguem obscuras e abrem margem para tratamentos de dados que não atendam necessariamente aos interesses do titular de dados e que vulnerem a sua autonomia e a autodeterminação informativa.

O art. 14 merece destaque, por trazer a disciplina do tratamento de dados pessoais de crianças e adolescentes. A redação do artigo em questão foi alvo de ampla discussão acadêmica, especialmente pela previsão existente no §1º, que aparentemente condicionava o tratamento de dados pessoais ao “consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal”, sendo assim, entendia-se inicialmente que, em regra, a única base legal do tratamento de dados de crianças e adolescentes seria o consentimento. Entretanto, a questão foi sanada após emissão do *Enunciado CD/ANPD nº. 1, de 22 de maio de 2023*[102], esclarecendo que

> O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei. (ANPD, 2023).

Impende salientar, o art. 18 que traz o rol de direitos do titular que impõe aos agentes de tratamento a adoção de canais de comunicação com o mesmo, por meio dos quais ele possa realizar solicitações referentes a esses direitos. Conforme destacado, em âmbito normativo restam pontos nebulosos que demonstram a ausência de real vocação da LGPD para proteger o

---

serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência
I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência
II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019) Vigência
§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019) Vigência

[102] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em 25 Mai. 2023.

corpo digital, das medidas adotadas por plataformas para viabilizar o ciclo da despossessão e o acesso aos dados pessoais como insumos, conforme descrito nos capítulos anteriores.

Quanto ao perfilamento enquanto estratégia de enriquecimento de dados, ou seja, de refinamento de dado coletado como material bruto, vale uma observação adicional: em que pese as normas de proteção de dados em geral contenham preocupação quanto à explicabilidade da operação do sistema de decisão automatizada e com a transparência no tocante aos critérios inseridos na programação para a decisão, permitem que o perfilamento, genericamente considerado, fuja à conformidade com esses princípios. Isso porque ele é operado por inferências construídas pelo cruzamento de informações coletadas pela interação com diferentes plataformas, ou seja, a agregação das informações pode decorrer de tratamentos de dados pessoais realizados por variados agentes de tratamento.

Vale reforçar a racionalidade empregada nas normas de proteção de dados atinente ao direito de revisão de decisões automatizadas que afetem a pessoa natural, comumente previsto em normas de proteção de dados (e inserido na LGPD como um dos direitos do titular de dados pessoais) não alcança a potencialidade lesiva do perfilamento, por refletir o direcionamento de obrigação de prestar esclarecimentos aos agentes de tratamento de dados específicos. E as organizações que utilizam o perfilamento se valem de uma variedade de fontes para subsidiar as atividades de predição ou a tomada de decisão, visando contingenciar riscos aos interesses organizacionais (geralmente ligados a questões financeiras e patrimoniais), como buscas na internet, redes sociais, hábitos de compra, estilo de vida, dados congregados no uso de celulares, imagens de sistemas de vigilância, *IoT,* entre outros.

São relevantes os artigos 42 ao 45, da LGPD, que estabelecem o regime de responsabilidade e de ressarcimento de dados para os agentes de tratamento, prevendo em regra um regime de responsabilidade solidária entre Controladores e Operadores, destacando o dever dos Controladores de oferecerem orientações sobre o tratamento de dados pessoais aos Operadores, e destes de seguirem essas orientações. A responsabilização solidária milita em favor da proteção aos direitos do titular e estimula os agentes de tratamento envolvidos na cadeia de tratamento de dados a se fiscalizarem mutuamente, como medida de contingenciamento de riscos. Os artigos 46 ao 51 focam na segurança e no estímulo à boas práticas de governança de dados.

Por fim, importante destacar o artigo 52, que traz o rol de sanções administrativas aplicáveis pela violação às exigências da LGPD para o tratamento de dados pessoais, a serem apuradas em processo administrativo assegurada a ampla defesa. Entre as penalidades figuram advertência com indicação de prazo para adoção de medidas corretivas; multa simples de até

2% do faturamento do agente de tratamento, limitada à R$50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; 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; 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; proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. O §1º estabelece critério para a aplicação proporcional de forma gradativa, com uma escalabilidade de sanções menos gravosas para mais gravosas, de acordo com o comportamento do ofensor e com sua disposição para reparar danos e sanar as violações. Essa escalabilidade progressiva é ratificada pelo regulamento de dosimetria publicado pela ANPD em maio de 2023. Impende destacar que o produto da arrecadação das multas aplicadas é destinado ao Fundo de Defesa de Direitos Difuso, conforme §5º do art. 52 da LGPD.

Assim, de acordo com a redação da LGPD, os meios existentes para que o titular de dados possa exigir os direitos atinentes à proteção de dados são: diretamente ao agente de tratamento (Controlador ou Operados de dados); por petição à ANPD, após a tentativa de autocomposição com o agente de tratamento; perante órgãos de defesa do consumidor, quando a situação envolver relação de consumo, conforme caracterizada no *Código de Defesa do Consumidor*; e em juízo.

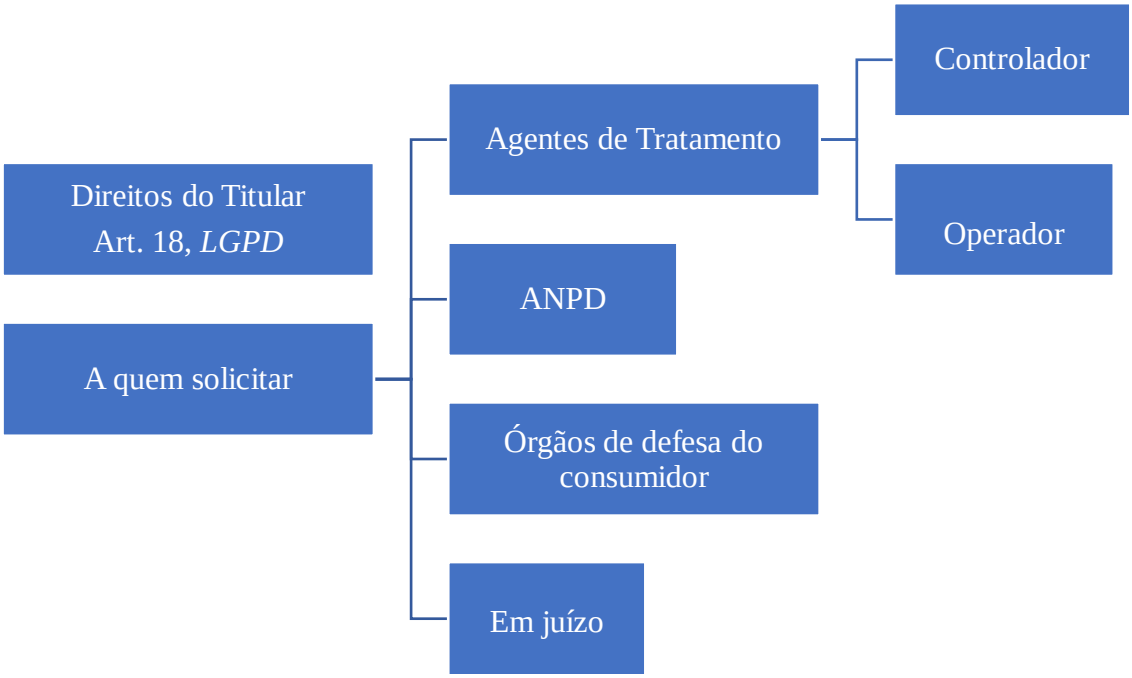

Figura 3- Infográfico Exercício dos direitos do titular - Fonte Autora

4.2 ANPD e CNPD: design de *enforcement* da Política Nacional de Proteção de Dados Pessoais

Para a compreensão da política pública de proteção de dados pessoais como tal, é importante rememorar o conceito de Maria Paula Dallari Bucci de política pública, como

> o programa de ação governamental que resulta de um processo ou conjunto de processos juridicamente regulados [...] visando coordenar os meios à disposição do estado e as atividades privadas para a realização de objetivos socialmente relevantes e politicamente determinados. Como tipo ideal, política pública deve visar a realização de objetivos definidos, expressando a seleção de prioridades, a reserva de meios necessários à sua consecução e o intervalo de tempo em que se espera o atingimento de seus resultados. (BUCCI, 2006, p. 39).

Do conceito acima colacionado é possível extrair três elementos estruturantes de uma política pública, quais sejam, a ação coordenada, a implantação de processos, no sentido de conjunto de ações coordenadas para um fim, e a implantação de um programa, que pressupõe a medição de resultados para oportunizar redirecionamento dos objetivos e prioridades, assim como o melhoramento contínuo. As políticas públicas são o meio através do qual o Estado fomenta a concretização de direitos previstos em lei.

Importante notar que a LGPD traz os objetivos da política pública que propõe linhas gerais para a estruturação do sistema de proteção de dados pessoais. Referida lei prevê o design

preliminar do programa a ser instituído. Entretanto, as ações coordenadas e os processos ficaram sob responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados e Privacidade (CNPD), que integra a Autoridade.

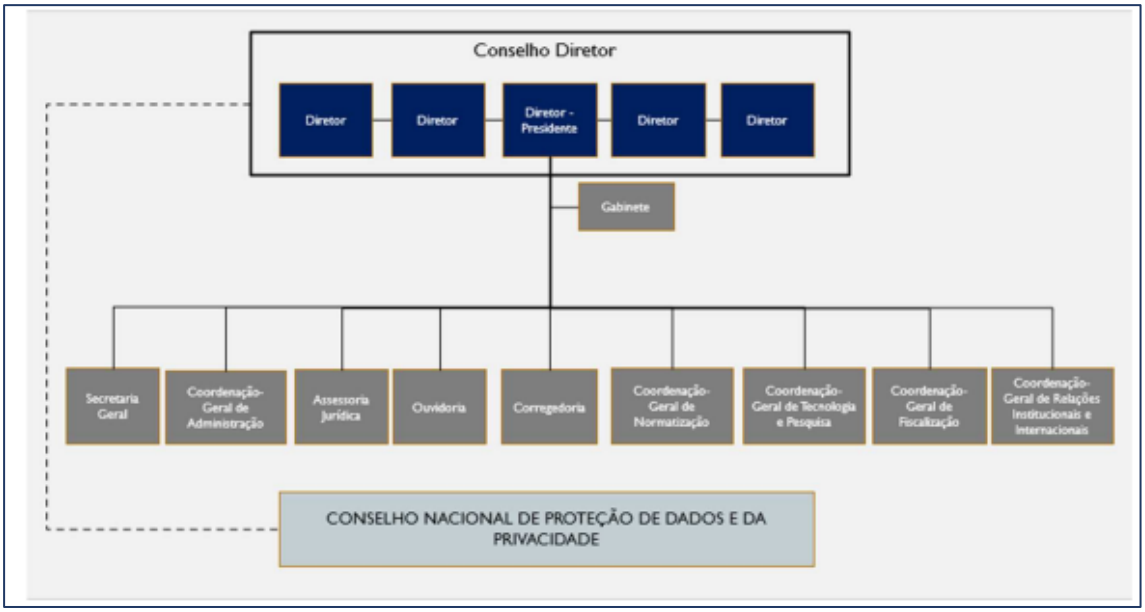

Figura 4 - Organograma ANPD - Fonte: ANPD – Jan. 2023.

Ocorre que houve uma demora na instituição e operação desses órgãos, assim como na modificação da natureza jurídica da ANPD, que foi instituída inicialmente como órgão da Presidência da República. A ANPD acaba de encerrar seu primeiro biênio de operação, e até 2023 atuou mais de maneira a fomentar a cultura de privacidade e proteção de dados, firmando convênios e desenvolvendo ações no sentido de entender as demandas dos agentes de tratamento e as suas dificuldades no processo de adequação às exigências da LGPD. Vale destacar que essa atuação aparentemente incipiente é reflexo da ausência de verba destinada às suas atividades[103]. Conforme informações dispostas na página eletrônica[104] da ANPD os gastos expendidos de 2020 a 2022 foram todos somente para pagamento de diárias dos seus membros, ao passo que a Autoridade seguia vinculada à Presidência da República e desprovida de autonomia financeira e orçamentária. Todos os servidores em atuação na ANPD durante o período eram requisitados de outros órgãos e entes da administração pública, ou remunerados

[103] Conforme destacado pelo Professor Flávio Couto Bernardes na disciplina "Direito e Políticas Públicas" ministrada no âmbito do PPGD PUC-MG no primeiro semestre de 2022, a execução de políticas públicas e o sucesso dos seus resultados estão intimamente conectados com a existência de dotações orçamentárias.

[104] Disponível em https://www.gov.br/anpd/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas-1. Acesso 10 Jun. 2022. Em 2023, com a modificação da natureza jurídica da ANPD, o seu site foi reestruturado, contando com abas de detalhamento quanto ao emprego do orçamento, constado informações somente quanto ao exercício de 2021 e realçando a ausência de autonomia orçamentária vigente quanto ao ano em questão (acesso em 26 Nov. 2023).

por função. Já o CNPD teve os membros da sua primeira formação nomeados somente em agosto de 2021, tendo atuação no mesmo sentido de dar suporte às diretrizes interpretativas da LGPD e das ações educacionais.

A demora na instituição da ANPD, da modificação na sua natureza jurídica para que tenha autonomia financeira, além da autonomia técnica que já possuía, e o baixo investimento financeiro levaram a Autoridade a ter uma ação sutil no reforço da cultura de proteção de dados, tendo realizado somente algumas campanhas educativas e emitido alguns guias orientativos aos agentes de tratamento de dados, além de ter firmado convênios com autoridades internacionais. Todas as ações realizadas são de grande valia, mas não tiveram o potencial de atingir o grande público, de conscientizar e efetivamente difundir a cultura de proteção de dados entre os titulares. Vale frisar que no sistema de proteção instituído no Brasil, a atuação do titular de dados para buscar a concretização do direito à proteção de dados é crucial.

A estrutura reduzida fez com que a ANPD não tivesse a capacidade até 2023 de analisar individualmente as petições de titulares de dados que chegam até ela e de interferir na resolução das violações às exigências da LGPD por agentes de tratamento. Todas as reclamações e denúncias recebidas contra agentes de tratamento são analisadas de maneira agregada com a finalidade de orientar o planejamento da atuação da ANPD (vide fluxo de petição abaixo, disponibilizado no website da ANPD). Dessa forma, na prática, caso o titular não consiga resolver a questão diretamente com o agente de tratamento que tenha violado seu direito, ele só tem como alternativa recorrer à justiça para ver as penalidades previstas na LGPD eventualmente aplicadas, assim como para ter seus danos ressarcidos e compensados.

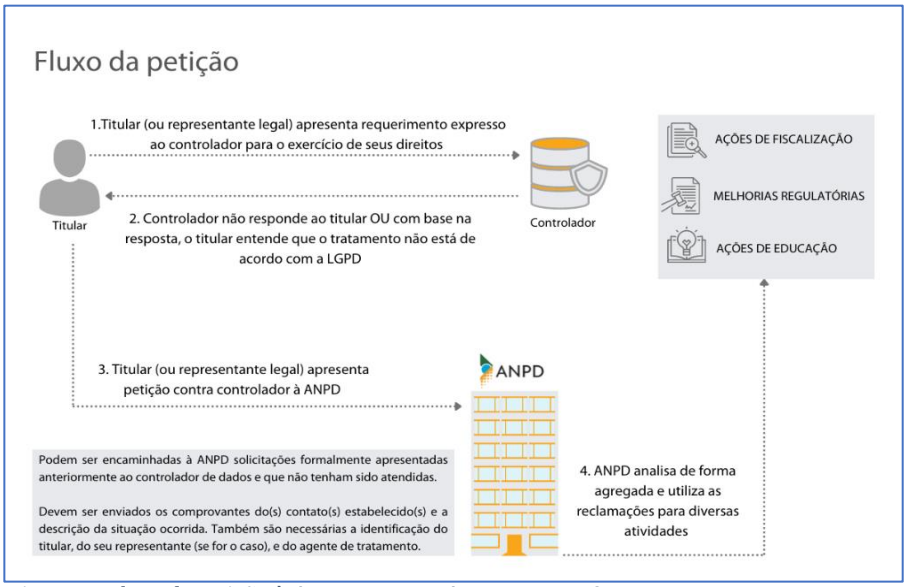

Figura 5- Fluxo da petição à ANPD - Fonte: ANPD – Jan. 2023.

É de se notar que o CNPD tem entre as suas competências a de fornecer subsídios e propor diretrizes estratégicas para a Política Nacional de Proteção de Dados Pessoais e da privacidade (BRASIL, 2018). O que demonstra que, em que pese a LGPD e as normas impostas aos agentes de tratamento estejam em pleno vigor, ainda não existe a estrutura sedimentada para a concretização da política pública de proteção de dados em todas as vertentes de incentivo à responsividade pela educação e pela instituição e aplicação de penalidades previstas na lei.

Fonte: ANPD.

Figure 6- Mapa estratégico ANPD - Fonte: ANPD

Assim, todo o atraso atinente à estruturação da ANPD tem impactado no alcance dos objetivos traçados no seu planejamento estratégico[105], conforme mapa estratégico colacionado acima (ANPD, 2022, p. 8).

4.3 Aplicação da LGPD e a tutela do direito à proteção de dados: a construção da política e o papel preponderante do judiciário no cenário brasileiro

Conforme mencionado, a consolidação de direitos não ocorre simplesmente pela sua previsão numa lei. Cumpre reiterar que a presente tese é centrada no questionamento da efetividade da política pública, entendida como o conjunto de ações governamentais

[105] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico-anpd-2021-2023. Acesso em 28 Out. 2022.

coordenadas para resolver um problema complexo. Sendo assim, no caso da proteção de dados, a Política Nacional de Proteção de Dados não se confunde com a LGPD, que é apenas o seu suporte normativo. É sabido que a eficácia de uma norma depende, inquestionavelmente, da sua entrada em vigor. Ou seja, a aptidão para produzir efeitos jurídicos da LGPD é plena. O que se investiga é o quão efetivas para a proteção do titular e do corpo digital são as medidas derivadas da norma.

O fato de frequentemente a tutela da lei não ser concretizada no plano material, fomenta a visão de que muitas normas protetivas instituídas no Brasil são dotadas apenas de valor simbólico, e que o sistema normativo é inefetivo. Esse déficit de efetividade pode ser mitigado pela implementação de políticas públicas, com a instituição de estruturas e estratégias para fomentar o direito e gerar engajamento. No caso da Política Nacional de Proteção de Dados, citam as estratégias de atuação da ANPD em campanhas educativas, em atividades investigativas, firmando convênios e parcerias com outras autoridades e com agentes de tratamento de dados pessoais, assim como, pelo reforço das diretrizes legais pelo Judiciário. O direito de petição, de recorrer ao Judiciário para fazer valer uma tutela legalmente garantida é um efeito da normatização que extrapola a mera simbologia e que tem o potencial de contribuir para a modulação da cultura organizacional, institucional e social no sentido de conscientização quanto a um dado direito ou valor. A judicialização é o único meio para o titular obter compensação financeira por danos morais e materiais decorrentes de violações aos seus direitos de proteção de dados.

No caso da política pública de proteção ao consumidor, os PROCONs e as Cortes ocuparam papel de extrema relevância para a adequação dos estabelecimentos comerciais. As punições pautadas no *Código de Defesa do Consumidor* funcionaram como uma espécie de reforço positivo, no sentido de que a prevenção pela adequação à norma passou a ser mensurada por fornecedores como um investimento válido (e não como um custo). Existe a tendência de que o mesmo ocorrerá com a Política Nacional de Proteção de Dados, especialmente a partir da *Resolução nº. 4, de 24 de fevereiro de 2023*, que aprova o *Regulamento de Dosimetria e Aplicação das Sanções Administrativas* previstas na LGPD. Somente com o vigor desse regulamento de dosimetria a ANPD começará a aplicar as sanções e a efetivamente investigar e realizar fiscalizações[106]. Essas ações administrativas certamente movimentarão o Judiciário também com questionamentos acerca das conclusões e das medidas aplicadas pela ANPD.

[106] Em junho de 2023 a ANPD divulgou a lista de processos de investigação em andamento. Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao. Acesso em 07 Jun. 2023.

Em 05 de julho de 2023 a ANPD aplicou a primeira sanção oriunda de processo administrativo, no Processo Administrativo Sancionador nº. 00261.000489/2022-62 em face da *Telekall Inforservice*, empresa de telemarketing. O agente de tratamento penalizado foi investigado pelo uso de banco de dados pessoais para disparo de mensagens em massa durante o período eleitoral de 2020. A empresa oferecia os serviços pelo site, mas quando interpelada pela ANPD para responder sobre a fonte dos dados pessoais que tratava, que base legal era empregada nos tratamentos de dados, quem era o encarregado de proteção de dados da empresa e quais seus dados, ao passo que a informação não constava no site em violação à LGPD, e se havia registro das operações de tratamento de dados e relatório de impacto à proteção de dados pessoais, limitou-se, inicialmente, a negar ter realizado as operações de tratamento de dados. A empresa foi penalizada com advertência, pela violação do dever de indicar encarregado de proteção de dados, multa simples de R$7.200,00 pelo tratamento de dados pessoais sem base legal, e multa de R$ 7.200,00 pela violação aos deveres dos agentes regulados quando forem alvos de investigação pela ANPD (*Resolução CD/ANPD nº1/2021*).

Até outubro de 2023 a ANPD emitiu mais três decisões em Processos Administrativos Sancionadores. No Processo nº. 00261.001969/2022-41[107], em face do *Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo*, foi aplicada advertência pela ausência de comunicação de incidente de segurança da informação (art. 48, LGPD), com imposição de medida corretiva para disponibilização no site do agente de tratamento autuado de comunicado acerca de incidente de segurança da informação, com orientações para os eventualmente atingidos. A ANPD aplicou outra advertência com imposição de medida corretiva, para comprovar a instituição de processo de adequação das atividades de tratamento de dados pessoais às exigências da LGPD, com comprovações sobre as medidas adotadas e sobre o nível de adequação aos requisitos de segurança da informação e às boas práticas de governança de dados pessoais. No processo nº. 00261.000574/2022-21[108], em face do *Instituto de Pesquisas Jardim Botânico do Rio de Janeiro,* a decisão foi pelo arquivamento, uma vez que a base de dados afetada por suposto incidente de segurança da informação não continha dados pessoais, de maneira que não houve qualquer infração por parte do agente de tratamento, nos termos da LGPD. Já no processo nº. 00261.001886/2022-51[109], em face da *Secretaria de Estado da Saúde*

[107] Decisão datada de 05 de outubro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4286376_relatorio_2_2023.pdf. Acesso em 23 Out. 2023.
[108] Decisão datada de 15 de setembro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4504630_relatorio_3.pdf. Acesso em 23 Out. 2023.
[109] Decisão datada de 11 de outubro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-mais-um-orgao-publico/Relatorio_4_2023_e_DOU_versopblica.pdf. Acesso em 23 Out. 2023.

de Santa Catarina, a ANPD aplicou a sanção de advertência pela não apresentação do Relatório de Impacto à Proteção de Dados, após a solicitação pela ANPD (Art. 38, LGPD), advertência com imposição de medida corretiva para manutenção de comunicado sobre o incidente de segurança da informação no site do agente de tratamento autuado (violação ao Art. 48, LGPD, pela não comunicação do incidente à ANPD em prazo razoável), advertência por violação ao Art. 49, LGPD, já que o sistema do agente de tratamento não atendia os requisitos de segurança adequados.

A utilização da LGPD como instrumento para lastrear pleitos judiciais já tem ocorrido e cresce exponencialmente, desde 2020. Existe a tendência de que o número de ações pautadas na LGPD siga sendo incrementado ao longo do tempo, conforme aponta pesquisa realizada pelo Centro de Direito, Internet e Sociedade (CEDIS) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), em parceria com o JusBrasil, *LGPD nos tribunais*[110]. Assim, para compreender o panorama da Política Nacional de Proteção de Dados é preciso analisar as decisões administrativas e judiciais proferidas com base na LGPD.

Conforme mencionado, em razão da data de entrada em vigor da lei e da aceleração do potencial nocivo do tratamento indevido de dados pessoais num contexto pós-pandêmico, em que a utilização de plataformas para trabalho, estudo, interação e comunicação remotos é uma realidade, e levando em conta o tempo para a finalização da pesquisa, o recorte temporal adotado para a realização da análise de decisões judiciais e administrativas foi de decisões proferidas de 2020 a 2022.

Em razão da maneira com que a ANPD conduz a análise de petições e denúncias contra agentes de tratamento, não existem decisões administrativas da Autoridade passíveis de análise dentro do recorte temporal estabelecido. Para as decisões judiciais, tendo em vista o objetivo de utilizar o método de direito comparado com o panorama australiano, selecionou-se Cortes de incidência nacional e representativas para orientação de precedentes. Dessa forma, o levantamento de casos para análise ocorreu perante o Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF). As pesquisas ocorreram diretamente nos ambientes digitais de pesquisa jurisprudencial dos tribunais, utilizando os indexadores “Lei Geral de Proteção de Dados”, “LGPD” e “Lei nº13.709/2018”. O foco para a análise se deu com relação aos Acórdãos, por serem mais representativos do posicionamento dos Colegiados selecionados para pesquisa.

[110] Disponível em: https://painel.jusbrasil.com.br/. Acesso em 05 Nov. 2022.

A pesquisa jurisprudencial ocorreu em duas etapas. Primeiro, foi realizado o levantamento quantitativo de Acórdãos por ano, com base nos indexadores aplicados. Num segundo momento, passou-se à análise qualitativa das decisões. Primeiramente verificando a duplicidade de ocorrências de decisões nas pesquisas com diferentes indexadores, para depois analisar o conteúdo das decisões e categorizá-las de acordo com a relevância da LGPD para a resolução do caso e nas interpretações extraídas delas (como o STJ e o STF estão enxergando conceitos e condicionando a aplicação da LGPD nos casos concretos).

A pesquisa perante o STJ apresentou os seguintes resultados: para o indexador "Lei Geral de Proteção de Dados" foram proferidos 0 Acórdãos em 2020, 0 em 2021 e 5 em 2022; para o indexador LGPD houve retorno de 0 Acórdãos proferidos em 2020, 0 em 2021 e 0 em 2022; por fim, o indexador "Lei nº. 13.709/2018" retornou com 0 Acórdãos proferidos em 2020, 0 em 2021 e 0 em 2022.

A pesquisa perante o STF apresentou os seguintes resultados: para o indexador "Lei Geral de Proteção de Dados" foram proferidos 2 Acórdãos em 2020, 1 em 2021 e 4 em 2022; para o indexador "LGPD" houve retorno de 2 Acórdãos proferidos em 2020, 1 em 2021 e 3 em 2022; por fim, o indexador "Lei nº. 13.709/2018" retornou com 1 Acórdão proferido em 2020, 0 em 2021 e 1 em 2022. Com a retirada de duplicidades, passou-se à análise de 7 Acórdãos, 2 proferidos em 2020, 1 em 2021 e 4 em 2022.

A análise preliminar dos resultados quantitativos acima elencados demonstra que o STF não possui um parâmetro rígido para se referir ao suporte normativo da Política Nacional de Proteção de Dados, usando diferentes designações e sem uma uniformização de referência nas ementas. O STJ, por sua vez, apresenta homogeneidade ao se referir à LGPD, optando pelo indexador "Lei Geral de Proteção de Dados". A uniformização quanto a referência à norma é desejável e milita em favor da facilitação de pesquisas realizadas com base na lei, assim como possui o efeito pedagógico de ratificar a tutela por ela estabelecida ao unificar os dados relativos a decisões que utilizem a norma como parâmetro.

O gráfico abaixo mostra uma tendência de aumento da judicialização de questões atinentes à proteção de dados. A referida tendência à judicialização da proteção de dados é ratificada pela pesquisa *LGPD nos tribunais* (CEDIS/IDP, JUSBRASIL, 2022), já mencionada. Esse aumento sinaliza para duas causas: um maior conhecimento por parte da população sobre o teor da LGPD e sobre os direitos que a lei assegura, e, por outro lado, uma necessidade de reforço positivo na cultura de proteção de dados dos agentes de tratamento, ao passo que as questões judicializadas correspondem a solicitações que não foram resolvidas no contato direto entre o titular de dados e o agente de tratamento.

Ademais, a curva crescente de demandas judiciais é repercussão da não atuação mais incisiva da ANPD para resolver conflitos concretos envolvendo a proteção de dados. A judicialização é um meio válido (e imprescindível) de concretização de direitos, entretanto opera seletivamente, ao passo que demanda adoção de medidas que obstaculizam a persistência no pleito pelo direito para muitos segmentos da população, por exigir conhecimento sobre as instituições competentes para receber petições, em muitos casos impõe a representação por advogado, entre outras. Medidas que representam emprego de esforço e dispêndio material para a efetivação do direito, possuindo um peso de dissuasão para grande parte da população.

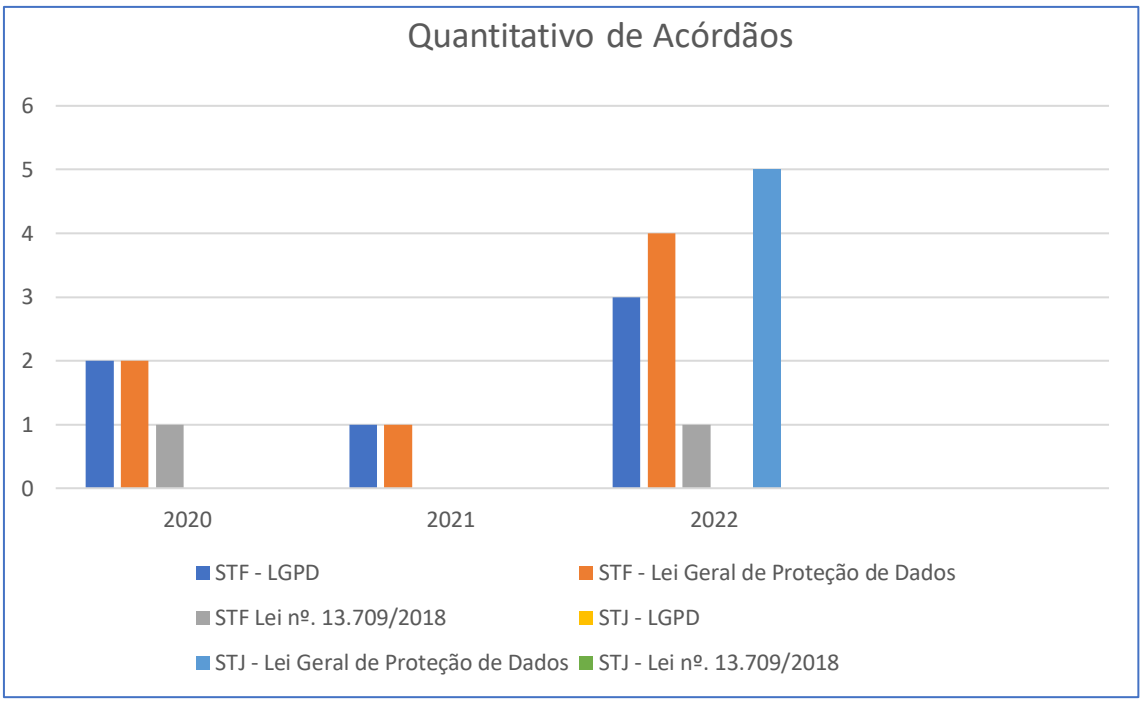

Figura 7- Gráfico quantitativo de Acórdãos STJ e STF - Fonte: Autora – baseada no retorno da pesquisa com os indexadores indicados

4.3.1 Proteção de dados nos Acórdãos do STJ

Conforme mencionado, a pesquisa resultou em cinco acórdãos publicados pelo STJ em 2022 para análise qualitativa. Somente em um dos casos a proteção de dados era a questão central (Ag. Int. nos Embargos de Declaração no Recurso em Mandado de Segurança (RMS 55819/MG) nº. 2017/0300125-6), versando sobre a legalidade de exigência de decreto estadual no sentido de obrigar os servidores públicos estaduais a disponibilizar informações sobre seus bens e evolução patrimonial para a administração pública anualmente. No julgamento a Primeira Turma se valeu de posicionamento firmado pelo STF no julgamento da Arguição por

Descumprimento de Preceito Fundamental (ADPF) 411, de que os servidores públicos já estão obrigados por lei a, na posse, e anualmente, disponibilizar informações sobre seus bens e evolução patrimonial, de maneira que o decreto analisado não estaria extrapolando o poder regulamentar, estando em sintonia com os princípios que regem a Administração Pública, previstos no art. 37 da CF/88. Ademais, a LGPD não seria um impeditivo para esse fornecimento.

> 4. A entrega dos dados à Administração não implica dizer que eles deverão ser expostos ao público em geral, cabendo àquela, já com as informações em mãos, adotar as cautelas necessárias para dar concretude ao art. 5º, LXXIX, da CF, e à Lei Geral de Proteção de Dados Pessoais, ou seja, tais normas não proíbem a coleta dos dados, mas, antes, asseguram que os entes políticos-administrativos deverão respeitar o tratamento nelas conferido. (STJ, PRIMEIRA TURMA, 2022).

Nos demais, a LGPD foi usada para sanar questão incidental, ou somente citada. No Agravo Regimental na Cautelar Inominada Criminal nº. 2021/0335441-1, um caso versando sobre a legalidade de medidas de quebra de sigilo bancário e fiscal durante atividade de persecução penal da Polícia Federal, a Corte Especial somente citou a LGPD, que em seu art. 4º, III, 'd' estabelece que a lei não se aplica ao tratamento de dados realizado para fins exclusivos de atividade de investigação e repressão de infrações penais. Assim, a citação foi para enfatizar a inaplicabilidade da LGPD ao caso concreto.

No Recurso Especial (REsp) nº. 1914596/RJ (2021/0002643-4) e no Agravo Interno nos Embargos de Declaração no REsp nº. 1841944/CE (2019/0298766-8), o tema central era o acesso aos dados cadastrais em um caso de difamação e mensagens ofensivas na internet e em outro atinente à fraude de computadores. Em ambas as decisões, a LGPD é mencionada para enfatizar a existência de um diálogo das fontes com o *Marco Civil da Internet* (*Lei Federal nº. 12.956/2014*), reafirmando-se a obrigatoriedade de tanto os provedores de conexão quanto os de acesso à internet fornecerem dados cadastrais e informações de acesso dos usuários mediante ordem judicial. No REsp. nº. 1914596/RJ a Quarta Turma vai além e afirma que

> havendo indícios de ilicitude e em se tratando de pedido específico voltado à obtenção dos dados cadastrais (como nome, endereço, RG e CPF) dos usuários cuja remoção já tenha sido determinada - a partir dos IPs já apresentados pelo provedor de aplicação -, a privacidade do usuário não prevalece. (STJ, QUARTA TURMA, 2022).

Por fim, no REsp. nº. 1995458/SP (2022/0097188-3) em caso pertinente a cobrança de débitos efetuados em cartão de crédito após fraude sofrida por cliente idoso, a LGPD é utilizada para fundamentar que o Banco e a administradora do cartão de crédito não estão isentos de responsabilidade pelo incidente, ao passo que falharam no dever de segurança, autorizando compras que fugiam ao perfil de consumo do cliente. Como não houve culpa exclusiva do titular

de dados no tratamento dos dados de cartão de crédito, não seria caso de aplicabilidade da inteligência do art. 43 da LGPD[111] para isenção da responsabilidade dos agentes de tratamento quanto a autorização das transações fraudulentas.

Para elucidar o nível de proteção de dados concretizada pelo Judiciário, especialmente com base em julgados do STJ, interessante mencionar o Acórdão de 07 de março de 2023, referente ao Agravo em Recurso Especial nº 2.130.619 - SP (2022/0152262-2). O Acórdão em questão versa sobre pedido de indenização por danos morais pelo vazamento de dados pessoais tratados por concessionária de energia elétrica. O recurso foi movido contra decisão de tribunal que reformou a sentença fixando danos morais em decorrência do vazamento comprovado. A Segunda Turma firmou o entendimento de que a despeito de o vazamento de dados pessoais consistir em falha indesejável no tratamento de dados da pessoa natural, não tem o condão de gerar dano moral indenizável, se considerado isoladamente: "[...] ou seja, o dano moral não é presumido, sendo necessário que o titular de dados comprove eventual dano decorrente da exposição dessas informações." (STJ, SEGUNDA TURMA, 2023). O Acórdão enfatiza que não basta o titular provar que o vazamento de dados aconteceu, sendo necessário que comprove dano decorrente da exposição dos dados, diretamente atrelado e decorrente do vazamento.

A análise qualitativa o conteúdo dos Acórdãos denota o caminho que precisa ser percorrido para a conscientização sobre a proteção de dados como um direito fundamental entre a população. E a urgência de que as campanhas da ANPD nesse sentido foquem no quanto os dados pessoais formam um corpo digital na sociedade informacional, que potencialmente torna o titular de dados vulnerável tanto no âmbito de vivência material como no digital. entrada em vigor da LGPD ocorreu em agosto de 2020

4.3.2 Proteção de Dados nos Acórdãos do STF

Tendo em vista a existência de decisões proferidas em 2021 que somente foram publicadas em 2022, a análise qualitativa das decisões será feita com base na data de publicação.

Em 2020 foram encontrados dois Acórdãos referentes à Medidas Cautelares em Ações Diretas de Inconstitucionalidade (ADIs) – Medida Cautelar na ADI 6.387 Distrito Federal e

[111] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Medida Cautelar em ADI 6.561 Tocantins. Em ambos os casos a LGPD foi decisiva para o deferimento das Medidas Cautelares e suspensão dos atos normativos impugnados nas ADIs, mesmo não havendo entrado em vigor ao momento das decisões em questão, ao passo que a entrada em vigor da LGPD ocorreu em agosto de 2020, com eficácia plena das sanções somente em agosto de 2021.

A decisão por referendar o deferimento da Medida Cautelar na ADI 6.387 Distrito Federal, datada de 07 de maio de 2020, foi marcante para a consolidação da proteção de dados enquanto direito fundamental autônomo no sistema jurídico brasileiro (vale lembrar que, conforme mencionado, a proteção de dados somente foi oficialmente reconhecida como direito fundamental a partir da EC 115/2022, que incluiu no rol do art. 5º, LXXIX). A ADI em questão foi movida contra a *Medida Provisória (MP) nº. 954/2020* que visava autorizar o Instituto Brasileiro de Geografia e Estatística (IBGE) a obter o compartilhamento de dados pessoais dos usuários de serviços de telefonia fixa e móvel junto às empresas fornecedoras, para fins de implementação de políticas para enfrentamento da pandemia do Coronavírus. Na decisão da Medida Cautelar em 24 de abril de 2023, a Ministra Rosa Weber explicitamente aborda a proteção de dados como direito fundamental derivado dos direitos à intimidade e à vida privada (art. 5º, X, XI e XII). Essa referência e abordagem da proteção de dados como direito autônomo é seguida no voto do Ministro Gilmar Mendes,

> A rigor, entre nós, há mais de duas décadas, já se ensaia a evolução do conceito de privacidade a partir da edição de legislações setoriais que garantem a proteção de dados pessoais, tais como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet – que inclusive assegura aos usuários da internet, entre outros direitos, a inviolabilidade e o sigilo do fluxo de comunicações e dos dados armazenados (art. 7º, II e III) – e, mais recentemente, a Lei Geral de Proteção de Dados (Lei 13.709/2018). Este último diploma assenta de maneira clara que "a disciplina da proteção de dados pessoais tem como fundamentos o respeito à privacidade e a autodeterminação informativa" (art. 2º, incisos I e II).
> [...] Para além desses desenvolvimentos normativos, a abertura do texto constitucional ao reconhecimento da autonomia do direito fundamental à proteção de dados pode ser identificada na própria jurisprudência desta Corte. Ao apreciar o tema 582, da repercussão geral (Recurso Extraordinário 673.707, Rel. Min. Luiz Fux), o Plenário do STF entendeu pelo cabimento de habeas data para fins de acesso a informações incluídas em banco de dados denominado SINCOR – Sistema de Conta-Corrente de Pessoa Jurídica, da Receita Federal. (RE 673.707, Rel. Min. Luiz Fux, Tribunal Pleno, julgado em 17.6.2015, DJe 30.9.2015).

Dando seguimento ao seu voto o Ministro Gilmar Mendes destaca que, partindo da valorização da dignidade humana, da proteção constitucional à intimidade e da vitalização do *habeas data* como elementos centrais da noção ampla do direito fundamental à proteção de dados, é possível identificar uma dupla dimensão desse direito – subjetiva e objetiva. E pela

sua fundamentalidade, o Ministro Gilmar Mendes destaca que não se trata de um direito que acarreta a mera proibição de intervenção (ou seja, num sentido negativo de tutela), mas, sim, num direito que postula uma proteção, que demanda a ação para promover a tutela suficiente.

Enquanto dimensão subjetiva, citando Laura Schertel Mendes, o Ministro Gilmar Mendes destaca a necessidade de proteção do indivíduo contra os riscos que ameaçam a sua personalidade. Assim, a dimensão subjetiva resultaria numa imposição ao legislador do ônus de apresentar uma justificativa constitucional para qualquer intervenção que impacte à autodeterminação informacional, que só poderia ser afastada excepcionalmente. E a justificativa constitucional demandada se traduz na "identificação da finalidade e no estabelecimento de limites ao tratamento de dados em padrão suficientemente específico, preciso e claro para cada área" (p. 113). Como desdobramentos da dimensão subjetiva da proteção de dados, o Ministro destaca que emergem importantes subprincípios: o princípio da proibição, segundo o qual todo tratamento de dados carece de justificação, o princípio da vinculação à finalidade, que impõe que os dados somente podem ser tratados e utilizados pela instância responsável para a finalidade para a qual foram captados, e o princípio da transparência, que se desdobra no direito do titular de dados de proceder a um controle próprio da forma como se lida com os seus dados, assim como no dever do agente de tratamento de efetuar a verificação prospectiva da licitude do tratamento dos dados, acompanhada do dever de documentação (p. 114).

No que tange a dimensão objetiva do direito à proteção de dados, o Ministro Gilmar Mendes destaca que tal direito "impõe ao legislador um verdadeiro dever de proteção (*Schutzpflicht)* do direito à autodeterminação informacional" (p. 115). Por sua vez, essa efetiva proteção deve ser acompanhada da previsão de mecanismos institucionais para salvaguarda, através da instituição de normas de organização e procedimentais, além de normas de proteção. E a positivação dessas normas seria o meio de garantir o "controle efetivo e transparente do indivíduo quanto à circulação dos seus dados, tendo como chave-interpretativa da juridicidade desse controle a noção de consentimento" (p. 115).

Para além dessa importância no reforço à noção de fundamentalidade da proteção de dados e da sua relação direta com a dignidade da pessoa humana, o Acórdão da Medida Cautelar na ADI 6.387 Distrito Federal inicia já explicitamente destacando que o respeito à privacidade e à autodeterminação afirmativa foram positivados na LGPD como fundamento da proteção de dados ao passo que são decorrências dos direitos da personalidade. Um dos pontos positivos da decisão foi a fundamentação primeiramente lastreada nas normas nacionais (LGPD e CF/88),

para depois partir para o apelo a instrumentos internacionais (*Regulamento Sanitário Internacional - RSI 2005* – adotado pela Organização Mundial de Saúde (OMS)).

Com base na necessidade, na adequação e na proporcionalidade, o Plenário do STF referendou o entendimento de que não emergia na MP 954/2020, nos moldes em que foi proposta, interesse público legítimo no compartilhamento de dados pessoais dos usuários dos serviços de telefonia. Isso porque a MP não definia adequadamente como e para que seriam utilizados os dados coletados, deixando de atender à garantia do devido processo legal (art. 5º, LIV, da CF/88). Ademais, o texto não oferecia condições de avaliação quanto à adequação e necessidade (ou seja, não deixava clara a compatibilidade do tratamento dos dados pessoais com as finalidades informadas e a fixação de limitações ao mínimo necessário para atingir essas finalidades) e não apresentava mecanismo técnico ou administrativo apto a proteger de acessos não autorizados, vazamentos acidentais ou utilização indevida os dados pessoais, descumprindo exigências extraídas da interpretação do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.

Atrelado a esses fatores, a previsão de manutenção dos dados coletados por 30 dias foi considerada excessiva e incompatível com a finalidade manifesta da coleta, resultando em agravamento da ausência de garantias de tratamento adequado e seguro dos dados compartilhados, especialmente porque ao tempo da decisão a LGPD não se encontrava em vigor ainda. Assim, o referendo ao deferimento da Medida Cautelar se deu para a suspensão da eficácia da MP 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada dos usuários dos serviços de telefonia fixa e móvel.

Já no caso da Medida Cautelar na ADI 6.561 Tocantins, a lei impugnada propunha a criação de um Cadastro Estadual de Usuários e Dependentes de Drogas no âmbito da Secretaria Estadual do de Segurança Pública (*Lei estadual n. 3.528, de 12 de agosto de 2019*), alimentado por dados provenientes de registros policiais ou outras fontes oficiais e contendo o nome da pessoa, a droga que portava e o meio que utilizou para obter a droga. A norma foi considerada eivada de inconstitucionalidade formal, ao passo que abordava matéria penal, matéria de competência privativa da União, conforme art. 22, I da CF/88, e por violar norma federal – L*ei federal nº. 11.343/2006*, que dispõe que a sistematização de informações sanitárias é de competência da União (art. 8º-A, XXI da referida lei). Eivada, ainda, de inconstitucionalidade material, ao passo que a maneira com que o cadastro seria constituído era pautada em seletividade social, sendo incompatível com o Estado de Direito e com os direitos fundamentais, entre os quais a proteção de dados (além da igualdade, da dignidade da pessoa humana, da intimidade, da vida privada e do devido processo legal).

A LGPD foi utilizada como suporte para reforçar o argumento pela inconstitucionalidade material da lei estadual impugnada. A redação do Acórdão frisa o quanto a LGPD representa a atualização de princípios que já se inscreviam no texto da Constituição, pela derivação da privacidade e da intimidade no direito fundamental à proteção de dados, colmatado pelos fundamentos da autodeterminação informativa e da inviolabilidade da intimidade, da honra e da imagem. A decisão ainda enfatiza a incompatibilidade da proposição da lei que não previa adequado protocolo para o tratamento dos dados, que conforme a redação da LGPD são dados pessoais sensíveis, merecendo regime especial de tutela, conforme art. 11 da LGPD.

Em 2021 foi publicada uma decisão envolvendo a aplicação da LGPD, Recurso Extraordinário (RE) 1.010.606 Rio de Janeiro (de 11/02/2021). Trata-se de caso de grande notoriedade por ter tramitado por longos anos e por versar sobre o "direito ao esquecimento". No julgamento do RE 1.010.606 Rio de Janeiro, a LGPD foi utilizada para analisar se o direito à proteção de dados pessoais permitiria a afirmação da existência de um direito ao esquecimento no âmbito digital (apesar de a LGPD se aplicar a tratamentos de dados pessoais não somente em meio digital, mas também em meios analógicos). Conforme enfatizado no inteiro teor do acórdão, na LGPD "não se localiza dispositivo voltado a assegurar, em âmbito digital, que os sujeitos protegidos pela norma não possam ser confrontados com os dados que, no passado, tenham sido licitamente objeto de divulgação" (p. 70).

O voto do Ministro Dias Toffoli frisa que o legislador foi explícito ao tratar do término do tratamento de dados no art. 15 da LGPD, e propositalmente manteve-se silente quanto ao um direito ao esquecimento. E segue destacando que no art. 17 da LGPD encontra-se garantida expressamente aos indivíduos a titularidade de seus dados pessoais e a observância dos direitos fundamentais da liberdade, de intimidade e de privacidade. O voto já destacava a fundamentalidade do direito à proteção de dados:

> A meu ver, sob essa ordem normativa, a proteção de dados pessoais guarda caráter de direito fundamental. [...] Em sintonia com a proteção constitucional, a LGPD buscou ampliar o alcance protetivo, dispondo aplicar-se "a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio" (art. 3º). Estabeleceu, ainda, que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação, da responsabilização e da prestação de contas. Assegurou, ademais, ao titular o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva (art. 9º). A LGPD ainda dispôs, em sessão própria, sobre o tratamento de dados sensíveis e dados pessoais de crianças e de adolescentes. A autodeterminação, por sua vez, foi prevista no art. 18, possibilitando ao titular dos dados a confirmação de seu tratamento; o acesso

> a eles; a correção de dados incompletos, inexatos ou desatualizados; a anonimização, o bloqueio ou eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a lei; a portabilidade, a eliminação dos dados pessoais voluntariamente fornecidos; a informação das entidades públicas e privadas com as quais o controlador compartilhou dados; a informação sobre a possibilidade de não consentimento e sobre as consequências da negativa; e a revogação do consentimento, tudo nos termos da Lei. (BRASIL, p. 71-72, 2021).

Por fim, o Ministro Dias Toffoli explicita que a legislação de fato agrega ampla proteção aos dados pessoais, mas não carrega a pretensão de que essa proteção seja absoluta, ao passo que em nenhum dos dispositivos trouxe um direito ao indivíduo de se "opor a publicações nas quais dados licitamente obtidos e tratados tenham constado" (p. 72). O caso em análise versava sobre um episódio do programa televisivo "Linha Direta" da emissora Rede Globo, que abordou caso de feminicídio bastante noticiado, ocorrido em 1958, conhecido como Caso Aída Curi. Os irmãos da vítima ingressaram com ação buscando compensação por danos morais, pelo uso não autorizado da imagem e dos dados da irmã assassinada. Assim, o voto destaca, ainda, as exceções constantes do art. 4º, II, a, da LGPD, entre as quais encontra-se a inaplicabilidade da lei quanto ao tratamento de dados pessoais realizado para fins exclusivamente jornalísticos ou artísticos.

Ainda quanto à fundamentalidade do direito à proteção de dados, o voto enfatiza que a privacidade e a autodeterminação informativa foram positivadas na LGPD por serem decorrentes dos direitos da personalidade (p. 181). Ademais, Dias Toffoli ressalta que a proteção da privacidade e dos direitos da personalidade sob os moldes do pretenso direito ao esquecimento resultaria em conclamar uma "hipoinformação", danosa aos próprios direitos fundamentais por violar a liberdade de expressão, e o direito à informação. No julgamento a maioria dos ministros decidiu pelo indeferimento do RE e fixou a seguinte tese para o tema nº 786 da repercussão geral:

> É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir de parâmetros constitucionais – especialmente os relativos à proteção à honra, da imagem, da privacidade e da personalidade em geral – e das expressas e específicas previsões legais nos âmbitos pena e cível. (BRASIL, 2021).

Sendo assim, a LGPD não lastrearia um direito ao esquecimento pautado no decurso do tempo, como fator que implique na proibição da circulação de informações que se caracterizem como dados pessoais. O fundamento na autodeterminação informativa, que é um direito complementar ao direito à proteção de dados pessoais, não implica numa ditadura ou num

obscurantismo que dote o titular de poder absoluto de vedar o tratamento dos seus dados. A proteção de dados, assim como outros direitos fundamentais, está sujeita a exceções e mitigações a dependerem das circunstâncias do caso concreto.

Em 2022 foram publicados quatro Acórdãos envolvendo intepretação e aplicação da *LGPD*, um pela Primeira Turma do STF (Ag.Reg. em Mandado de Segurança 36.150 Distrito Federal) e três proferidos pela Segunda Turma (Ag.Reg. na Medida Cautelar em Mandado de Segurança 37.963 Distrito Federal, Ag.Reg. na Medida Cautelar em Mandado de Segurança 37.970 Distrito Federal, e Ag.Reg. na Medida Cautelar em Mandado de Segurança 38.061 Distrito Federal).

O Ag. Reg. em Mandado de Segurança 36.150 Distrito Federal, se deu em sede de Mandado de Segurança impetrado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), contra acórdão do Tribunal de Contas da União (TCU), que determinou a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família. Em que pese a decisão do agravo, movido pela União menciona somete a LGPD, ressaltando que a sua análise não foi feita ao passo que o ato coator em avaliação ocorrera durante o período de *vacatio legis* daquele diploma legal, a negativa de seguimento se dá destacando que

> As informações prestadas ao INEP são fornecidas por jovens estudantes para o atendimento de uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo das informações pessoais. A transmissão desses dados para finalidade diversa (i) subverte a autorização daqueles que concordaram em prestar as declarações e (ii) coloca em risco a capacidade do INEP de pesquisar e monitorar políticas públicas. (BRASIL, 2022, p. 1).

Sendo assim, confirmada a liminar que anulou a determinação de entrega dos dados individualizados do Censo Educacional e do Exame Nacional do Ensino Médio (ENEM) dos anos de 2013 a 2016, requisitados pelo acórdão 2.609/2018 do TCU, bem como as sanções impostas ao INEP pela negativa da entrega dos dados. A decisão, ainda que não analisando a fundo a *LGPD*, e destacando a necessidade de respeito ao sigilo estatístico, com base no art. 5º, X, XIV e XXXIII da *CF/88*, e na *Lei nº. 12.527/2011*, *Lei de Acesso à Informação*, é fiel ao disposto no art. 6º da LGPD, que prevê que as atividades de tratamento de dados pessoais deverão observar a boa-fé e, entre outros princípios, a finalidade. O princípio da finalidade consiste na limitação dos tratamentos de dados pessoais à propósitos legítimos, específicos, explícitos e informados ao titular, com vedação da possibilidade de tratamento posterior de forma incompatível com as finalidades informadas. Cumpre destacar, ainda, que no caso em análise a base legal, ou seja, a hipótese que autorizava a coleta e tratamento dos dados dos estudantes legitimamente pelo INEP era o consentimento (art. 7º, I, LGPD). Ademais, merece

foco a ênfase dada ao Ministro Luís Roberto Barroso, no seu voto, ao impacto e potencial danoso do regime de compartilhamento de dados entre órgãos públicos para a proteção de direitos fundamentais.

No Agravo Regimental na Medida Cautelar em Mandado de Segurança 37.963 Distrito Federal, a impetrante do Agravo, Sra. Mayra Isabel Correia Pinheiro, buscava reverter indeferimento de liminar para obstar diligências determinadas pela Comissão Parlamentar de Inquérito (CPI) da COVID-19, que implicavam na quebra de sigilo de comunicações efetuadas entre ela, enquanto ocupante do cargo de Secretária de Gestão do Trabalho e da Educação na Saúde do Ministério da Saúde, e responsável por formular políticas públicas orientadoras da gestão, formação e qualificação dos trabalhadores e da regulação profissional na área de saúde no Brasil, e órgãos de prestação de serviço de saúde. A agravante alegava solicitação do acesso aos dados referentes às comunicações através do uso de aplicativos (*Google, Facebook, Whatsapp* e *Apple*) era deficiente, por não apresentar fatos hígidos e concretos a ela imputados. A Segunda Turma do STF decidiu por maioria negar provimento ao agravo, nos termos do voto do Ministro Ricardo Lewandowski (relator), com ressalvas do Ministro Gilmar Mendes, e vencido o Ministro Nunes Marques, por considerarem que, em que pese as CPIs não tenham competência sancionatória, ou seja, não tenham poder de punir quem quer que seja, desempenham papel relevante na elucidação de fatos de interesse coletivo. Por essa razão a *CF/88*, no art. 58, §3º, dotou as CPIs de poderes de investigação próprios das autoridades judiciais, facultando-lhes a realização de diligências que julgarem necessárias porquanto atuem em nome do povo soberano do qual são representantes, não sendo possível, por isso mesmo, opor a elas quaisquer limitações no exercício de importante múnus público, salvo, como é evidente, se vulnerarem direitos e garantias fundamentais dos investigados, o que não foi verificado no caso analisado.

Os Ministros Gilmar Mendes e Ricardo Lewandowski entenderam que a situação enfrentada pelo país e o fato de restar demonstrado que por mais de uma vez a impetrante encaminhou e subscreveu correspondências em que defende ser inadmissível a não utilização pelos profissionais de saúde de medicamentos sabidamente inúteis para o tratamento e a prevenção da COVID-19 (Ivermectina e Cloroquina). Ainda, tendo em vista o firme e longevo entendimento do STF de que as CPIs devem ter como ponto de partida elementos indiciários para a solicitação de diligências sob a égide do art. 58, §3º da CF/88. Sendo assim, não se exige delas a fundamentação exaustiva das diligências que determinam no curso dos seus trabalhos, desde que não haja abusos. E os abusos seriam verificados a partir da inequívoca demonstração da falta de pertinência temática entre os atos questionados e os fatos investigados pela CPI.

A LGPD é mencionada para fundamentar a ressalva de que mesmo sendo possível a quebra do sigilo telefônico e telemático por determinação da CPI, a jurisprudência do STF tem se mantido no sentido da viabilidade do controle judicial das deliberações, notadamente a fim de avaliar a existência de fundamentação adequada para a medida excepcional. Esse foi o argumento para posição divergente do Ministro Nunes Marques que considerou que a menção à morte de 480 mil pessoas no país em decorrência da COVID-19 e das más práticas de gestão da saúde não seria fundamento suficiente para a medida excepcional. Ainda mencionando a LGPD, em seu voto, o Ministro Gilmar Mendes avaliou se a lei autorizaria a interceptação do conteúdo das mensagens trocadas pelos aplicativos, e citou o art. 4º que traz a exceção, atividades a que a LGPD não se aplica, entre as quais as atividades exclusivamente de investigação e repressão de infrações penais. E o §1º, do mesmo artigo que dispõe que o tratamento de dados pessoais nas atividades excepcionais será regido por legislação específica que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD.

Os Agravos Regimentais nas Medidas Cautelares em Mandados de Segurança 37.970 Distrito Federal e 38061 Distrito Federal, também foram impetrados contra diligência determinada pela CPI da COVID-19 para investigar os Srs. Eduardo Pazuello e José Matheus Salles Gomes, respectivamente. A justificativa da CPI para a quebra de sigilos de Eduardo Pazuello foi o fato de ele ter sido Ministro da Saúde, e antes de ocupar o cargo em questão, ter atuado como secretário-executivo do Ministério da Saúde (segundo cargo na hierarquia desse ente público), estando diretamente envolvido tanto com as políticas públicas adotadas pelo Estado Brasileiro para enfrentamento da COVID-19, quanto com as omissões em face dos fatos investigados pela CPI. Já no caso de José Matheus Salles Gomes, a justificativa apresentada pela CPI para a quebra dos sigilos do impetrante foi o fato de que ele, na qualidade de integrante do chamado "Gabinete do ódio", haver propalado a utilização de medicação sem eficácia comprovada e apoiado terias como a de imunidade de rebanho, razões que se vinculam diretamente aos objetivos da CPI da COVID-19. Contra José Matheus Salles Gomes, assim, havia indícios de produção e disseminação de notícias falsas na internet "com o objetivo de executar estratégias de confronto ideológico e de radicalização dos ataques nas redes sociais contra adversários" (STF, 2022, p. 13-14).

Da mesma maneira, a LGPD foi mencionada para reforçar que a previsão constitucional de poderes da CPI não é absoluta, devendo haver o respeito aos direitos fundamentais do art. 5º da CF/88 e cuja tutela foi reforçada pelo *Marco Civil da Internet* e pela LGPD. Em todos os

Acórdãos citados proferidos pela Segunda Turma do STF foi enfatizado o fato de a vida estar cada vez mais intermediada por tecnologias de comunicação, de maneira que os computadores pessoais e *smartphones* são usados na contemporaneidade para registrar as mais diversas informações e são meios de execução de diversas tarefas profissionais e pessoais. Dessa forma, ante a convergência de informações para esses mecanismos, assim como em face da "hiperdocumentação" do dia a dia das pessoas, resultante desse fenômeno, tem-se que as autoridades investigativas tem o dever de minimizar o acesso aos dados pessoais dos investigados, limitando-o ao estritamente necessário à investigação, sob pena de violação irreparável do direito à intimidade e à privacidade.

Os Ministros Gilmar Mendes e Edson Fachin fizeram ressalva para ressaltar que o STF precisa na análise do mérito dos Mandados de Segurança traçar balizas sólidas e homogêneas para o controle dos atos praticados por CPIs, com fulcro em promover a transparência e a prestação de contas na seara da fiscalização operacionalizada pelo Poder Legislativo.

Reforçando a fundamentalidade da proteção de dados como direito autônomo, foram encontradas mais decisões envolvendo a aplicação da LGPD no âmbito do STF, Corte dedicada à guarda da Constituição Federal, do que do STJ. Perante o STF, a LGPD foi objeto de discussões centrais nas decisões proferidas, à exceção da decisão exarada no Agravo Regimental em Mandado de Segurança 36.150 Distrito Federal. No âmbito normativo a LGPD de fato veio trazer coesão para uma série de direitos fundamentais que se encontravam pulverizados em diversas normas no sistema jurídico brasileiro, sendo reconhecida como tal pelo teor das decisões analisadas, que foram de grande influência para a aprovação da EC 115/2022, que reconhece a proteção de dados como direito fundamental no sistema jurídico brasileiro. E a questão mais explorada nas decisões foi quanto a aplicabilidade da norma aos casos concretos e a sua extensão. Dessa forma, tem-se que a atuação das cortes contribui para a interpretação do disciplinamento da tutela prevista na LGPD, mas ainda se revela incipiente para operar o efeito pedagógico de modulação da cultura organizacional e social pelo entendimento e respeito à proteção de dados como um direito fundamental.

4.4 Política Pública de Proteção de Dados Brasileira e Cultura de Compliance com a privacidade e a proteção de dados

Para o desenvolvimento desta seção foram utilizadas pesquisas conduzidas pela *Palqee* e pela *Copenhagen Business School*, com apoio dos escritórios *Peck Advogados*, *Privacy Rocket* e *Diferenciall*, referente à cultura de privacidade nos primeiros anos de vigência da

LGPD: *Relatório Privacy Culture 2021*[112] e *Relatório Privacy Culture 2022*[113]. Utilizou-se como fontes, ainda, a pesquisa *LGPD nos Tribunais*[114], já mencionada nesta tese, a fim de interpretar o nível de engajamento dos titulares de dados pessoais (ao passo que o *Relatório Privacy Culture* foca na introjeção da privacidade e proteção de dados no âmbito corporativo, ou seja, é pertinente à cultura organizacional). Por fim, realizou-se a análise das *Resolução CD/ANPD nº. 5, de 13 de março de 2023*, atinente à aprovação da agenda de avaliação de resultado regulatório para o período de 2023-2026, e a *Resolução CD/ANPD nº. 4, de 24 de fevereiro de 2023*, que aprova o regulamento de dosimetria e aplicação de sanções administrativas pela ANPD. Os documentos emitidos pela ANPD demonstram o engajamento da Autoridade em trabalhar estratégias de reforço à cultura de privacidade e proteção de dados pela aplicação de sanções (o que não foi feito nos dois primeiros anos de vigência da LGPD), assim como pela iniciativa de medir os resultados regulatórios para realinhar as estratégias se necessário, apostando no melhoramento contínuo da política pública de proteção de dados.

Por tratar-se de uma pesquisa realizada por amostragem com empresas que se cadastraram para tanto, o *Relatório Privacy Culture* não é utilizado como parâmetro para aferir a cultura organizacional predominante no Brasil. O questionário aplicado foca em questões relativas às expectativas, às percepções, aos comportamentos e às reações dos respondentes a situações relativas à Gestão de riscos e *compliance*, no que diz respeito à privacidade e à proteção de dados. Como destacado no Relatório de 2021, os dados são enviesados, ao passo que 90% das empresas que se cadastraram para participar da pesquisa ou já implementaram programas de governança de dados ou estavam em processo de adequação à LGPD, já tendo empenhado investimentos para fomentar a cultura de privacidade e proteção de dados entre os colaboradores (RELATÓRIO PRIVACY CULTURE 2021, p. 11).

Em que pese o alerta quanto ao enviesamento, é interessante observar a metodologia empregada, que segregou a cultura de proteção de dados em dez pilares, atribuindo notas para cada um dos pilares, com base nas respostas aos questionários aplicados, assim como uma média final. Os pilares destacados são: transparência (existem políticas de privacidade e de controle de acessos à dados pessoais, essas normas são revisadas regularmente e disponibilizadas para fácil acesso, sendo todas as mudanças relevantes comunicadas para os

---

[112] Disponível em: https://palqee.com/resources/privacy-culture-index-brasil-2021/. Acesso em 10 Jul. 2022.

[113] Disponível em: https://d1huxt1mr63m7u.cloudfront.net/resources/PrivacyCulture%C2%AE+INDEX+BRASIL+2022+(EN).pdf. Acesso em 23 Abr. 2023.

[114] Pesquisa conduzida pelo IDP CEDIS, em parceria com o Jusbrasil, que contou com a participação nos dois anos de importantes pesquisadores do campo da proteção de dados no Brasil como Laura Schertel Mendes e Danilo Doneda. Disponível em: https://painel.jusbrasil.com.br/. Acesso em 10 Jul. 2023.

afetados), direitos dos titulares (clientes, usuários e colaboradores recebem instruções de como exercer seus direitos de privacidade e proteção de dados, e a organização possui uma estrutura e procedimentos claros para atendê-los), segurança da informação (existem medidas administrativas, técnicas e operacionais implementadas sendo seguidas e monitoradas pelos colaboradores para proteger os dados pessoais dos titulares) , gestão de riscos (a organização possui níveis de riscos definidos e documentação em dia para a gestão de riscos de privacidade e proteção de dados, incluindo instruções para avaliar, monitorar e reportar riscos às partes envolvidas), gestão de incidentes (existem processos claros para a identificação de incidentes de segurança de dados e vazamentos, com instruções sobre os procedimentos a adotar para comunicar as autoridades e as partes afetadas), governança organizacional (existe uma estrutura organizacional bem definida foi implementada, com papeis e responsabilidades claros e comunicados aos colaboradores, com suporte da diretoria e dos executivos, além de "*privacy champions*" apontados), princípios de tratamento (a empresa possui operações e procedimentos implementados que garantem que o tratamento de dados pessoais é limitado à necessidade, possui escopo definido e o dado é mantido somente pelo tempo necessário), finalidades de tratamento (as pessoas da empresa sabem por qual motivo estão tratando os dados pessoais e qual sua base legal de tratamento para cada atividade), treinamento (a organização possui políticas, treinamentos e suporte disponíveis e de fácil acesso para seus colaboradores, e a participação em treinamentos é monitorada pelos gestores da empresa regularmente), e compartilhamento de dados (existem contratos e/ou acordos de tratamento de dados pessoais assinados e em dia, com todas os fornecedores e parceiros com os quais dados pessoais são compartilhados, com a clara definição de como essas empresas devem tratar tais dados).

Com base na média obtida pelas empresas, a nota geral atribuída à amostragem analisada em 2021 foi 7,8 (numa escala de 0 a 10). Analisando os pilares, observa-se que a menor pontuação foi para treinamento (média de 7,0), enquanto a maior pontuação foi para segurança da informação (8,3). Pela atual configuração das operações em empresas, com a política de *home office* mais difundida, existe uma tendência de apostar em segurança da informação pelo investimento em *softwares* e estruturas digitais de segurança, principalmente a partir da adoção de aparatos tecnológicos e medidas administrativas mais robustas (autenticação de e-mails e logins em três ou mais etapas, antivírus, gradação de credenciais de acesso à documentos, entre outros). Entretanto, se os colaboradores não tiverem a consciência dos motivos para cada medida de cautela recomendada, para cada política implementada, a cultura de privacidade e proteção de dados não estará efetivamente sendo reforçada no âmbito da organização. Os treinamentos são de extrema relevância para alinhamento interno e para a

autopercepção quanto à responsabilidade envolvida no tratamento de dados pessoais e o quanto todos, sem exceção, numa organização são importantes para a integridade no que tange a privacidade e a proteção de dados.

O relatório de 2021 apontou uma divergência entre as expectativas, as percepções e o efetivo comportamentos dos respondentes frente aos temas atinentes à privacidade e à proteção de dados. A pesquisa aponta que a discrepância comportamental pode ser resultado da absorção de alguns conceitos de privacidade somente no nível teórico, sem o entendimento de como se aplicam na rotina de operações da organização e nas atividades diárias de cada colaborador (RELATÓRIO PRIVACY CULTURE 2022, p. 21). Outra demanda identificada para a promoção da cultura organizacional de privacidade foi a de investimento em treinamentos customizados, focando no aprofundamento de temas sensíveis para cada área específica, além da disciplina sobre o compartilhamento de dados formalizada em Acordos de Compartilhamento de Dados, deixando claras as atribuições de cada um dos envolvidos e explicitando as medidas para mitigar os efeitos de eventuais incidentes de segurança de dados. Esses acordos figuram como instrumento para disciplinar responsabilidades e registrar orientações do Controlador de dados em relação ao Operador de dados em uma relação contratual que implique em tratamento de dados pessoais.

O relatório de 2022 foi conduzido com mesma metodologia e comparativamente traz indicadores de melhoria da nota geral atribuída à amostragem (de 7,8 para 8,3), decorrente de uma melhoria na média de todos os pilares traçados para a cultura de privacidade e proteção de dados, com exceção de "princípios de tratamento", que passou a ser o pilar com menor nota, por ter crescido somente 0,17, em relação à média do ano anterior (em 2021 a nota foi 7,3 e em 2022, 7,43 para "princípios de tratamento"). "Segurança da informação" se manteve como pilar com maior nota (8,55). A nota do pilar "treinamentos" foi a que mais subiu em relação ao ano anterior, de 7,0 para 7,63). Entretanto, as médias apontam que a difusão sobre a aplicação da LGPD nas atividades diárias segue deficitária, tendo em vista a nota de "princípio de tratamento". O relatório de 2022 aponta, ainda, que a incerteza quanto as medidas a serem adotadas para responder a solicitações de titulares de dados continuam a ser marcantes (RELATÓRIO PRIVACY CULTURE 2022, p. 17).

Assim, o progresso dos dados colhidos na pesquisa destaca a tendência de que a adaptação às exigências da LGPD esteja sendo conduzida de maneira procedimental e formalista no ambiente corporativo, tendo como resultado a desconexão entre expectativas e percepções em relação ao comportamento adotado em situações envolvendo o tratamento de dados pessoais. Pode-se dizer que o fortalecimento da cultura organizacional de privacidade e

proteção de dados está em fase inicial, mas ainda carecendo de integração aos processos e de efetiva valorização para que possa ser introjetado na rotina das empresas.

No que diz respeito à cultura de privacidade e proteção de dados entre os cidadãos de uma maneira geral (designada na tese de cultura social), percebe-se que a consciência quanto aos direitos do titular e ao valor dos dados pessoais ainda não é suficientemente difundida. Nas relações consumeristas existe uma preocupação por parte das empresas fornecedoras de legitimar práticas a partir da documentação de consentimentos (no caso de programas de fidelidade, com coleta de diversos dados pessoais, por exemplo), mas essa preocupação não se reflete em transparência quanto ao que é feito com os dados coletados, muitas vezes pautada em termos lacunosos e generalistas assinados, ou na manifestação de ciência e concordância com uma política de privacidade não lida. O que o consumidor leva em conta é apenas o desconto obtido, ou a vantagem imediata concedida supostamente de forma gratuita. Segue predominando um misto de desconhecimento para a grande maioria, e de descrença para uma minoria informada sobre o extrativismo de dados (uma espécie de sentimento de que a exposição dos dados pessoais é inevitável, ou um ceticismo quanto ao potencial de ser alvo de uso malicioso desses dados).

A minoria mais informada e consciente dos direitos reforçados pela LGPD faz parte da tendência de judicialização da proteção de dados, conforme apontado pela pesquisa *LGPD nos tribunais*, conduzida pelo IDP CEDIS de outubro de 2021 a setembro de 2022, em parceria com o Jusbrasil. Como a compensação por danos sofridos pela violação à proteção de dados no Brasil somente ocorre pela via judicial, é plausível cogitar, ainda, que o perfil desse titular mais informado decorre do seu acesso à aconselhamento jurídico (a serviços de assistência jurídica).

Os dados relativos aos capítulos mais explorados nas decisões pela pesquisa *LGPD nos tribunais* (IDP, CEDIS) analisadas em 2021 (Capítulo I – Disposições Preliminares) e em 2022 (Capítulo VI – Dos agentes de tratamento de dados pessoais, com especial foco na responsabilidade e ressarcimento por danos) demonstram que a proteção de dados tem ganhado destaque nas decisões judiciais, que tem sido, de acordo com os pesquisadores envolvidos (IDP, CEDIS), cada vez mais robustas. Conforme conclusões exaradas na pesquisa de 2022 o "amadurecimento vertiginoso" da proteção de dados nos tribunais é demonstrado não somente pelas fundamentações aportadas pelos julgadores, mas também pela maior complexidade das discussões apresentadas por ambos os polos das demandas (IDP, CEDIS, 2022). As análises dos acórdãos cujos registros foram feitos nesta tese em seções anteriores corroboram com esse entendimento. Enquanto em 2021 as discussões nos Acórdãos orbitavam em torno de debates principiológicos, em 2022 as demandas passam a tratar com mais frequência da aplicação

efetiva da LGPD no que tange o exercício de direitos do titular (para cessar tratamentos indevidos, sem lastro em bases legais, para acesso à documentos contendo dados pessoais, para sanar efeitos de incidentes de segurança da informação, entre outros). Ademais, os pesquisadores do CEDIS e IDP destacam que o número de decisões relevantes, abordando a LGPD de maneira central quase que triplicou de um ano para o outro.

Em que pese a judicialização tenha relevância no que toca a modulação da cultura de privacidade e de proteção de dados, tanto entre a população quanto ao pressionar as plataformas digitais, há que se ter em mente que no sistema de proteção estabelecido pela política pública de proteção de dados pessoais brasileira, até junho de 2023, não existem mecanismos para resolução de um conflito envolvendo proteção de dados administrativamente, a não ser que o conflito se dê em uma relação consumerista, o que faz com que os PROCONs possam atuar.

Vale lembrar que a ANPD tem recebido petições e denúncias individuais sobre violações à LGPD, mas ainda não tem aparato para investigar e analisar individualmente as petições e denúncias, que são avaliadas de maneira agregada, e tomadas como indicador para direcionar a atividade fiscalizatória da ANPD. E que, mesmo que passe a analisar individualmente as petições dos titulares individualmente, na redação atual da LGPD e nas normas emitidas pela ANPD para moldar a política pública, não existe a possibilidade de a própria ANPD atuar na conciliação do conflito entre o Controlador/Operador e o titular, tampouco de resolver o conflito fixando um valor para composição de danos materiais e morais advindos da violação a proteção de dados. Ante esse panorama, somente pela via judicial é que o titular pode buscar seus direitos, o que implica em muitos casos (a exceção de demandas que possam ser processadas nos Juizados Especiais, se não houver recurso) em custos, que nem todos os indivíduos podem suportar. Dessa forma, mesmo reconhecendo que a efetivação normativa tem efeito para além do simbólico ao dotar o indivíduo de possibilidades de ação para exigir o direito, é forçoso reconhecer que no panorama brasileiro vigente em junho de 2023 a proteção de dados é efetivada de maneira elitista e seletiva. Vale dizer, a proteção de dados existe para alguns titulares.

No âmbito governamental institucional, em que pese o Brasil já tenha instituído um *Conselho de Monitoramento e Avaliação de Políticas Públicas*[115] (CMAP)[116], que funciona no

[115] Para maiores informações, veja https://www.gov.br/economia/pt-br/acesso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/cmap. Acesso em 10 jan. 2023.

[116] "A Portaria Interministerial, de 08.04.2016, instituiu o Comitê de Monitoramento e Avaliação de Políticas Públicas Federais (CMAP), com o objetivo de aperfeiçoar as políticas públicas, programas e ações do Poder Executivo Federal para o alcance de melhores resultados; o aprimoramento na alocação de recursos e melhoria na qualidade do gasto público. […]" (ANDRADE, SANTANA, 2017, p. 787).

âmbito da Presidência da República, e é composto pelos Comitês de Monitoramento de Políticas de Subsídios (CMAS) e de Gastos Diretos (CMAG), as políticas avaliadas são selecionadas anualmente. A seleção é feita com base em critérios determinados por Programas Finalísticos do Plano Plurianual. Vale frisar, somente algumas políticas públicas passam por processo de avaliação e monitoramento por este órgão. E as análises são pautadas em busca pela eficiência, com a quantificação de investimentos feitos (por gastos diretos e subsídios) e de resultados diretos quantificáveis (por exemplo, no relatório pertinente ao ano base 2020, o Programa Minha Casa, Minha Vida (p. 21-22) é avaliado em termos de nível de eficiência com base no aporte recebido – R$129,8 bilhões em subsídios públicos até 2019 – confrontado com o número de imóveis entregues – mais de 4 milhões até 2019 – e com o déficit habitacional existente). Tendo em vista que a ANPD somente teve autonomia orçamentária a partir de outubro de 2022 (*MP nº. 1.124/2022*, ratificada como *Lei nº. 14.160/2022*), sendo até então órgão da Presidência da República, e conforme dados levantados desde 2020, demonstrando que não havia dotação orçamentária para a política pública de proteção de dados até então, essa política não poderia ser medida pelo CMAP.

Ante o exposto, entende-se que a iniciativa da ANPD de conduzir a medição dos resultados, a partir da construção de indicadores para as atividades contidas no planejamento estratégico da autoridade é de grande valia para o aprimoramento da política pública de proteção de dados. A agenda para avaliação de resultado foi aprovada na *Resolução CD/ANPD nº. 5 de 13 de março de 2023*, e tem previsão de conclusão do primeiro ciclo de avaliações em dezembro de 2026. Da mesma maneira, o estabelecimento de parâmetros para aplicação das sanções administrativas previstas na LGPD é de extrema importância para a efetivação da atividade fiscalizatória da ANPD e para o reforço da cultura de privacidade e proteção de dados. A *Resolução CD/ANPD nº. 4, de 24 de fevereiro de 2023* aprova o regulamento de dosimetria e aplicação de sanções administrativas. A aplicação das sanções é pautada no princípio da proporcionalidade, tendo em conta a gravidade da violação e o impacto dessa violação para os titulares de dados afetados. A postura do agente de tratamento respondendo ao processo administrativo será levada em consideração para a dosimetria da sanção, assim como para a incidência de descontos nas sanções pecuniárias. A construção do procedimento e dos parâmetros para dosimetria visa claramente o estímulo à proatividade na adequação às exigências da LGPD, assim como à cooperação com os propósitos regulatórios, espelhando os elementos basilares da regulação responsiva abordados no Capítulo 3.

Mesmo reconhecendo o esforço dos evolvidos na operacionalização da ANPD (muitos com formação acadêmica com pesquisas dedicadas aos desafios e repercussões da sociedade

informacional, abordados no Capítulo 2, e militantes da proteção de dados enquanto direito autônomo), entende-se que a efetividade da atuação para a promoção da cultura de privacidade e proteção de dados demanda a possibilidade de a ANPD apreciar individualmente as denúncias que receber. Vale reforçar que o sentido de efetividade trabalhado nesta tese parte da perspectiva do titular de dados, quanto aos mecanismos existentes para buscar concretizar o direito e a real proteção promovida ao seu corpo digital. Essa possibilidade tornaria a busca pela efetivação dos direitos do titular mais democrática, podendo prescindir do apelo ao judiciário para o endereçamento das demandas. A partir dessa possibilidade, a urgência em moldar cultura organizacional no sentido de proteger os direitos dos titulares seria maior por parte dos agentes de tratamento, especialmente no que tange a criação de canais de comunicação para que o titular pleiteie o seu direito diretamente junto ao agente de tratamento, e de maior conscientização e alinhamento dos colaboradores nas empresas para entender a necessidade de responder a essas solicitações. No âmbito de prioridades de ação, a proteção de dados ganharia um *status* de urgência. Isso ao passo que condenações reais que impliquem em prejuízos financeiros e reputacionais, ao passo que uma das penalidades previstas é a de publicização da infração após devidamente apurada (art. 52, IV da LGPD), passariam a ser mapeadas como riscos para a sustentabilidade das operações das plataformas digitais e do ambiente empresarial de maneira geral.

Ademais, ao realizar esse tipo de análise a ANPD teria a oportunidade de atuar na conscientização dos titulares de maneira mais próxima, ao notificar sobre as decisões, por exemplo, fazê-lo em linguagem mais simples e acessível, instruindo sobre meios para recorrer ou buscar o judiciário para resolver a questão. Essa possibilidade geraria, ainda, a noção de que todos aqueles cuja atuação demanda o tratamento de dados pessoais precisam se adaptar e respeitar as normas de privacidade e proteção de dados. A fiscalização pontual, como está estabelecida no panorama vigente em 2023 contribui para uma postura desidiosa por parte dos agentes de tratamento menores ou cujas atividades não estejam tão em evidência, militando em desfavor do fomento à cultura de privacidade e proteção de dados (além de reforçar a percepção de que a proteção de dados em verdade é um direito para alguns, somente). Ademais, as decisões proferidas pela ANPD gozam de maior congruência por serem proferidas por entidade especializada no tema da proteção de dados.

O próximo capítulo é dedicado ao estudo do panorama de privacidade e de proteção de dados existente na Austrália. A abordagem seguirá os mesmos parâmetros metodológicos aplicados para o estudo da política pública de proteção de dados brasileira: uma justificativa da escolha de efetuar o estudo comparado com o panorama australiano, a breve contextualização

sobre a tutela da privacidade no sistema legal australiano, seguida pela abordagem no plano normativo, e do plano institucional e dos mecanismos de *enforcement* (de como a proteção à privacidade é reforçada na prática).

5 CONTEXTO AUSTRALIANO DE PRIVACIDADE: por que buscar outras referências para além dos países Europeus?

Este capítulo argumenta que a regulação da privacidade foi desenvolvida pela reprodução dos "melhores padrões" estabelecidos por organizações internacionais, sendo colonizada pelas plataformas que dominam as economias (e as pessoas) pelo emprego da concentração de poder econômico e de poder instrumentário (derivado da divisão do aprendizado e do conhecimento). As plataformas são usadas para exercer seu poder modulando a vontade pública e determinando, de forma muito suave, sutil e generalizada, como a regulação será estabelecida. A convergência regulatória extrapola o objetivo alegado de combater um problema transnacional, para neutralizar os direitos de privacidade e proteção de dados tanto quanto possível. Assim, quanto maior a exploração de diferentes pontos de vista regulatórios, maior será a viabilidade de criar soluções inovadoras para efetivação do direito à proteção de dados.

Como a Austrália tem uma maneira única de desenvolver políticas, apostando na transparência e na cooperação, sendo, ainda, o berço da regulamentação responsiva (também implementando algumas iniciativas de *Behavioural Public Policy - BPP*) e encarando a lei e as estruturas regulatórias como um sistema cíclico que deve ser monitorado e melhorado constantemente para perceber a eficácia, a avaliação da experiência australiana mostrou-se profícua para oxigenar a produção científica em torno da proteção de dados e da política pública destinada a promovê-la. Essa comparação do sistema de proteção de dados brasileiro com o australiano é importante para a tese por possibilitar acesso a conhecimento sobre um plano normativo e institucional pouco explorado nas pesquisas do Brasil. A grande maioria das pesquisas científicas em Direito que lançam mão do método comparado optam por operacionalizá-lo em sistemas jurídicos europeus, no sistema estadunidense ou na América Latina. Cumpre enfatizar que um dos objetivos da presente tese é contribuir para a avaliação da Política Nacional de Proteção de Dados Pessoais e para o seu melhoramento contínuo, sendo a busca por perspectivas diversas salutar para esse propósito.

O capítulo se dedica a mapear como os direitos de privacidade são aplicados na Austrália, com foco na estrutura estabelecida pelo *Privacy Act 1988* (Cth). A exploração se baseia na lei e em quais ferramentas estão à disposição do titular dos dados para reivindicar privacidade. Assim, a análise foi realizada por meio do estudo de decisões administrativas e judiciais baseadas no *Privacy Act 1988* (Cth) tomadas de 2020 a 2022, o mesmo período analisado na estrutura brasileira. O capítulo conclui que da perspectiva da proteção do corpo

digital, a forma como os mecanismos de *enforcement* ao *Privacy Act 1988* (Cth) são conduzidos é mais contundente para modular a cultura organizacional, institucional e social de engajamento com a proteção estabelecida pela norma, resultando em maior efetividade para atender às demandas dos titulares de dados. Em que pese o *Privacy Act 1988* (Cth) possuir conteúdo que pode ser considerado desatualizado e merecedor de revisão, se levar-se em conta a visão predominante na doutrina da proteção de dados pessoais de que o *GDPR* é o regulamento standard, a concretização dos direitos atinentes à proteção de dados no *Commonwealth* australiano mostra-se mais efetiva sob a perspectiva do titular de dados e de tutela do corpo digital.

Neste capítulo é analisado o desenvolvimento da privacidade e da proteção de dados na Austrália, através do estudo da base legal fixada no *Privacy Act 1988* (Cth) e suas alterações, para depois se examinar a estrutura e as estratégias adotadas pelo OAIC para engajar as agências e as pessoas em geral, terminando com uma análise sobre a forma como a lei está sendo vista e experimentada pelos titulares de dados e pelos agentes de tratamento (o nível de cumprimento e de compreensão).

Apesar da confirmação parcial em relação à hipótese de que o sistema australiano de proteção à privacidade é resultado de influências externas, incorporadas ao sistema jurídico, e mesmo diante do fato de que o sistema brasileiro de proteção de dados é, pelo menos à primeira vista, mais apto de promover os direitos da personalidade[117] do que o sistema australiano, o contraste entre os dois sistemas leva a insights interessantes relacionados ao processo de inovação no direito e nas políticas públicas, que podem agregar valor ao aprimoramento contínuo do cenário da política pública brasileira.

5.1 O foco nas normas do *Commonwealth*

A Austrália é uma federação com as funções legislativa e executiva compartilhadas entre o *Commonwealth* e os estados e territórios, de modo geral semelhante ao modelo federal dos Estados Unidos da América. O *Commonwealth* da Austrália foi formado pelas seis colônias australianas que foram fundadas pelos britânicos entre 1788 e 1859. O movimento em direção

[117] Vale mencionar que a referência aos direitos da personalidade se dá com o significado de direitos subjetivos fundamentais que são essenciais para o livre desenvolvimento das pessoas, conforme abordado no capítulo 3. Nas palavras de Adriano de Cupis (2008), os direitos da personalidade são um conjunto de direitos cuja ausência tornaria a personalidade jurídica desprovida de qualquer valor concreto. Em outras palavras, sua ausência tornaria todos os outros direitos subjetivos praticamente inúteis para o indivíduo. A noção de proteção de dados como um direito autônomo, relacionado à privacidade, é crucial porque trata da capacidade de autodeterminação informativa, de controlar os resultados das interações na sociedade informacional.

à independência nacional e à federação ganhou ritmo na década de 1890. As discussões culminaram em duas convenções constitucionais de representantes eleitos pelas colônias para produzir um projeto de constituição para uma nação federada. O projeto de constituição foi submetido a referendos do povo em todas as colônias para aprovação. Após a aprovação, o projeto de constituição foi enviado ao Parlamento Imperial em Westminster para ser promulgado. A proclamação do *Commonwealth of Australia Constitution Act 1900* (Cth) pela Rainha Vitória ocorreu em 1º de janeiro de 1901. A Constituição não foi acompanhada de uma declaração de independência, portanto a federação permaneceu dentro do Império Britânico. A independência ocorreu gradualmente por volta da Segunda Guerra Mundial, com a dissolução progressiva do Império Britânico (TAYLOR, 2010, p. 171-173).

Como uma Federação, a Austrália foi estruturada para ter um "federalismo coordenado", no qual é enfatizada a paridade de importância entre estados federados e União ocupando esferas independentes de atividades[118] (WINDHOLZ, 2011, p. 4). No entanto, embora a Austrália tenha esse federalismo coordenado, ao longo do século XX ele teve suas características mitigadas[119], com o *Commonwealth* expandindo seu escopo e atuação sobre os estados federados. Isso resultou na migração do federalismo australiano de uma relativa paridade de forças entre entes federados e União, para um centralismo da União[120] (WINDHOLZ, 2011, p. 5).

---

[118] O *Commonwealth of Australia Constitution Act 1900 (Cth)* preserva o direito dos estados de manter suas próprias constituições estaduais. Há mais duas fontes de lei constitucional na Austrália: o S*tatute of Westminster 1931 (Cth)*, um ato do Parlamento do Reino Unido, que permitiu que a Austrália revogasse a legislação do Reino Unido e legislasse extraterritorialmente e removeu o poder do Reino Unido de fazer leis para a Austrália (antes disso, a Austrália era reconhecida como um domínio independente de fato do Reino Unido, mas não tinha legislação que concedesse o reconhecimento legal da independência antes); e o *Australia Act 1986 (Cth*), estatutos conjuntos entre os parlamentos do Reino Unido e da Austrália, que romperam os laços entre os parlamentos do Reino Unido e da Austrália e deram poderes aos parlamentos estaduais para revogar a legislação do Reino Unido.

[119] Como Windholz aponta, essas intervenções foram ocasionadas por uma série de crises que exigiram ação da Commonwealth, bem como pelo contexto econômico e político global que exige um poder central mais assertivo: "[…]Since federation, a series of national crises requiring national responses, Australia's increasing international obligations, concerns over service delivery at the State level, and a growing belief that a more seamless national economy is required to ensure Australia's competitiveness in a global economy, have combined to encourage the Commonwealth to intervene in areas once thought of as traditional State responsibilities. Such Commonwealth interventions have generally been upheld by a High Court that has interpreted the Constitution to support this expanded Commonwealth role. For example, the High Court has upheld the Commonwealth's ability to provide tied grants to States on the condition the States do not raise their own income tax or that they spend it consistent with Commonwealth policy;4 broadly interpreted the Commonwealth's monopoly on excise; and applied a literal and expansive interpretation to Commonwealth powers such as the external affairs and corporation's powers. This has resulted in a situation in which the Commonwealth is able to involve itself in many areas traditionally thought of as State responsibilities – either through direct action (in reliance on its expanded Constitutional powers) or indirectly (through its ability to provide 'tied grants' to the States) – and an Australian Constitution that provides for significant overlap and interdependence in the exercise by the Commonwealth and States of their powers." (WINDHOLDZ, 2011, p. 5).

[120] Vale a pena mencionar que, embora o federalismo australiano tenha uma forma Concorrente, ele tem um modo de concorrência "Coopetição" (*co-opetition)*, misturando o comportamento concorrente e cooperativo de suas

É necessário esclarecer, então, que o foco da pesquisa quanto ao suporte normativo para a política pública de privacidade na Austrália se deu com base na lei federal, do *Commonwealth*. Isso não significa que o *Commonwealth* tenha competência e jurisdição exclusiva sobre a regulação da privacidade na Austrália (CTH, *AUSTRALIA CONSTITUTION ACT*, *chapter* V). Vale reforçar, muitos estados australianos têm leis próprias que regulam a privacidade, e essas leis possuem vigência e compatibilidade em paralelo com o *Privacy Act 1988* (Cth), lei de privacidade federal.

Como herança da colonização britânica, a Austrália tem um sistema jurídico de *common law*, portanto, diferenças na forma como a privacidade de dados é protegida, já que o Brasil tem um sistema jurídico de *civil law*, eram esperadas. A Austrália é reconhecida por sua eficácia em políticas públicas e como o berço da regulação responsiva, que apresenta estratégias que são uma tendência nos novos sistemas de regulação no Brasil. Vale mencionar que a regulação responsiva propõe estratégias para estimular os regulados a cumprir as normas e a cooperar com a consecução dos objetivos regulatórios, conforme argumentado no Capítulo 3.

Como mencionado, a LGPD foi influenciada pelo *GDPR*. Assim, como a tese visa contribuir para a melhoria contínua da Política Pública Nacional de Proteção de Dados brasileira, o contraste com um sistema não diretamente influenciado pela estrutura europeia representa uma oportunidade de pensar em perspectivas inovadoras e diversas para um problema transnacional, como a necessidade de promover a privacidade, a proteção de dados e a autodeterminação informativa.

A política pública é um reflexo do esforço do Executivo para fomentar o alcance de objetivos coletivos. Assim, as políticas públicas buscam diferentes objetivos e lidam com diversos campos do conhecimento para planejar e agir, sendo uma área que exige uma abordagem interdisciplinar. É fundamental encarar os sistemas jurídicos e todas as outras formas sistemáticas de abordar os problemas sociais com um olhar voltado para a ideia aplicada pela pesquisa e desenvolvimento de novos produtos, serviços e processos, o *design thinking*[121]

---

entidades. Esse tipo de concorrência permite que a Federação Australiana tenha uma maneira mais flexível de lidar com questões políticas, permitindo maior capacidade de resposta e eficácia (WINDHOLZ, 2011).

[121] O *design thinking* é uma metodologia e um processo de abordar problemas e construir soluções com base nos valores de empatia, colaboração e experimentação. Encontrar uma solução adotando o *design thinking* demanda a adoção das seguintes etapas: empatia, definição, ideação, prototipagem, teste e iteração. Se necessário, repete-se o processo para o aprimoramento contínuo da solução, começando com os motivos do fracasso da solução anterior. A esse respeito, veja os vídeos do *Centre for Legal Innovation* do *College of Law*, disponíveis em: https://www.cli.collaw.com/resource-hub. Acesso em 27 Jun. 2023. O processo mencionado segue a mesma lógica da a avaliação de padrões no gerenciamento de processos e planejamento, o *Ciclo de Deming* ou *método PDCA*, baseado nas etapas de *Plan (planejar)*, *Do* (fazer), *Check* (verificar) e *Act* (agir) (DUDIN, SMIRNOVA, VYSOTSKAYA, FROLOVA, VILKOVA, 2017). O DT ensina que o progresso é mais importante do que a

(DT), entendendo as soluções legais e regulatórias propostas como um rascunho inicial que pode ser atualizado, enriquecido.

5.2 Privacidade e proteção de dados na Austrália: uma breve contextualização

O caminho da privacidade no mundo está vinculado ao caminho do desenvolvimento da Internet e da tecnologia da computação, conforme demonstrado nos Capítulos 2 e 3. Quanto mais crescia a dependência da comunicação, surgiam não apenas novas ameaças, mas também a crescente compreensão de que a proteção da propriedade[122], como a privacidade era concebida na época, não era suficiente para preservar os interesses individuais. Na década de 1950, foi concebida a primeira convenção que demonstrava preocupações sobre como o aumento do uso de novas tecnologias pode ser intrusivo, a *Convenção do Conselho da Europa – Convenção 108* (RODOTÀ, 2008). Na década de 1970, a primeira geração de leis se concentrou na privacidade (SAMPAIO, 1998), mas como um direito estático de ser deixado em paz. Essa geração foi seguida por uma segunda e mais ampla concepção de privacidade, considerando aspectos relacionados à proteção de interesses possessórios, com foco na proteção de uma espécie de propriedade na década de 1980 (SAMPAIO, 1998). Para estar em conformidade com as orientações da OCDE (GUNASEKARA, 2021, p. 20) sobre o fluxo de dados transfronteiriços e a proteção da privacidade, lançadas em 1980, bem como após os primeiros relatórios da *Australian Law Reform Commission (ALRC)*, a privacidade tornou-se uma questão política na Austrália (ALLARS, 2014, p. 116; M.D.K, 1981). Tornou-se urgente a promulgação de proteções e medidas de privacidade para garantir o tratamento legal de informações pessoais.

A menção às *Diretrizes da OCDE* é importante, considerando que a Austrália é membro da Organização desde 1971[123] (M.D.K., 1981, p. 163). Além disso, vale ressaltar que o presidente de um grupo de especialistas da OCDE responsável pela compilação mencionada dessa organização também era presidente da *Australian Law Reform Commission (ALRC)*

perfeição ao lidar com problemas. A mesma visão deve ser aplicada para tratar de problemas sociais e para o controle e melhoramento das políticas públicas.

[122] No que diz respeito à longa jornada da privacidade, vale mencionar que, inicialmente, o direito à privacidade tem uma proteção indireta, derivando diretamente do direito de propriedade os direitos à inviolabilidade do lar, com base na máxima da *Common Law* "*Man's house is his castle*" (a casa do homem é seu castelo), o direito autoral, com base no conceito de valor histórico e propriedade material do conteúdo, para uma noção de propriedade imaterial, com base na quebra de confiança ou quebra de contrato, e o direito à imagem, também com base na propriedade imprescritível de cada pessoa sobre sua imagem, seu rosto e seu retrato.

[123] A Seção 1 do *Privacy Act 1988* (Cth) menciona explicitamente a filiação da Austrália à OCDE como uma das motivações da lei, com o objetivo de proteger a privacidade dos indivíduos.

quando esta produziu seu relatório sobre proteção da privacidade, o juiz Michael Kirby[124] (Current Topics, n. 315, 1986, p. 318; KIRBY, 2001, p. 8). Kirby também é patrono da *Australian Privacy Foundation (APF)*, que é uma organização voltada para a luta contra questões emergentes que representam ameaças à liberdade e à privacidade dos australianos e tem como objetivo defender o direito dos indivíduos de controlar suas informações pessoais e de ficar livres de intrusões excessivas[125]. O *Justice* Kirby, que acabou atuando na *High Court of Australia*, é um juiz conhecido e um tanto controverso, visto por alguns críticos como ativista judicial[126], por defender que, no sistema jurídico da *common law*, os juízes devem agir para integrar o direito, derivando-o das declarações antigas e usando a analogia para lidar com os novos desafios impostos pelos contextos em mudança. Emprega-se a expressão "ativismo judicial" no sentido de "disposição de um juiz para derrubar a ação de outro ramo do governo ou para anular um precedente judicial" (BRITANNICA ACADEMIC, *s.v. Judicial activism*[127], *tradução nossa*). Portanto, um juiz ativista seria um juiz que não adota uma postura restritiva ao que a lei aborda.

O juiz Kirby é uma figura importante na trajetória da privacidade na Austrália. Em sua carreira, ele ocupou muitos cargos nacionais e internacionais relacionados à proteção de direitos subjetivos, lutando por uma maneira melhor de lidar com a AIDS (Kirby foi membro da Comissão Global sobre HIV e Direito das Nações Unidas) e pelo aprimoramento da estrutura de privacidade na Austrália. Kirby tinha um compromisso pessoal especial com a regulamentação da privacidade. Membro da comunidade LGBTQI+, ele passou a maior parte de sua carreira "escondendo" sua vida pessoal e vivendo com medo de ser revelado, pois a

---

[124] Para conhecer a trajetória do Justice Kirby e sua importância como advogado, juiz e ativista dos direitos humanos na Austrália, é recomendável assistir ao documentário "*Michael Kirby: Don't forget the Justice bit*", da Art Media (2010). *Justice* Kirby é uma figura muito importante cujo trabalho foi determinante para a trajetória dos direitos humanos na história do sistema jurídico australiano. Ele é um dos juízes mais longevos dos tribunais australianos, tendo atuado na *Federal Court of Australia* (de 1983 a 1984), na *Court of Appeal of New South Wales* (de 1984 a 1995), na *Court of Appeal of Solomon Islands* (de 1995 a 1996). E até mesmo na High Court of Australia (de 1996 a 2009).

[125] Para obter mais informações, consulte o site https://privacy.org.au/about/contacts/advisorypanel/.

[126] *Justice* Kirby entende que: "In some court systems, there may indeed be nothing that can be done about unreasonable invasions of privacy. But it is important to realise that in common law systems at least, it is not necessarily the case that the law will decline to intervene. The rules of the common law, and of its sister equity, have been developed over centuries by judges to respond to individual cases brought before them. If there is no settled doctrine, those judges will consider whether it is possible to derive new law, by analogical reasoning, from the old statements of the common law. It is in this way that our legal system is never, ultimately, without a solution to a legal problem. So long as it can be done consistently with the body of pre-existing legal principles, and is not in breach of tile Australian Constitution or statute law, judges can sometimes provide remedies in cases which their predecessors could not even imagine. […]" (KIRBY, 2001, p. 9).

[127] Disponível em: https://academic-eb-com.eu1.proxy.openathens.net/levels/collegiate/article/judicial-activism/488008.. Acesso em 20 Jun. 2023.

homossexualidade ainda era uma ofensa criminal na Austrália durante um período de sua vida profissional e, quando deixou de ser crime manteve estigma significativo (BROWN, 2011).

A ALRC também foi determinante para a forma como a privacidade foi tratada na legislação australiana. A ALRC é um órgão independente do governo australiano que fornece recomendações de reforma legislativa ao governo sobre questões encaminhadas a ele pelo Procurador-Geral da Austrália (CTH, 1996). A ALRC desempenha um papel decisivo no aprimoramento do sistema jurídico australiano, em termos de atualização dessas normas e de torná-lo adequado para lidar com as demandas contemporâneas desde 1975, ano em que a ALRC iniciou seu trabalho.

É inegável que não apenas a promulgação do *Privacy Act 1988* (Cth), mas também seus aprimoramentos ao longo de décadas, são resultado do trabalho realizado pela ALRC. A maneira como a comissão trabalha é peculiar. Todos os relatórios elaborados pela ALRC são, em teoria, resultado de um trabalho misto, cooperativo e complementar, pois, embora a ALRC seja um órgão independente, ele inicia seu trabalho com base nas referências fornecidas pelo Procurador-Geral da República[128], que desempenha o papel de Ministro do Governo; no entanto, seus relatórios são dirigidos ao Parlamento federal. A independência da agência faz com que seu trabalho tenha maior probabilidade de tentar chegar à experiência dos cidadãos em relação à lei e à forma como a lei afeta a vida cotidiana. Como resultado, os relatórios não são apenas um conjunto de recomendações para alterações e inovações na lei, mas principalmente uma medição da efetividade, que aponta caminhos para o aprimoramento.

O trabalho da ALRC para um relatório final[129] é orientado por duas abordagens diferentes: a abordagem de "instituto de pesquisa", "em que as recomendações são geradas por especialistas que analisam dados relevantes e literatura acadêmica" (TRANTER, 2015, p. 324, *tradução nossa*), e a abordagem de "envolvimento da comunidade", "em que as recomendações são localizadas como tendo surgido de um processo de consulta à comunidade" (TRANTER, 2015, p. 324, *tradução nossa*). A coleta de dados é feita sob uma estrutura específica apresentada nos "Termos de Referência" fornecidos pelo Procurador-Geral[130]. O trabalho

---

[128] É pertinente observar que, atualmente, o Departamento do Procurador-Geral costuma abrir espaço para coletar contribuições sobre temas que serão apresentados como referência à ALRC. Veja, por exemplo, o que ocorreu com o *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*. Isso também abre espaço para consultas sobre a Declaração de Impacto da Regulamentação. As contribuições relevantes são publicadas e disponibilizadas para acesso público. Consulte https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/published_select_respondent. Acesso em 15 Dez. 2022.

[129] Todos os relatórios finais produzidos pela ALRC estão disponíveis em: https://www.austlii.edu.au/au/other/lawreform/ALRC/. Acesso em 15 Dez. 2022.

[130] Veja mais sobre o processo de reforma da lei no site da ALRC. Disponível em https://www.alrc.gov.au/about/law-reform-process/. Acesso em 15 Dez. 2022.

preliminar é concretizado em documentos denominados questões (*Issues*) e documentos de discussão (*Discussion Papers*) para análise posterior. A consulta tem como objetivo atingir idealmente quatro propósitos:

> […]to gather information and opinion; to test preliminary ideas against interest groups and their perspectives; to protect the Commission from criticism of special interests; and to strengthen political decision makers so that they accept the reform proposals that have been tested in the community. (KIRBY, 2003, p. 60)

Justice Kirby (2003, p. 60) destaca ainda que a ampla consulta tem um impacto benéfico ao ajudar a desmistificar a lei e seu desenvolvimento, cooperando também em termos de melhorar a compreensão da comunidade sobre a lei na Austrália. Entretanto, a ideia de uma abordagem de envolvimento da comunidade tem seus riscos, conforme enfatizado por Kieran Tranter (2015). Em um estudo baseado em relatórios finais emitidos de 1992 a 2012 pela ALRC, Tranter descobriu que, de fato, existe a predominância de uma abordagem de envolvimento da comunidade. No entanto, os relatórios finais são centrados em citações das submissões recebidas, e muito menos baseados em pesquisas (principais e secundárias) no campo de discussão (TRANTER, 2015, p. 340-345). O foco na abordagem das submissões é discricionário, o que pode levar a relatórios lastreados por dados anedóticos, em vez de verdadeiramente representativos (TRANTER, 2015, p. 361). O estudo mencionado constatou que existe uma tendência de a ALRC considerar mais submissões feitas por organizações tradicionais (TRANTER, 2015, p. 353-355), o que sugere que as recomendações resultantes dos trabalhos da ALRC podem não ser tão democráticas ou diversificadas quanto parecem. Independentemente das críticas, é fato que a ALRC desempenhou um papel importante nas mudanças do *Privacy Act 1988* (Cth) ao longo dos anos.

O primeiro relatório sobre privacidade (*Privacy and the Census - Report nº. 12*), apresentado no Parlamento federal em novembro de 1979, concentrava-se em questões de privacidade relacionadas ao Censo demográfico e concluía que ele tinha como objetivo produzir informações estatísticas válidas para serem usadas pelos governos, pelo setor e por organizações voluntárias no planejamento e na tomada de decisões que afetam o bem-estar de todos os australianos (ALRC, 1979, p. x). Os benefícios a serem obtidos com as informações do censo eram enormes, embora as preocupações sobre a necessidade de proteção consistente das informações pessoais fossem válidas. Por esse motivo, o *Relatório nº. 12* terminou com as seguintes recomendações principais: o público deveria ser informado tanto sobre a necessidade das informações do Censo quanto sobre as medidas tomadas para proteger a confidencialidade; as informações do Censo não deveriam ser destruídas, mas transferidas para a segurança dos Arquivos Nacionais; o acesso às informações do Censo deveria ser proibido para a maioria dos

propósitos por setenta e cinco anos; informações altamente sensíveis não deveriam ser solicitadas de forma compulsória, a menos que houvesse uma necessidade altamente convincente (ALRC, 1979, p. xv-xvi).

O segundo relatório sobre privacidade foi o *Privacy - Report nº. 22*, apresentado em dezembro de 1983. Esse relatório abordou as principais recomendações com base no reconhecimento do estágio de perigo que ameaça a privacidade, delineando que a privacidade estava em perigo atualmente e, ainda mais, prospectivamente, de maneira que: uma Lei de Privacidade deveria ser aprovada para estabelecer os princípios de privacidade das informações; e a Lei deveria prever a nomeação de um Comissário de Privacidade (ALRC, 1983, p. 14, vol. 2). As fontes de perigo foram identificadas como os crescentes poderes oficiais, as novas práticas comerciais e a nova tecnologia da informação (ALRC, 1983, p. 8, vol. 2). É notável que o trabalho do ALRC foi crucial para a promulgação do *Privacy Act 1988* (Cth), que criou o cargo de *Privacy Commissioner* e implementou muitas das recomendações relacionadas à privacidade das informações, além de todas as emendas posteriores. No entanto, embora o Relatório nº. 22 tenha recomendado a regulamentação do tratamento de informações pessoais nos setores público e privado, o *Privacy Act 1988* (Cth) inicialmente tratava apenas do *Commonwealth* e das autoridades públicas como agentes de tratamento de informações pessoais[131].

O objetivo[132] do *Privacy Act 1988* (Cth)[133] não era apenas implementar as diretrizes da OCDE, conforme explicitamente mencionado em seus propósitos e objetivos, mas também cumprir, ao menos parcialmente, o artigo 17 do *Pacto Internacional sobre Direitos Civis e Políticos (ICCPR)* (ALLARS, 2014, p. 116). A versão original do *Privacy Act 1988* (Cth) trazia onze princípios que deveriam ser levados em conta pelas "agências" (*agencies)*, conceito que incluía, na época, os tomadores de decisão do governo federal, como ministros, departamentos,

---

[131] Consulte o site do OAIC sobre a expansão da cobertura do *Privacy Act 1988* (Cth) Disponível em https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/history-of-the-privacy-act. Acesso em 15 Dez. 2022.

[132] Para mais informações sobre a História do *Privacy Act 1988* (Cth) consulte o site do OAIC. Disponível em. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/history-of-the-privacy-act. Acesso em 15 Dez. 2022.

[133] Seus objetivos estatutários estão definidos na seção 2ª. Objects of this Act. "The objects of this Act are: (a) to promote the protection of the privacy of individuals; and (b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities; and (c) to provide the basis for nationally consistent regulation of privacy and the handling of personal information; (d) to promote responsible and transparent handling of personal information by entities; and (e) to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected; and (f) to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected; and (g) to provide a means for individuals to complain about an alleged interference with their privacy; and (h) to implement Australia's international obligation in relation to privacy."

autoridades estatutárias e afins, ao lidar com informações pessoais. Para o escopo do *Privacy Act 1988* (Cth), informações pessoais (*personal information*)[134] significam "informações ou opiniões sobre um indivíduo identificado, ou um indivíduo que seja razoavelmente identificável: (a) quer as informações ou opiniões sejam verdadeiras ou não; e (b) quer as informações ou opiniões sejam registradas de forma material ou não". (CTH, 1988).

Os onze Princípios de Privacidade da Informação (*Information Privacy Principles* – IPPs*)*, apresentados no texto original do *Privacy Act 1988* (Cth) eram atinentes à: coleta de informações pessoais (IPP 1); solicitação de informações pessoais de indivíduos (IPP 2); solicitação geral de informação pessoal (IPP 3); armazenamento e segurança de informações pessoais (IPP 4); informações relacionadas aos registros mantidos por um registrador (IPP 5); acesso à registros que contenham informações pessoais (IPP 6); alteração de registros que contenham informações pessoais (IPP 7); verificação da precisão das informações pessoais por um detentor de registros antes do uso (IPP 8); informações pessoais a serem usadas para fins relevantes (IPP 9); limites do uso de informações pessoais (IPP 10); e limites de divulgação de informações pessoais (IPP 11).

Inicialmente, os IPPs foram aplicados somente ao setor público da *Commonwealth*, de modo que o setor privado permaneceu sujeito somente a algumas regras setoriais, geralmente relacionadas a crédito ao consumidor, números de arquivos fiscais e seguro de saúde. Os movimentos em torno da autorregulação foram incentivados pelo *Privacy Commissioner* por meio dos *National Principles for Fair Handling of Personal Information*, um código voluntário para encorajar o setor privado a desenvolver práticas adequadas. Somente em dezembro de 2001, a *Privacy Amendment (Private Sector) Act 2000* (Cth) entrou em vigor e estendeu sua aplicabilidade a algumas organizações do setor privado. Desde a alteração citada, dez princípios, os Princípios Nacionais de Privacidade (*National Privacy Principles* - NPPs), foram introduzidos no *Privacy Act 1988* (Cth), estabelecendo padrões para as organizações do setor privado. A emenda mencionada teve como objetivo revisar o sistema existente de autorregulação do setor privado, que foi considerado inconsistente e insuficiente para atingir os padrões internacionais[135], resultando em riscos relevantes para as finalidades comerciais australianas.

---

[134] Seção 6 do *Privacy Act 1988* (Cth).

[135] Conforme mencionado por Margaret Allars (2014), "Naquela época, o governo reconheceu que, se as empresas australianas não cumprissem a Diretiva da UE, poderia haver um custo para as relações comerciais da Austrália e uma redução nas oportunidades de comércio eletrônico entre fronteiras". *Tradução nossa.*

O *Privacy Amendment (Private Sector) Act 2000* (Cth) redefiniu a noção de "agências" para incluir nesse conceito indivíduos que lidam com dados para fins econômicos, corporações, parcerias e outras entidades do setor privado, além de estabelecer o *Office of the Privacy Commissioner*, posteriormente integrado ao *Office of the Australian Information Commissioner* (OAIC), desde sua criação em 2010[136]. O OAIC é o órgão regulador responsável pelo *Privacy Act 1988* (Cth) e, como tal, tem o poder de iniciar investigações sobre práticas que possam violar os deveres de privacidade e de orientar os regulados, agentes de tratamento de informações pessoais, a realizar a Avaliação de Impacto na Privacidade (*Privacy Impact Assessment* - PIA) sobre as atividades ou funções que realizam (TAYLOR, 2020, p. 739). Por outro lado, excluiu quatro classes relevantes do dever de seguir os NPPs: pequenas empresas, atos ou práticas de empregadores em relação a registros de funcionários, mídia e fontes jornalísticas e, finalmente, partidos políticos, incluindo representantes políticos e conselheiros do governo local por seus atos e práticas relacionados a uma eleição, referendo ou outra participação no processo político.

Os NPPs tratam de Coleta (NPP 1); Uso e divulgação (NPP 2); Qualidade dos dados (NPP 3); Segurança dos dados (NPP 4); Abertura (NPP 5); Acesso e correção (NPP 6); Identificadores (NPP 7); Anonimato (NPP 8); Fluxos de dados transfronteiriços (NPP 9); e Informações sensíveis (NPP 10). Como IPPs, as NPPs têm particularidades em termos de exceções, como o uso de informações pessoais para uma finalidade secundária, uma vez que seu uso ou divulgação seja exigido ou autorizado por lei.

É necessário enfatizar que, apesar de os NPPs se enquadrarem no conteúdo das *Diretrizes* da OCDE, eles foram além para lidar com os fluxos de dados transfronteiriços, com a expectativa de permitir que a Austrália alcançasse a adequação à *Diretiva Europeia (46/95/CE)*, em vigor naquele momento. A lei de privacidade australiana foi considerada inadequada em termos de proteção à privacidade e às informações pessoais, o que poderia causar prejuízos às relações comerciais com os membros da UE, especialmente após o relatório do *Grupo de Trabalho do Artigo 29 (Article 29 Working Party)*, da *Diretiva da UE*, emitido em 2001, que se recusou oficialmente a reconhecer a lei de privacidade australiana como adequada ao nível de proteção desejável conforme o referido artigo. De olho no que estava acontecendo no cenário internacional, bem como com base nos interesses comerciais australianos, a ALRC

[136] O *Australian Information Commissioner Act 2010* (Cth) criou o *Office of the Australian Information Commissioner* (OAIC) em 1º de novembro do mesmo ano. Desde então, o *Office of the Privacy Commissioner*, criado em 2001, foi integrado ao OAIC. O OAIC é chefiado pelo *Australian Information Commissioner*, que conta com o apoio do F*reedom of Information Commissioner* e do *Privacy Commissioner.*

preparou uma proposta de revisão do *Privacy Act 1988* (Cth), composta de duzentas e noventa e cinco recomendações para reforçar sua efetividade. Como resposta ao ALRC *For Your Information: Australian Privacy Law and Practice - Report nº. 108*, o *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) - que entrou em vigor em 12 de março de 2014 - introduziu disposições que substituem os IPPs e NPPs pelos *Australian Privacy Principles*[137] (APPs), aplicáveis aos setores público e privado, coletivamente chamados de "entidades APPs" (*APP entities*).

Os APPs se referem ao manejo aberto e transparente de informações pessoais (APP 1); Anonimato e pseudonimato (APP 2); coleta de informações solicitadas (APP 3); tratamento de informações pessoais não solicitadas (APP 4); notificação de coleta (APP 5); uso ou coleta (APP 6); marketing direto (APP 7); divulgação transfronteiriça (APP 8); adoção, uso ou divulgação de identificadores relacionados ao governo (APP 9); qualidade (APP 10); segurança de informações pessoais (APP 11); acesso (APP 12); e correção (APP 13). Os APPs entraram em vigor em 12 de março de 2014 e são aplicados a organizações privadas e órgãos públicos[138]. Os APPs definem as obrigações a serem observadas quando uma organização ou agência coberta pelo *Privacy Act 1988* (Cth) estiver lidando com informações pessoais. Constituem o centro da estrutura de proteção de privacidade no *Commonwealth*, e incorporam a preferência australiana pela regulação baseada em princípios que devem ser respeitados no manejo de informações pessoais, em vez de uma abordagem prescritiva à proteção de dados[139] (WITZLEB, 2018, p. 380). Vale reforçar: a importância dos APPs é tal que no sistema de proteção do *Privacy Act 1988* (Cth) as interferências na privacidade são definidas pela violação a um ou mais APPs.

Outra alteração relevante ocorreu em 2018, com o *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)[140]. Desde então, todas as organizações ou agências cobertas pelo *Privacy Act 1988* (Cth) devem notificar os indivíduos afetados e o OAIC no caso de uma violação de dados que possa causar danos graves àqueles cujos dados pessoais estejam envolvidos. Após ser notificado, o OAIC incentiva a conformidade com o *Esquema de*

---

[137] Cada um desses princípios é desenvolvido em vários subprincípios. Consulte "*Schedule 1 - Australian Privacy Principles*" do *Privacy Act 1988* (Cth).

[138] Para mais detalhes sobre quem está coberto e tem responsabilidades de acordo com o *Privacy Act 1988* (Cth), consulte: https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities#OrgAndAgencyPrivacyActCovers. Acesso em 14 Dez. 2022.

[139] "*They are the central of Australia's privacy protection framework and embody its preference for principles-based regulation over a prescriptive approach to data protection*" (WITZLEB, 2018, p. 380).

[140] O *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) estabeleceu que é considerada uma violação de dados quando as informações pessoais mantidas por uma agência ou organização são perdidas ou sujeitas a acesso ou divulgação não autorizados.

Violações de Dados Notificáveis (*Notifiable Data Breaches* - NDB), tratando reclamações, investigando e tomando outros tipos de ações regulatórias, oferecendo consultoria e orientação às organizações reguladas e fornecendo informações à comunidade sobre a operação do esquema NBD.

O *Privacy Act 1988* (Cth), que pode ser considerado pioneiro em seu foco na privacidade, estabelece, de fato, medidas de segurança informacional, que não abrangem todas as facetas da proteção geral da privacidade (WITZLEB, 2018, p. 377). No sistema jurídico australiano, não há um direito geral explícito à privacidade, nem um direito autônomo de proteção de dados (no sentido que existe no sistema jurídico brasileiro), nem uma previsão expressa de autodeterminação informativa. Assim, uma vez que não há um direito próprio à privacidade, algumas ações incidentais protegem indiretamente alguns aspectos da vida privada. São exemplos de causas de ação que tratam da proteção incidental à privacidade as ações por quebra de confiança, invasão de terras, assédio, difamação, perturbação, inflição intencional de danos psiquiátricos e violação de direitos autorais. Considerando essas causas de ação e o *Privacy Act 1988* (Cth), é possível perceber que o sistema jurídico australiano apresenta uma noção restrita de privacidade, em comparação com o *GDPR*, tomado como uma lei padrão, pois a falta de proteção geral impacta uma visão de privacidade associada à propriedade ou a interesses de posse.

Recentemente, o Departamento do Procurador-Geral iniciou uma coleta de sugestões sobre uma nova revisão do *Privacy Act 1988* (Cth). A coleta de sugestões foi encerrada em 10 de janeiro de 2022[141]. A próxima revisão deve abranger diferentes áreas[142], com foco na avaliação das últimas emendas e no aprimoramento da estrutura, incluindo o escopo e a aplicação do *Privacy Act 1988* (Cth); se a lei protege efetivamente as informações pessoais e fornece uma estrutura prática e proporcional para a promoção de boas práticas de privacidade; se os indivíduos devem ter direitos diretos de ação para fazer cumprir as obrigações de privacidade nos termos do *Privacy Act 1988* (Cth); se um delito legal para invasões graves de privacidade deve ser introduzido na legislação australiana; o impacto do esquema de violação de dados notificáveis e sua eficácia no cumprimento de seus objetivos; a eficácia dos poderes e mecanismos de aplicação o *Privacy Act 1988* (Cth) e como eles interagem com outras estruturas regulatórias do *Commonwealth*; além disso, a conveniência e a viabilidade de um esquema de

[141] Após algumas alterações, centradas no aumento das sanções do *Privacy Act 1988* (Cth), foi aberto um prazo para a apresentação de observações sobre o relatório elaborado pela revisão do Attorney-General's Department, que deverá ser apresentado em 31 de março de 2023.

[142] Consulte a *Review of the Privacy Act 1988 - Terms of Reference*, disponível em https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988. Acesso em 11 Nov. 2022.

certificação independente para monitorar e demonstrar a conformidade com a lei de privacidade australiana.

Em resposta à violação de dados da *Optus* (PARLIAMENT OF AUSTRÁLIA, 2022)[143], que afetou vários australianos, um projeto de lei contendo parte dos objetivos da revisão foi apresentado em 26 de outubro de 2022[144] e recebeu o consentimento real em 28 de novembro de 2022 - o *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* (Cth). A última inovação foi principalmente o aumento do regime de penalidades para interferências graves ou repetidas com a privacidade do máximo de AU$ 2,22 milhões para um montante de AU$ 50 milhões, três vezes o valor de qualquer benefício obtido com a conduta que constitui a interferência[145], ou 30% do faturamento ajustado de uma entidade na Austrália durante o período relevante, para se concentrar nas consequências das violações de dados, que, ao mesmo tempo, significam a falha de uma entidade em proteger as informações pessoais que detém contra acesso não autorizado, violando os APPs, especialmente o APP 11[146] (relacionado à segurança das informações pessoais). Além disso, conforme apontado pelo Procurador-Geral Mark Dreyfus[147] (2022, p. 10), as recentes violações de dados mostraram que o dano à reputação sofrido pelas entidades em decorrência desses incidentes não é suficiente, em comparação com o potencial de causar sérios danos financeiros e emocionais aos australianos. O aumento tem outros objetivos para aplicar o APP 3, que visa desencorajar a coleta excessiva de informações pessoais.

É importante destacar que o *Privacy Commissioner* não tem poderes, de acordo com o *Privacy Act 1988* (Cth), para impor diretamente uma penalidade civil a uma entidade regulada. Ele tem o poder, por meio de uma determinação, de compensar perdas econômicas ou não econômicas, derivadas da interferência na privacidade. As perdas não econômicas são verificadas na forma de ansiedade, angústia e constrangimento, que possam ser demonstrados como vinculados ao evento de interferência. Para fixar o valor da compensação, o

---

[143] Veja nas informações sobre o contexto que levou ao ato normativo Disponível em https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2223a/23bd030. Acesso em 11 Nov. 2022.

[144] A revisão está em andamento, e a aprovação do referido projeto de lei, transformando-o em lei, é parcial em relação ao escopo inicial definido para a revisão.

[145] Se for possível determinar o valor do benefício obtido direta ou indiretamente, que seja razoavelmente atribuível à conduta que constitui a contravenção, consulte 13G, 3, b do *Privacy Act 1988* (Cth).

[146] De acordo com as diretrizes do OAIC, o APP 11 exige que as *APP entities*: tomem medidas razoáveis para proteger as informações pessoais que detêm contra uso indevido, interferência e perda, bem como contra modificação ou divulgação; tomem medidas razoáveis para destruir ou tornar anônimas as informações pessoais que não são mais necessárias.

[147] *Bill Digest nº 30, 2022-23*, disponível em https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2223a/23bd030. Acesso em 20 Dez. 2022.

Commissioner utiliza como parâmetro as decisões em casos de antidiscriminação e, em relação às perdas econômicas, verifica se a perda foi diretamente causada pela ação ou inação do respondente (WITZLEB, 2018). Esses testes podem ser resumidos em dois questionamentos: um atinente ao histórico sobre como um determinado dano ocorreu; e outro de cunho normativo acerca da possibilidade e razoabilidade de a responsabilidade legal pelo dano específico ser atribuída a uma determinada pessoa (WITZLEB, 2018, p. 389). Mesmo quando as determinações envolvem compensações financeiras, a decisão sobre uma determinação fica a critério do *Commissioner* e não tem efeitos executórios. Assim, o OAIC deve litigar no Tribunal (*Federal Court of Australia* ou *Federal Circuit and Family Court of Australia*) contra a entidade regulada considerada culpada de interferência grave ou repetida com a privacidade para buscar a imposição de penalidade civil. A penalidade civil foi aplicada apenas uma vez[148], desde seu início em março de 2014. Na ocasião, o OAIC aplicou uma penalidade civil à *Meta* (*Facebook*) referente ao escândalo de dados da *Cambridge Analytica* ocorrido na década de 2010.

Mesmo com todas as emendas adicionadas ao *Privacy Act 1988* (Cth) e com a construção de suas regras como uma colcha de retalhos de estímulo internacional e resposta nacional, como ocorreu com as leis de privacidade em todo o mundo, a forma como a privacidade é considerada no sistema jurídico australiano continua desatualizada para proteger efetivamente a proteção de dados pessoais como um direito da personalidade. Isso ocorre porque não existe o direito de controlar o uso de dados pessoais pelo titular dos dados. Esse tipo de controle é extremamente importante no contexto da sociedade informacional, na qual as pessoas são medidas e definidas por seus registros digitais. Também é fundamental proteger a integridade do corpo digital (parte da dignidade como seres humanos).

Enfatizando a desconexão da noção de privacidade na legislação australiana com o contexto atual da sociedade da informação, Giorgina Dimmopoulos (2022) argumenta que a Austrália ainda não tem um direito à privacidade estabelecido. Isso ocorre porque a Austrália continua reconhecendo o direito à privacidade com um entendimento de " *privacy as protection against the misappropriation or misuse of personal information, and as the antitheses of publicity* "[149] (DIMOPOULOS, 2022, p. 8).

---

[148]Para detalhes, consultar o site do OAIC Disponível em https://www.oaic.gov.au/newsroom/commissioner-launches-federal-court-action-against-facebook. Acesso em 25 Jan. 2023.

[149] "privacidade como proteção contra a apropriação indevida ou uso indevido de informações pessoais e como antítese da publicidade" (DIMOPOULOS, 2022, p. 8)

No *Privacy Act 1988* (Cth), não há definição de "privacidade", a forma como a proteção é fornecida ocorre por meio da definição de "interferências na privacidade" na Seção 13, e é com base na análise do texto que é possível extrair uma noção de privacidade como antítese da publicidade. A noção de "interferência na privacidade" é limitada e técnica, significando principalmente a prática que viola um APP ou um *APP Code* registrado aplicável, que é um código de prática escrito sobre privacidade de informações, geralmente específico para uma determinada entidade ou setor, registrado pelo *Privacy Commissioner* que funciona como um instrumento legislativo. O *Privacy Act 1988* (Cth) fornece um conceito[150] de "informações pessoais" ao invés de “dado pessoal”, como informações ou opiniões sobre um indivíduo identificado, ou um indivíduo que seja razoavelmente identificável, sejam elas verdadeiras ou não, e estejam elas registradas de forma material ou não. Nota-se, assim, que no contexto australiano, não apenas a identificabilidade do indivíduo define uma informação como pessoal, mas também o fato de que a informação seja sobre o indivíduo. De forma um pouco diferente, a LGPD considera dados pessoais como qualquer informação relacionada a uma pessoa física identificada ou identificável (da mesma forma que o *GDPR*).

É interessante notar que a lei australiana concebe a privacidade de forma semelhante ao que é defendido nos EUA, ou seja, que a privacidade é um componente do patrimônio dos indivíduos. Como afirma Stefano Rodotà (2008), esse tipo de abordagem baseada na propriedade é uma concepção errônea que representa uma ameaça à privacidade, pois permite uma interpretação de que, uma vez que se receba um pagamento, a pessoa pode ter sua vida privada invadida legitimamente. Além de apontar para a disponibilidade de um direito fundamental de grande importância a proteção do corpo digital. Embora esse seja um caminho comum em outros sistemas jurídicos, ou seja, uma concepção patrimonial que evolui para uma compreensão mais profunda da privacidade como parte da personalidade, como um direito fundamental, ela estimula uma compreensão deficiente da privacidade e da proteção de dados, o que argumenta que a aplicação do espaço aberto protegido está sujeita a violações. "[...] O direito à proteção de dados tem a ver com a proteção da personalidade, não da propriedade. Isso significa que certas categorias de dados, especialmente as de natureza médica e genética, não podem ser usadas para fins comerciais." (RODOTÀ, 2008, p. 19).

Vale mencionar, adicionalmente, que o *Privacy Act 1988* (Cth) não fornece uma lista de bases legais expressas para o tratamento de informações pessoais, como faz a LGPD. Em vez disso, estabelece uma proibição geral sobre a coleta, uso ou divulgação de informações

[150] Seção 6 do *Privacy Act 1988* (Cth).

pessoais sensíveis, a menos que haja consentimento do titular dos dados ou uma das isenções aplicáveis. Além disso, o *Privacy Act 1988* (Cth) estabelece que as informações pessoais só podem ser coletadas ou mantidas por meios justos e legais e devem ser razoavelmente necessárias para as funções e atividades da *APP Entity.*

Em essência, mesmo com uma lei de privacidade, a Austrália pode melhorar sua aplicação para proteger esse direito. De acordo com David Vaile, em uma entrevista concedida em 2014, o *Privacy Act 1988* (Cth) "*gives the right to complain to the Privacy Commissioner, but there have only 11 determinations since the regime started in the late 1980s (an average of 0.26 matters leading to a determination per year*"[151] (20 Law Society Journal, 2014). Na oportunidade, Vaile alegou que não há proteção real à privacidade na Austrália, uma vez que não há nenhum direito aplicável sendo de fato protegido. Reforçando esse reconhecimento, Witzleb (2018) destaca que a reclamação pode resultar em determinações do *Office of the Australian Information Commissioner* (OAIC), no entanto, esse poder detido pelo OAIC não foi usado por muitos anos, resultando em inefetividade da tutela.

> […] The Privacy Commissioner is required to investigate a complaint if the act or practice in question may be an interference with the complainant's privacy and the complainant has first complained to the respondent. If an investigation by the Privacy Commissioner substantiates the complaint, the Commissioner has several remedial options, including the power to make a 'determination'.
> The Office of the Privacy Commissioner initially adopted a 'light touch' approach to regulation, which aimed to resolve most complaints through conciliation. In the first two decades of the Privacy Act's operations, determinations were exceedingly rare: over the first 20 years of the Privacy Act's operation, successive Commissioners issued only eight determinations. This led to criticism that the Office was too reluctant to use its powers and missed the opportunity to strengthen compliance with Australia's privacy laws through a more transparent and robust approach to enforcement. (WITZLEB, 2018, p. 378).

Isso revela que embora haja ferramentas disponíveis para o OAIC para reforçar a privacidade, elas não foram usadas por muito tempo. Conforme demonstrado até o final deste capítulo, esse cenário está mudando. Angelene Falk, atual Comissária (no cargo desde agosto de 2018), tem usado o poder de fazer determinações com mais frequência após a frustração da conciliação. Além disso, é notável que o direito de reclamar ao OAIC surge após a tentativa anterior de resolução com quem violou o direito informacional restar frustrada (o mesmo acontece com relação a fazer reclamações à autoridade brasileira de privacidade - ANPD). Assim, a única via disponível para o indivíduo que se sente alvo de interferência em sua privacidade é a administrativa. Isso significa que o titular dos dados não pode recorrer à justiça

[151] "dá o direito de reclamar ao Comissário de Privacidade, mas houve apenas 11 determinações desde que o regime começou no final da década de 1980 (uma média de 0,26 questões que levam a uma determinação por ano" (20 Law Society Journal, 2014). *Tradução nossa.*

batendo diretamente às portas do Judiciário, porque o sistema jurídico australiano ainda não tem uma causa de ação para a violação da privacidade.

No sistema de proteção de dados brasileiro (lastreado na LGPD), o titular dos dados tem múltiplas formas de agir em defesa de seus direitos à privacidade e à proteção de dados, ao menos em teoria, como reclamar à autoridade nacional diretamente, depois de reclamar ao processador ou controlador (agentes de tratamento para usar os termos da lei brasileira) e mover ações judiciais. Outro ponto interessante é que a LGPD e o sistema jurídico brasileiro permitem a defesa dos direitos à privacidade e à proteção de dados de forma singular ou coletiva. No entanto, o OAIC tem uma gestão mais eficaz das reclamações apresentadas a ele do que a ANPD, porque a ANPD não dá andamento às denúncias e às petições de forma singular, como faz o OAIC. A ANPD agrega as reclamações e as utiliza como referência para planejar suas ações investigativas. Como resultado, a apresentação de uma reclamação à ANPD (seja uma denúncia ou uma petição) tem o efeito apenas de contribuir para a política pública de proteção de dados em termos de seu engajamento, mas não é uma forma de resolver o problema do titular dos dados com relação à sua proteção de dados. A inexistência de resolução do problema em âmbito administrativo no Brasil gera um efeito de dissuasão, e pode sinalizar erroneamente para a menor importância do direito à proteção de dados, repercutindo negativamente na cultura de privacidade. Mesmo quando a ANPD começar a aplicar punições ao final das investigações administrativas, todas as sanções financeiras serão direcionadas ao fundo de defesa dos direitos difusos (art. 52, §5º, LGPD).

É importante observar que, assim como a LGPD (e a maioria das leis de privacidade em todo o mundo[152]), o *Privacy Act 1988* (Cth) não trata da privacidade de grupos ou de dados agregados. No caso de dados agregados, a identificabilidade dos indivíduos dos quais os dados foram coletados subsiste, se os dados forem considerados com informações adicionais. No caso de dados de grupo, mesmo que não seja possível identificar um membro do grupo, o que subsiste é a probabilidade de dano ao grupo, explicada mais adiante. A abordagem relativa à proteção de dados de grupos é extremamente necessária atualmente e provavelmente será um tópico de tendência em breve em nível internacional.

[152] "Since the OECD Guidelines were adopted in 1980, every major international privacy and data protection instrument, has formed a regulatory framework Around the concept of "personal data" or "personal information". The year after the OECD Guidelines were adopted the Council of Europe opened the Convention for the Protection of individuals with regard to the Automatic Processing of Personal Data (Treaty No 108) for signature (and accession by non-member states) in 1981. Notable about the title of Treaty No 108 is not only the focus on "personal data" but also the explicit recognition that the Convention is for the protection of *individuals.* In 1995 the EU Data protection Directive (95/46/EU) was adopted, and this was subsequently followed and replaced by the EU General Data Protection Regulation (GDPR) (2016/679). Both of these international instruments are founded on the belief that the proper object of concern is "personal data"." (TAYLOR, 2020, p. 733).

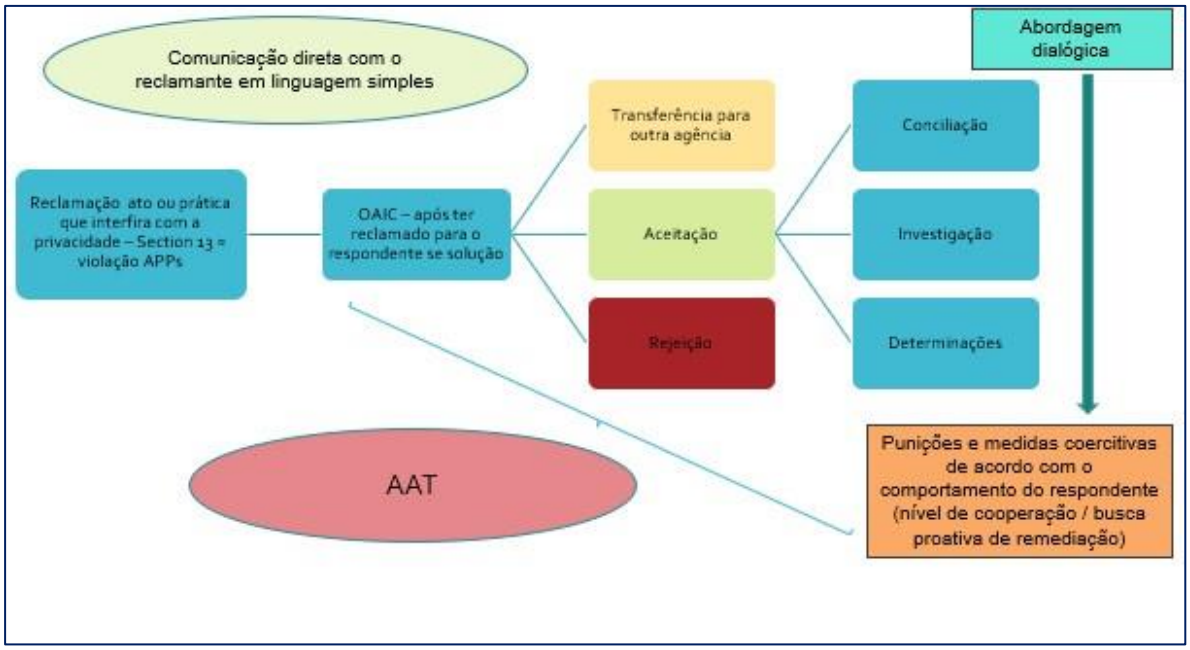

Figure 8 – Infográfico reclamação por interferência na privacidade - Fonte Autora om base no Privacy Act 1988 (Cth) e nas diretrizes do OAIC

O dano causado pelo tratamento naturalizado de dados de grupos como fora do domínio da privacidade é uma ameaça à democracia e à autonomia. Conforme observado por Stéfano Rodotà.

> [...] mesmo as coletâneas de dados anônimos podem ser manipuladas de forma gravemente lesiva aos direitos dos indivíduos: tenha-se em mente o uso que pode ser feito dos dados, agregados, que digam respeito a uma minoria racial ou linguística; ou às consequências de uma decisão política ou econômica tomada justamente com base na análise dos dados anônimos. Por que não permitir, também nesses casos, uma intervenção dos interessados com a finalidade de controlar a exatidão das informações coletadas e a correção do seu tratamento, exigindo, se necessário, as retificações oportunas? (RODOTÀ, 2008, p. 32)

No entanto, conforme demonstrado nos capítulos anteriores, a importância da privacidade e da proteção de dados é mais profunda e está relacionada a como os dados pessoais constroem um corpo digital, usado para subsidiar julgamentos e decisões sobre os titulares dos dados na sociedade informacional, em que a vida ocorre numa trama que uma mistura os mundos material e digital. Nesse contexto, os dados acumulados e as decisões informadas por esses dados afetam e impactam as chances e oportunidades dos seres, tornando o grupo vulnerável. As preocupações com os dados do grupo estão surgindo no contexto da pesquisa biológica e médica, considerando seus possíveis efeitos de submeter o grupo à discriminação[153]. Considerando-se o uso da tecnologia de reconhecimento facial e todas as questões relativas ao

[153] Sobre o tema recomenda-se a leitura de artigo de Joan L. McGregor intitulado "*Population Genomics and Research Ethics with Socially Identifiable Groups"*, publicado no J*ournal of Law, Medicine and Ethics* (2007, p. 356-370).

viés algorítmico, os corpos físicos de grupos em vulnerabilidade já são alvos de danos provenientes de decisões automatizadas, o que torna pertinente o argumento de Achille Mbembe (2019) de que os corpos são fronteiras na sociedade informacional ante o uso crescente da tecnologia. Conforme mencionado por Carissa Véliz (2021, p. 232), "a privacidade é uma questão coletiva e política", especialmente em uma era em que as plataformas digitais, o *big data*, a IA, entre outros componentes e derivados desempenham um papel crucial na vida de todos. Na sociedade informacional, muitos padrões de grupo que antes não eram percebidos podem ser mapeados.

Tendo analisado o contexto geral da estrutura do *Privacy Act 1988* (Cth), percebe-se que, enquanto a estrutura jurídica brasileira é, pelo menos em teoria, mais adequada para proteger os interesses do titular dos dados, com foco nos direitos fundamentais (foco no titular dos dados, no indivíduo e em sua expressão na sociedade informacional), a estrutura jurídica australiana é mais voltada para a segurança da informação, com forte ênfase nas informações pessoais em si.

A proteção mais forte dos direitos da personalidade no sistema jurídico brasileiro resulta de uma tradição jurídica e cultural e de uma influência relevante dos sistemas jurídicos nacionais europeus, conforme observado por Danilo Doneda e Raphael Zanatta[154] (2022). É possível inferir que o cenário jurídico australiano da privacidade busca atuar com base na educação para a privacidade, aplicando suas regras por meio de aconselhamento e orientando a forma correta de cumprir os APPs. No atual estágio de maturidade, o sistema brasileiro em nível administrativo também está focado na finalidade educativa, embora a LGPD admita modalidades de punição para os agentes de tratamento que violam a lei. No entanto, o OAIC desempenha um papel melhor do que a ANPD até o momento em sua intenção de moldar a conformidade cultural com a privacidade, considerando a forma como a autoridade australiana de privacidade lida com as reclamações, processando-as individualmente.

Ademais, a legislação brasileira tem uma proteção mais forte à privacidade no panorama normativo, já que desde a *Constituição Federal de 1988*[155] tutela a privacidade como direito fundamental. Entretanto, a efetividade dessa proteção depende fortemente de processos de judicialização, que sempre representam um custo para os indivíduos. Custo não somente em

[154] In: ALBERS, Marion; SARLET, Ingo Wolfgang (Ed.). **Personality and Data Protection Rights on the Internet: Brazilian and German approaches.** Cham: Springer, 2022.
[155] A *Constituição Federal* brasileira considera a privacidade u direito fundamental desde a sua promulgação. Em 2022 através da Emenda Constitucional 115/2022 o direito à proteção de dados passou a compor o rol de direitos fundamentais também.

termos financeiros, mas em demanda por conhecimento, por assistência jurídica e judiciária, sem mencionar a maior morosidade para a solução pela via judicial.

Assim, mesmo que o plano normativo australiano não preveja um direito à privacidade ou à proteção de dados propriamente dito, permitindo a busca pelo indivíduo da sua concretização pela judicialização, a tutela à privacidade é concretizada de maneira mais célere (conforme informações dispostas nos relatórios de desempenho do OAIC[156] a solução das reclamações de interferência com a privacidade tem sido alcançada em um tempo médio de 4,4 meses), mais barata (o peticionamento ao OAIC ocorre sem custo) e mais satisfatória, por já haver a composição de danos na esfera administrativa. Essa maneira de resolução apela para o entendimento de que a privacidade é importante, por isso o regime regulatório estabelece mecanismos democráticos para que o titular busque a sua concretização. A próxima seção aborda os mecanismos de *enforcement* existentes no sistema de proteção do *Privacy Act 1988* (Cth).

5.3 *Enforcement* da privacidade na aplicação do *Privacy Act 1988* (Cth)

Esta seção é dedicada à análise das decisões tomadas pelo OAIC, pelo AAT e pela FCA de acordo com o *Privacy Act 1988* (Cth), de 2020 a 2022. A pesquisa de decisões foi realizada usando "Privacy Act 1988 (Cth)" como indexador. As análises foram feitas para acessar não apenas os pontos mais relevantes do *Privacy Act 1988* (Cth) para os reclamantes, mas também como os agentes de tratamento de dados estão lidando com a privacidade na Austrália. Essas análises são importantes para a tese para averiguar o nível de efetividade da proteção conferida pela norma na prática, no sentido de proteger o corpo digital.

O AAT é a primeira instância para revisão das determinações do OAIC[157] e tem a natureza jurídica de uma agência de revisão de mérito, podendo, portanto, revisar questões factuais além das próprias decisões. Os reclamantes também podem solicitar uma revisão judicial perante o *Federal Circuit Court* (FCFCOA)[158] ou a *Federal Court of Australia* (FCA)

---

[156] Disponível em: https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/oaic-annual-reports/annual-report-201819/part-1-overview Acesso em 03 Jul. 2023.

[157] O OAIC pode decidir fazendo declarações e determinações. De modo geral, as determinações são feitas com a intenção de recomendar medidas a serem adotadas pelo requerido para remediar as situações e para evitar novas violações (foco na prevenção). As determinações são tratadas na Seção 96 do *Privacy Act 1988* (Cth).

[158] A *Federal Circuit and Family Court of Australia* (FCFCOA) também é responsável pela aplicação das determinações do OAIC. Os procedimentos de execução são instituídos por um reclamante ou pelo Comissário. Os procedimentos são feitos por meio de audiência de novo, mas as provas recebidas pelo Comissário estão disponíveis para a Corte, assim como as razões do *Commissioner*. O *Commissioner* pode emitir um certificado que

com relação a um erro na aplicação da lei pelo OAIC ou relacionado a um exercício indevido de poder pelo *Information Commissioner*. Os pedidos de revisão devem ser apresentados em até 28 dias a partir da data da determinação.

Perante o FCA, muitos casos importantes foram apresentados com relação à interpretação dada ao *Privacy Act 1988* (Cth). A pesquisa jurisprudencial foi realizada usando o mesmo indexador: "Privacy Act 1988 (Cth)", durante o mesmo período. O propósito de comparação entre o arcabouço australiano e o brasileiro justifica o período selecionado para a pesquisa. Conforme mencionado, a LGPD entrou em vigor em setembro de 2020. Além disso, desde 2019, uma série de violações de dados ocorreu no Brasil e na Austrália, colocando a privacidade como um assunto em voga. Em 2020, a pandemia da COVID-19 impactou a forma como as pessoas levam suas vidas em todo o mundo, acelerando a onipresença e a popularidade de muitas tecnologias que permitem interações remotas. Toda essa interação usa e produz dados, especialmente dados pessoais, o que torna mais evidente o temor quanto ao tratamento indevido dessas informações. Além disso, o Brasil e a Austrália (assim como outros países) tentaram[159] se precaver contra o avanço da pandemia usando tecnologia de vigilância. Em todo o mundo, até mesmo atividades sensíveis, como a jurisdição, foram realizadas remotamente, intermediadas por plataformas digitais, fazendo com que todas as informações geradas estivessem nas mãos de empresas privadas.

A exploração das decisões administrativas e judiciais foi realizada em três etapas. Primeiro, orientada pelo levantamento quantitativo, descrevendo as conclusões por ano em cada autoridade com base no indexador utilizado. Segundo, guiado por uma abordagem qualitativa, analisando cada uma das decisões, para identificar se o retorno da busca é pertinente com o *Privacy Act 1988* (Cth). E, por fim, analisando o conteúdo dos resultados considerados pertinentes às demandas de privacidade, categorizando as decisões de acordo com a

---

seja prova prima facie de uma violação do código de privacidade relevante ou dos Princípios de Privacidade da Austrália. Veja mais em: https://www.fcfcoa.gov.au/gfl/administrative-privacy. No entanto, no site da FCFCOA há informações sobre sua jurisdição, indicando que a FCFCOA tem jurisdição para ouvir qualquer assunto dentro da jurisdição do FCA que este transfira para o FCFCOA. Além disso, ao tentar obter resultados para uma pesquisa sobre o cumprimento da determinação, o sistema conduz a uma página relacionada às decisões do OAIC. Acesso em 10 Jan. 2023.

[159] Ambos os países falharam em seus propósitos por motivos diferentes. No Brasil, esse uso foi negado pelo Supremo Tribunal Federal (STF), que considerou a lei (MP 954/2020) que propunha a vigilância muito vaga e intrusiva, pois não demonstrava uma finalidade legítima para todos os dados que seriam coletados. Como resultado, o STF considerou a lei uma violação do direito constitucional à privacidade e um desrespeito ao direito fundamental à proteção de dados. Diferentemente, no contexto australiano, um aplicativo para smartphone foi lançado pelo governo australiano, o COVIDSafe, usado para auxiliar os rastreadores de contatos. Embora o aplicativo tenha se tornado muito popular, no espaço de um mês, ele revelou apenas um caso extra de COVID-19, tornando a invasão um custo enorme em comparação com a operação esperada. Consulte https://www.innovationaus.com/justice-kirby-on-why-we-must-fight-for-privacy/. Acesso em 30 Nov. 2022.

preocupação principal (interpretação de termos legais, tipos de violações mais comuns, entre outros).

Em geral, a aplicação do indexador mencionado retornou com: em 2020, houve 13 determinações feitas pelo OAIC, 1 recurso decidido pelo AAT, 18 decisões feitas pela FCA e nenhum dado disponível com relação ao FCFCOA; em 2021, houve 20 determinações feitas pelo OAIC, 3 recursos decididos pelo AAT, 9 decisões feitas pela FCA e nenhum dado disponível com relação ao FCFCOA; em 2022, houve 10 determinações feitas pelo OAIC, 7 recursos decididos pelo AAT, 22 decisões feitas pela FCA e nenhum dado disponível com relação ao FCFCOA. Os dados relacionados são demonstrados visualmente no gráfico a seguir.

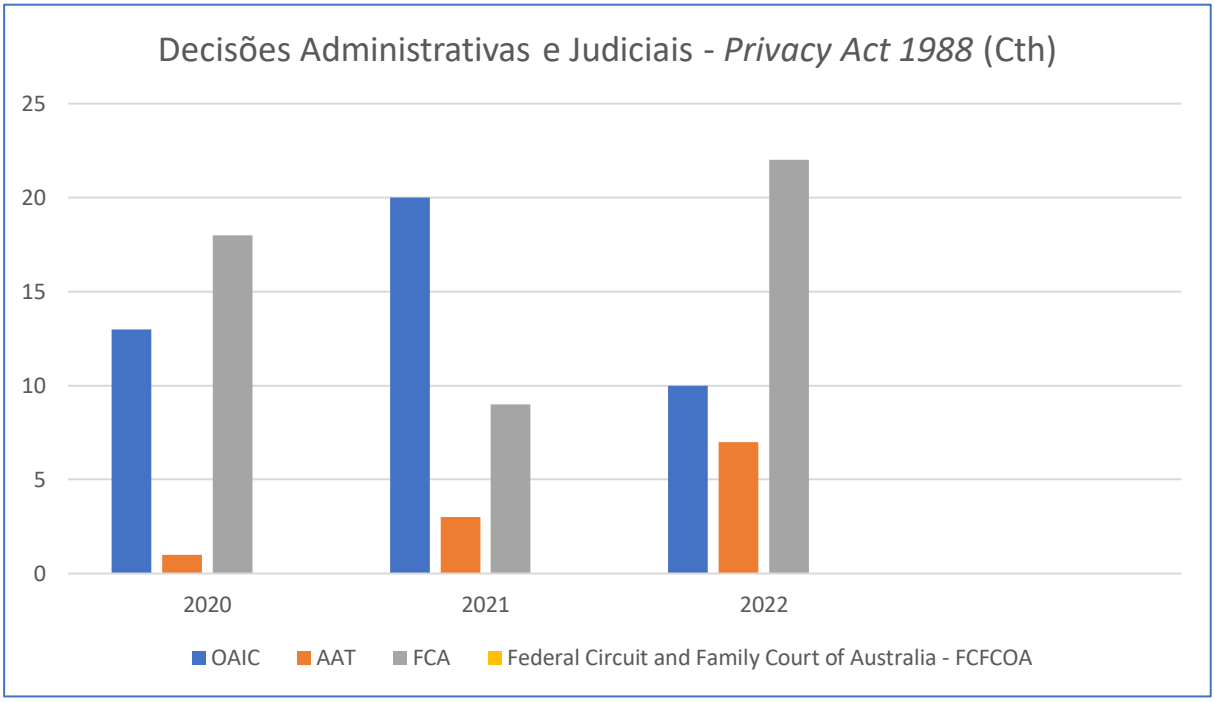

Figure 9 – Gráfico de decisões administrativas e judiciais Privacy Act 1988 (Cth) - Fonte - Autora com base nas decisões encontradas

5.3.1 Decisões do *Office of Australian Information Commissioner* – OAIC

O OAIC[160] é um órgão regulador nacional independente e tem competências relacionadas não apenas à regulação de interferências na privacidade, mas também à regulação da liberdade de informação, de acordo com o *Freedom of Information Act 1982* (Cth)[161]. Isso

[160] Veja mais em https://www.oaic.gov.au/. Acesso em 08 Fev. 2023.

[161] O *Freedom of Information Act 1982* (Cth) tem objetivos semelhantes aos da *Lei de Acesso à Informação* brasileira (*Lei Federal nº 12.527/2011*). Assim, essa lei tem como objetivo dar à comunidade australiana acesso às informações mantidas pelo governo da Commonwealth, exigindo que os órgãos publiquem as informações e

significa que o OAIC exerce uma função dupla, recebendo reclamações referentes a esses dois campos diferentes e, para promover e defender a privacidade e os direitos de acesso à informação, o OAIC tem poderes para conduzir investigações, lidar com reclamações, revisar decisões tomadas de acordo com o *Freedom of Information Act 1982* (Cth), monitorar a administração de entidades reguladas e aconselhar o público, organizações e agências sobre privacidade e liberdade de informação.

O OAIC foi criado em 2010 pelo *Australian Information Commissioner Act 2010* (Cth). Desde então, o órgão anterior que costumava supervisionar as reclamações relacionadas a interferências na privacidade, o *Office of the Privacy Commissioner,* foi integrado à sua estrutura. A organização atual de suas funções executivas é retratada no infográfico abaixo (figura 10).

Uma das intenções da revisão em andamento do *Privacy Act 1988* (Cth) é "aumentar as penalidades máximas de acordo com o *Privacy Act 1988* (Cth) e fornecer ao *Office of Australian Information Commissioner* poderes de aplicação aprimorados"[162] (CTH, 2022). As emendas darão mais poder ao OAIC para aprofundar sua função de investigação independente e proativa das agências de acordo com a lei. Até junho de 2023, a resposta do governo[163] ao *Privacy Act Review Report*, divulgado em 26 de fevereiro de 2023, não estava disponível, pois a coleta de opiniões sobre as 116 propostas contidas no relatório foi encerrada em 31 de março de 2023.

De acordo com a Seção 52 do *Privacy Act 1988* (Cth), quando uma investigação estabelece uma interferência na privacidade, o *Commissioner* pode fazer determinações quando uma reclamação não é resolvida por meio de conciliação. Essas determinações não são

concedendo o direito de acesso aos documentos. O OAIC trabalha nesse campo, revisando as solicitações feitas a uma agência da Commonwealth para acessar informações ou documentos quando o reclamante não concorda com o resultado.

[162] Consulte o site do *Attorney-General's Department* sobre a revisão do *Privacy Act 1988* (Cth). Disponível em https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988. Acessado em 20 Jun. 2023.

[163] Para obter mais informações sobre o processo de revisão, consulte https://consultations.ag.gov.au/integrity/privacy-act-review-report/. Acesso em 21 de Jun. de 2023.

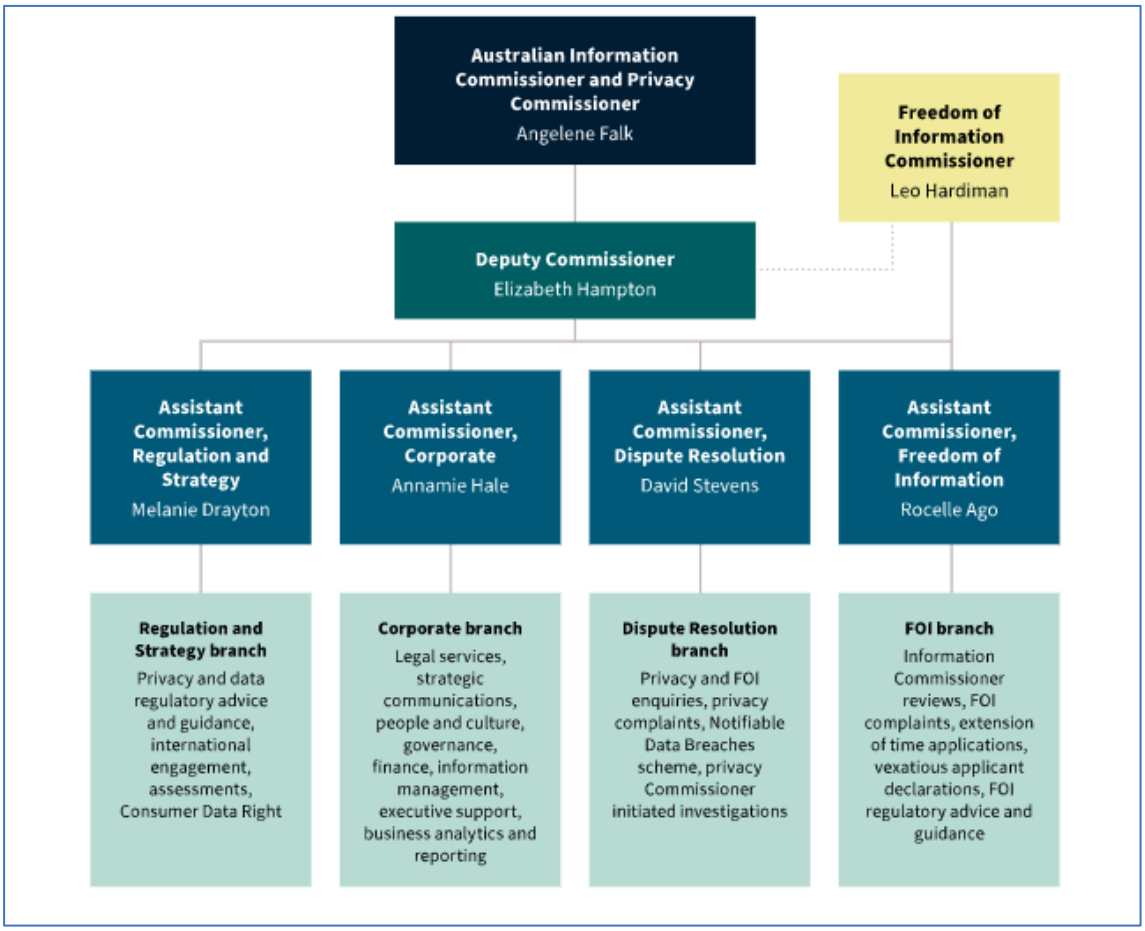

Figure 10 – Infográfico estrutura organizacional OAIC - Fonte: OAIC website - Fev. 2023.

irrestritas, são limitadas a várias declarações específicas e não são legalmente exequíveis. De acordo com Witzleb,

> […]This reflects the fact that Commonwealth judicial power can only be exercised by a court in accordance with Chapter III of the Australian Constitution. The Commissioner is not vested with judicial power, and cannot make a biding and directly enforceable decision that a breach of the Privacy Act has occurred and must be remedied. Therefore, if the respondent fails to act in accordance with the declaration or declarations made in the determination, the applicant or the Commissioner can seek to enforce the determination in Federal Court or the Federal Circuit Court of Australia. (WITZLEB, 2018, p. 381)[164]

A Seção 96 do *Privacy Act 1988* (Cth) afirma que as decisões tomadas de acordo com a Seção 52 estão sujeitas ao AAT, que fornece uma revisão de mérito independente das decisões. O AAT tem o poder de anular, modificar, ou ratificar uma determinação de privacidade (WITZLEB, 2018, p. 381). Isso é semelhante ao que está previsto na legislação

[164] [...] Isso reflete o fato de que o poder judicial da Commonwealth só pode ser exercido por um tribunal de acordo com o Capítulo III da Constituição Australiana. O Comissário não está investido de poder judicial e não pode tomar uma decisão vinculativa e diretamente executável de que ocorreu uma violação da Lei de Privacidade e que deve ser corrigida. Portanto, se o requerido não agir de acordo com a declaração ou declarações feitas na determinação, o requerente ou o Comissário podem buscar a execução da determinação no Tribunal Federal ou no Tribunal do Circuito Federal da Austrália. (WITZLEB, 2018, p. 381). *Tradução nossa.*

brasileira, em que as decisões administrativas não são finais e estão sujeitas à revisão judicial, uma vez que o Brasil tem um sistema de jurisdição una, de acordo com sua *Constituição Federal de 1988* (art. 5º, XXXV). No entanto, no Brasil, a revisão judicial é realizada apenas em relação à legalidade e à possível abusividade dos atos administrativos. Conforme mencionado por Antônio Sepulveda, Carlos Bolonha e Igor de Lazari (2019, p. 1), no Brasil, os órgãos administrativos recebem o "benefício da perícia especializada"[165]. O STF[166], a mais alta corte do Brasil, entende que a revisão judicial dos atos administrativos se limita à análise de eventual ilegalidade e abusividade, sendo inadmissível a revisão quanto ao mérito em razão do princípio constitucional da separação dos poderes.

Os resultados confirmaram que, no estado atual da legislação australiana, a dificuldade em identificar interferências na privacidade está ligada à inexistência de um "direito à privacidade" propriamente dito. Witzleb (2018, p. 395) menciona, como a pesquisa confirmou, que até o momento nem a lei comum nem o *Privacy Act 1988* (Cth) reconhecem explicitamente um “direito à privacidade". Conforme mencionado em relação ao contexto brasileiro, a existência de um direito expressamente reconhecido por lei é importante em termos de efetividade, pois possibilita ao sujeito de direito buscar a concretização por meio da jurisdição.

A partir da pesquisa sobre as decisões tomadas pelo OAIC em relação ao *Privacy Act 1988* (Cth), foram encontradas 40 decisões pertinentes, que foram analisadas em detalhes: Analisando as decisões ano a ano, em 2020 o APP mais violado foi o APP 11 (relativo à segurança de informações pessoais), seguido pelo APP 12 (atinente ao acesso a informações pessoais) e APP 6 (pertinente ao uso ou divulgação de informações pessoais). De 13 decisões com foco em privacidade, o *Privacy Act 1988* (Cth) foi fundamental para a discussão em 11. Em 2 casos, o *Privacy Act 1988* (Cth) foi citado apenas para se referir ao conceito de informações pessoais, e os casos eram sobre o *Crimes Act 1914* (Cth). Do número total de casos, apenas 4 eram sobre organizações ou entidades públicas como respondentes. Apenas 3 decisões concederam danos agravados. Apenas um caso, *[2020] AICmr 57*, foi iniciado sem uma reclamação, por uma investigação independente, de acordo com a Seção 40, sobre uma grande violação de dados causada pelo *Flight Centre Travel Group Ltd*. que afetou 6.919 indivíduos. Só uma reclamação foi indeferida. Por fim, o maior valor de indenização concedido foi de AU$ 13.400 em um caso grave de divulgação ilegal motivada por erro humano envolvendo dados

[165] Veja mais sobre o assunto no artigo "*Judicial Defence to Agencies' Decisions in Brazil and the United States*". Disponível em: https://www.theregreview.org/2019/07/24/sepulveda-bolonha-delazari-judicial-deference-agencies-decisions-brazil-united-states/. Acesso em 20 Jun. 2023.

[166] Veja as decisões tomadas no ACO 3568 Ref (2023), RE 1269736 ED-AgR (2022), RE 1222222 AgR (2020), entre outros.

confidenciais relacionados à saúde (*'SD' e 'SE' e Northside Clinic (Vic) Pty Ltd [2020] AICmr 21*).

Para esclarecer como foram perpetradas as principais interferências na privacidade, é relevante tratar de alguns detalhes dos casos em análise. A violação do APP 11 foi declarada a partir da constatação do uso indevido de informações pessoais, o que se tornou flagrante pelo fato de a organização não ter tomado medidas razoáveis para proteger as informações mantidas, por exemplo, no caso *'SD' e 'SE' e Northside Clinic (Vic) Pty Ltd [2020] AICmr 21*. Nesse caso, um e-mail com documentos referentes à participação em pesquisa experimental sobre o tratamento da AIDS foi enviado a dois indivíduos em um relacionamento do mesmo sexo (um deles tinha acabado de descobrir que estava infectado com o vírus da AIDS), mencionando o relacionamento deles e a doença. No entanto, o e-mail foi enviado para um endereço válido que não pertencia aos solicitantes, revelando todas as informações pessoais confidenciais a um terceiro. O OAIC declarou a violação do APP 6, ao passo que os dados foram usados com desvio da finalidade original para a qual foram coletados, e do APP 11, pela falha em checar os endereços de e-mail antes do compartilhamento das informações sensíveis.

Em outro caso, *'VI' e CSIRO (Privacy) [2020] AICmr 44*, envolvendo a divulgação de informações pessoais em um pedido de indenização de um trabalhador, o OAIC declarou a violação do APP 11 e do APP 6, porque uma pessoa da equipe da organização que no exercício de suas funções estava dando andamento à indenização, usou as informações pessoais divulgadas pelo indivíduo ao solicitar indenização para se valendo delas formular um pedido pessoal, em um flagrante desvio de finalidade. Por fim, em relação ao APP 11, em *'VJ', 'VK', 'VL' e 'VM' (Privacy) [2020] AICmr 45*, o *Commissioner* declarou uma violação da obrigação de tomar medidas razoáveis para proteger as informações mantidas pela entidade APP, porque, durante as audiências, a psicóloga (respondente e *APP entity* no caso) revelou que todos os prontuários médicos mantidos estavam armazenados em um armário localizado na garagem de sua residência (uma violação do APP 12 também foi declarada, pela demora da profissional em fornecer o acesso aos prontuários médicos exigidos pelos requerentes).

Todos os casos envolvendo uma violação do APP 12 estavam relacionados à relação médico-paciente, na qual os profissionais de saúde não forneceram devidamente aos requerentes (pacientes) acesso aos registros médicos (ver *'SF' e 'SG' (Privacy) [2020] AICmr 22, 'VJ', 'VK', 'VL' e 'VM' (Privacidade) [2020] AICmr 45*, *'VN' e 'VM' (Privacidade) [2020] AICmr 46*, e *'VU' e 'VV', 'VW' (Privacidade) [2020] AICmr 52*).

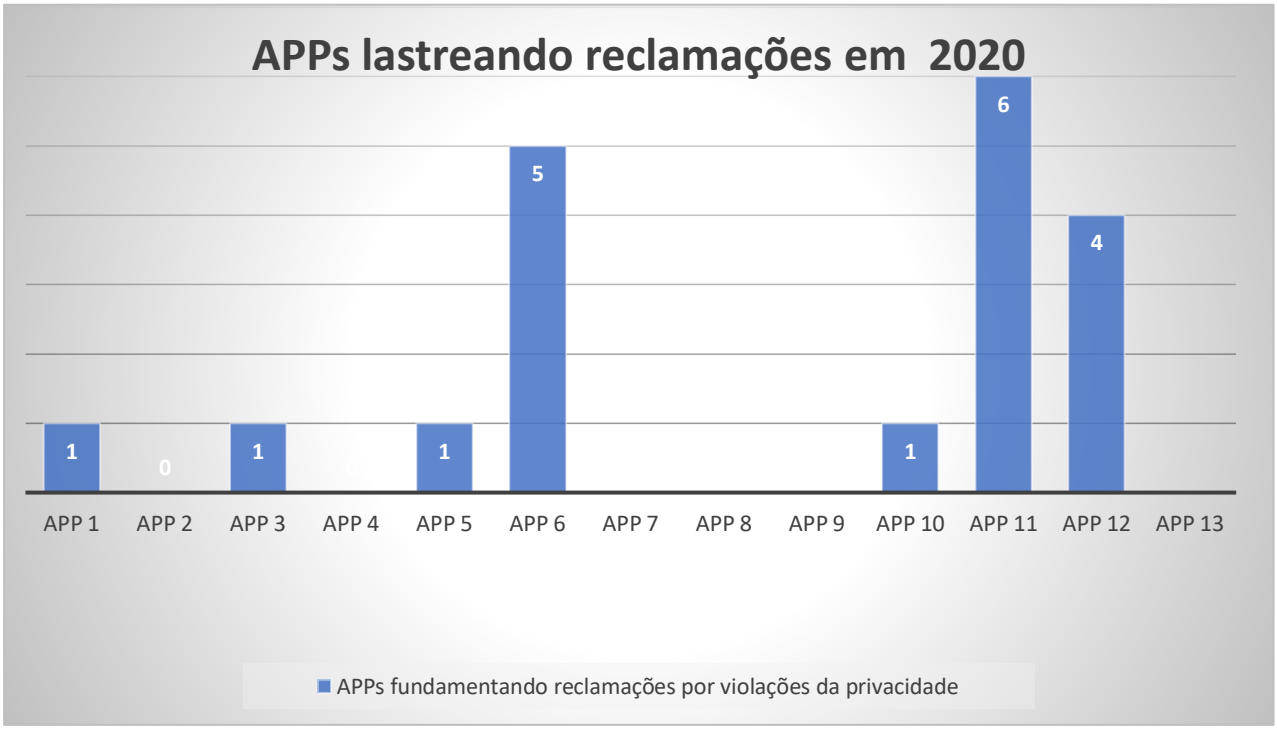

Figura 11- Gráfico APPs lastreando reclamações de privacidade em 2020 - Fonte Autora com base nas decisões do OAIC analisadas.

Em 2021, foram realizadas mais investigações independentes pelo OAIC[167]. Das 19 reclamações encontradas, 7 foram feitas contra organizações públicas[168] e 12 contra respondentes privados. Do total, 4 casos tiveram investigações iniciadas pelo OAIC, essas investigações foram motivadas pela violação de deveres de cuidado[169] após o uso irregular de dados confidenciais (dados biométricos faciais) sem uma Avaliação de Impacto na Privacidade (PIA) prévia e sem o consentimento regular e informado dos titulares dos dados[170]. Os APPs

[167] Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy) [2021] AICmr 34, Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) [2021] AICmr 50, Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54, and Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74. During the year were made 19 decisions, 7 dismissing the complaints after investigation ('WQ' and Commissioner of Taxation (Privacy) [2021] AICmr 4, 'WR' and Telstra Corporation Limited (Privacy) [2021] AICmr 5, 'WT' and Wurli-Wurlinjang Health Service (Privacy) [2021] AICmr 8, 'XO' and 'XP', 'XQ' t/a Priceline Pharmacy Camden (Privacy) [2021] AICmr 37, 'YD' and Secretary of the Department of Home Affairs (Privacy) [2021] AICmr 56, 'ZI' and MedHealth Pty Ltd t/as mlcoa (Privacy) [2021] AICmr 91, e 'ZN' and a School (Privacy) [2021] AICmr 95

[168] 'WP' and Secretary to the Department of Home Affairs (Privacy) [2021] AICmr 2, 'WQ' and Commissioner of Taxation (Privacy) [2021] AICmr 4, 'WZ' and Chief Executive Officer of Services Australia (Privacy) [2021] AICmr 12, 'XA' and Chief Executive Officer of Services Australia (Privacy) [2021] AICmr 13, 'YD' and Secretary of the Department of Home Affairs (Privacy) [2021] AICmr56, Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74, e 'ZJ' and Chief Executive Officer for the Australian Centre for International AgriculturalResearch (Privacy) [2021] AICmr 92.

[169] 'WP' and Secretary to the Department of Home Affairs [2021] AICmr 2 e Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. [2021] AICmr 34.

[170] [2021] AICmr 50 "Commissioner initiated an investigation into 7-Eleven Stores Pty Ltd", e [2021] AICmr 54 "Commissioner initiated na investigation into Clearview AI, Inc", e [2021] AICmr 74 "Commissioner initiated an investigation into the Australian Federal Police".

mais usados para embasar os casos foram a APP 6 (uso ou divulgação de informações pessoais - 9 casos), APP 11 (segurança de informações pessoais - 8 casos) e APP 10 (qualidade de informações pessoais - 7 casos).

É interessante notar que em 2021 não houve nenhuma decisão concedendo danos agravados. Esses dados indicam um entendimento progressivo por parte das entidades APP sobre a importância de cooperar durante as investigações do OAIC e adotar uma postura mais proativa ao lidar com informações pessoais, visto que desde 2018 o OAIC passou a usar mais os seus poderes de fazer determinações.

As violações em relação ao APP 6, por exemplo, ocorreram em um caso em que violações aos APP 11 e 10 também ocorreram, vide *'WZ' e Chief Executive Officer of Services Australia (Privacy) [2021] AICmr 12* - em que o novo endereço residencial de uma vítima de violência doméstica foi revelado ao seu ex-parceiro por engano, mesmo depois de a reclamante ter notificado a agência sobre a separação e solicitado a desvinculação de seu perfil daquele parceiro anterior (seu agressor). Este foi o caso em que ocorreu a compensação por perdas econômicas e não econômicas decorrentes da interferência na privacidade de valor mais alto: AU$ 19.980 (dezenove mil, novecentos e oitenta dólares australianos).

Em outros, a violação do APP 6 ocorreu pela divulgação de informações pessoais (endereço de e-mail a um terceiro sem consentimento – *'XU' e Amazon Australia Services Inc (Privacy) [2021] AICmr 42*, quando o reclamado (*Amazon*) estava dando feedback sobre uma acusação de difamação em um livro publicado anonimamente pelo reclamante em sua plataforma - e pela divulgação a uma agência externa de cobrança de dívida vencida de um reclamante *'XU' e Amazon Australia Services Inc (Privacy) [2021] AICmr 13*. Em relação ao APP 11, a declaração contra as práticas da *Uber* em *Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy) [2021] AICmr 34* foi feita porque a empresa não tomou medidas para garantir a segurança dos dados pessoais mantidos, ao passo que não comprovou possuir planos, políticas e procedimentos para orientar claramente sua equipe sobre a exclusão de informações não necessárias para a finalidade de seus serviços, sobre como agir para remediar uma violação detectada e outros requisitos estabelecidos para cumprir os APPs.

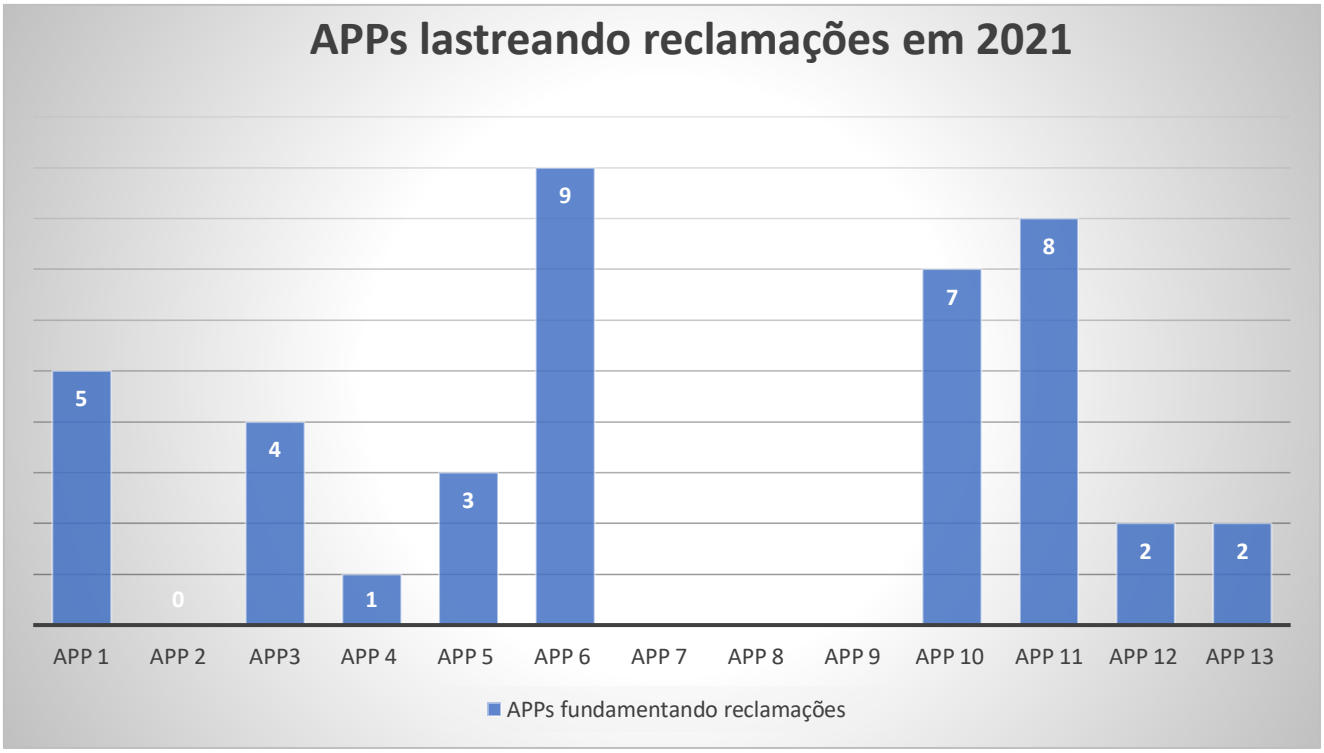

Figura 12 Gráfico APPs lastreando reclamações de privacidade 2021 - - Fonte Autora com base nas decisões do OAIC analisadas.

Em 2022, foram encontradas 10 decisões. Após avaliação adicional, restaram 8 decisões (as 2 não pertinentes eram sobre o *Freedom of Information Act 1982* (Cth)). Desses 8 casos, 1 era referente ao *Crimes Act 1914* (Cth)[171] e apenas citava o *Privacy Act 1988* (Cth) e, em 6 deles, os respondentes eram entidades ou organizações privadas, o que significa que entidades públicas foram respondentes em apenas 2 casos[172] decididos naquele ano. Os APPs mais usados para embasar as reclamações foram o APP 12 (acesso a informações pessoais), que apareceu em 3 casos[173], seguido pelo APP 5 (notificação da coleta de informações pessoais)[174] e 6 (uso ou divulgação de informações pessoais)[175], cada um deles apresentado em 2 casos, dados representados visualmente pelo gráfico abaixo. Apenas 2 reclamações foram indeferidas[176], e o único caso em que foi concedida indenização foi no valor de AU$ 2.500 para reparação de

[171] 'ABN' and CEO of the Independent Competition and Regulatory Commission ACT (Privacy) [2022] AICmr 48.
[172] '*ABN' and CEO of the Independent Competition and Regulatory Commission ACT (Privacy) [2022] AICmr 48*, regarding *Crimes Act 1914 (Cth)*, e *'ABR' and Civil Aviation Safety Authority (Privacy) [2022] AICmr 53.*
[173] *'AAQ' and Redimed Pty Ltd (Privacy) [2022] AICMr 7, 'AAS' and Spring Hill Specialist Day Hospital (The Trustee for QFD Day Theatres Unit Trust) (Privacy) [2022] AICmr 11*, e *'ABS' and Relationships Australia South Australia (Privacy) [2022] AICmr 54.*
[174] *'AAQ' and Redimed Pty Ltd (Privacy) [2022] AICmr 7, e 'ABR'* and *Civil Aviation Safety Authority (Privacy) [2022] AICmr 53.*
[175] *'ABG' and Body Corporate Services Pty Ltd (Privacy) [2022] AICmr 26*, e *'ABQ' and Serco Group Pty Limited (Privacy) [2022] AICmr 52.*
[176] *'ABN' and CEO of the Independent Competition and Regulatory Commission ACT (Privacy) [2022] AICmr 48*, e *'ACA' and 'ACB' (Privacy) [2022] AICmr 62*.

perdas não econômicas (*'ABQ' e Serco Group Pty Limited (Privacy) [2022] AICmr 52*). Não houve nenhum caso com concessão de dano agravado.

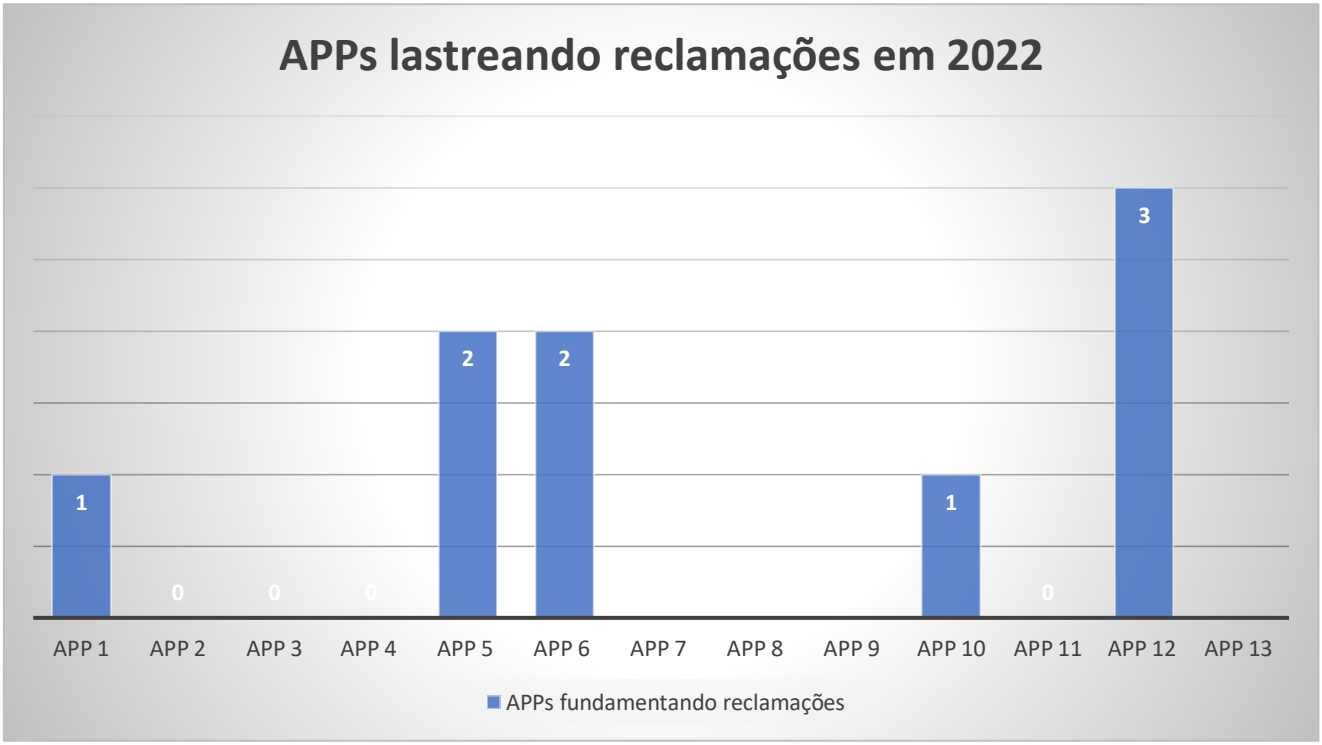

Figura 13- Gráfico APPs lastreando reclamações de privacidade 2022 - Fonte Autora com base nas decisões do OAIC analisadas.

A violação do APP 12 ocorreu em um caso em que o reclamante buscava acesso a informações pessoais contidas em um relatório médico prévio à contratação *('AAQ' e Redimed Pty Ltd (Privacy) [2022] AICmr 7*), em outro caso em que o reclamado se recusou a dar acesso a informações pessoais contidas nas notas de investigação referentes a um incidente envolvendo o objeto de uma reclamação de atendimento ao cliente feita pelo reclamante (*'AAS' e Spring Hill Specialist Day Hospital (The Trustee for QFD Day Theatres Unit Trust) (Privacy) [2022] AICmr 11*), e, por fim, em um caso em que o réu não forneceu acesso a informações pessoais mantidas de forma injustificada, conforme requerido pelo reclamante, e também não justificou as exceções alegadas (*'ABS' e Relationships Australia South Australia (Privacy) [2022] AICmr 54*). O *Privacy Act 1988* (Cth), ao tratar do APP 12, estabelece que, se a *APP entity* se recusar a dar acesso "da maneira solicitada pelo indivíduo, a entidade deve tomar as medidas (se houver) que forem razoáveis nas circunstâncias para dar acesso de uma forma que atenda às necessidades da entidade e do indivíduo" (CTH, 1988). Em *'ABS' and Relationships Australia South Australia (Privacy) [2022] AICmr 54*, a reclamada ofereceu acesso às informações em seu escritório, permitindo que o reclamante fizesse anotações e se recusando a fornecer cópias dos documentos, por exemplo.

A violação do APP 5 ocorreu em dois casos: Um em que o reclamado (Autoridade de Segurança da Aviação Civil) não notificou o reclamante, um piloto que estava solicitando uma licença específica, sobre a coleta de informações pessoais contidas em um relatório médico (*'ABR' e Autoridade de Segurança da Aviação Civil (Privacidade) [2022] AICmr 53*) – os resultados de um exame específico foram acessados diretamente pelo reclamado, sem o consentimento prévio do reclamante – e no caso já mencionado, *'AAQ' e Redimed Pty Ltd (Privacidade) [2122] AICmr 7*, referente ao relatório médico pré-contratação. Nesse último caso, o OAIC considerou que apenas o APP 12 foi violado porque a notificação sobre a coleta de dados ocorreu por meio de formulários, com a coleta do consentimento por escrito comprovado por documentos assinados pelo reclamante durante o processo de seleção.

Por fim, o APP 6 foi violado por um erro no nome do reclamante em uma lista de comunicações por e-mail, mantido mesmo após a reclamante ter solicitado a correção (*'ABG' and Body Corporate Services Pty Ltd (Privacy) [2022] AICmr 26*), e pela divulgação de informações pessoais do reclamante (que era um imigrante que estava sob detenção) relativas a uma compra de roupas feita pelo reclamante a um terceiro (uma pessoa que estava visitando o reclamante e tentando entregar algumas roupas e pertences – veja o caso *'ABQ' e Serco Group Pty Limited (Privacy) [2022] AICmr 52*). Em *[2022] AICmr 52*, a divulgação foi comprovada por mensagens recebidas do terceiro para o reclamante, questionando por que o reclamante pediu roupas, fazendo com que o terceiro gastasse tempo para chegar ao centro de detenção se havia comprado e já estava de posse delas).

O gráfico abaixo apresenta os dados gerais analisados com relação aos APPs que embasaram as reclamações de 2020 a 2022. Uma possível razão para a predominância dos APPs 6, 11 e 12 que embasam as reclamações é que todos esses princípios são, de certa forma, uma tradução da vedação ao uso indevido de informações pessoais. Conforme apontado por Na Moreham (2018), a noção de privacidade na *common law* foi construída com base em casos de uso indevido de informações privadas.

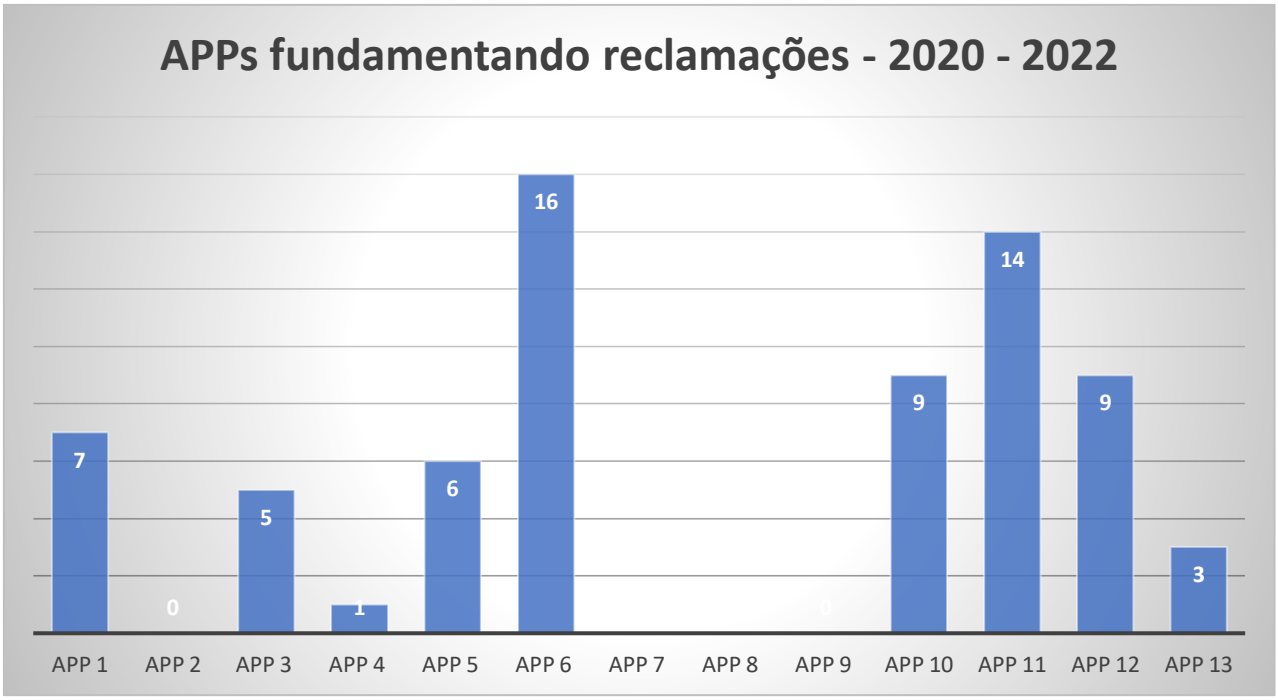

Figura 14 – Gráfico APPs lastreando reclamações 2020 – 2022 - Fonte Autora com base nas decisões do OAIC analisadas.

É possível notar que, em muitos casos, o *Commissioner* adotou a mesma posição ao priorizar a aplicação de determinações não pecuniárias com o objetivo de estabelecer a adoção de medidas para remediar interferências com a privacidade encontradas e corrigir as suas causas, prevenindo futuras violações. São exemplos de medidas não pecuniárias determinadas com frequência: a contratação de especialista ou auditor independente para avaliar processos e procedimentos relativos ao tratamento de dados, com a adoção de medidas indicadas pelo especialista e submissão de relatórios à OAIC sobre cada passo dado, além de manter o monitoramento da governança de dados (revisão de processos e procedimentos, avaliação de riscos, treinamento de pessoal, entre outras medidas). Considerando as indenizações concedidas, o valor mais alto foi de AU$ 19.980 (AU$ 10.000 referentes a perdas não econômicas, e o restante relativo a perdas econômicas) em um caso envolvendo a exposição da reclamante a perigo devido a um erro na execução de um procedimento para desvincular o perfil da reclamante de seu parceiro anterior (que foi acusado de violência doméstica) e atualizar seu endereço (*'WZ' e Chief Executive of Services Australia (Privacy) [2021] AICmr 12*).

Com base na análise das decisões do OAIC em relação à privacidade, é possível perceber que, apesar de o OAIC não ter o poder de executar suas decisões, sua postura na condução de investigações e decisões tende a ser muito mais efetiva do que a atuação da ANPD no mesmo campo (considerando que a ANPD começou a trabalhar na aplicação de penalidades apenas em 2023, após publicar a *Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023,*

estabelecendo como ocorreria a aplicação das punições previstas na LGPD). Não só pelo fato de o OAIC já ter mais maturidade para desempenhar esse papel, considerando sua atuação na área desde 2010, mas também porque as decisões são tomadas com base nas análises e investigações individuais das reclamações recebidas. Além disso, a possibilidade de aplicação de indenização por danos econômicos e não econômicos decorrentes da interferência na privacidade milita em favor do entendimento do titular dos dados sobre a privacidade como um valor relevante, permitindo que o titular dos dados resolva seu problema de forma mais célere e barata.

O foco das decisões do OAIC parece ser reparar as perdas do reclamante e educar os reclamados para evitar novas interferências na privacidade. Como resultado, em muitos casos, o OAIC determina que o reclamado contrate um auditor independente, implemente as medidas indicadas pelo auditor como necessárias para cumprir os APPs e informe o OAIC sobre a situação das medidas adotadas. Há muitos casos em que o OAIC determina que o reclamado emita uma carta reconhecendo a interferência na privacidade e pedindo desculpas ao reclamante (quando essa medida é solicitada e esperada pelo reclamante). Tal postura estimula uma cultura de privacidade e reforça o foco do OAIC nos fundamentos basilares do compliance enquanto um sistema de proteção para a integridade (prevenir, detectar e remediar violações). E o estímulo ocorre não somente pela literal determinação de medidas, mas pelo custo que responder a investigações passa a representar para agentes de tratamento de dados (vale reforçar: esse passa a ser um risco contabilizado), ao passo que existe a certeza de que eventuais violações chegarão ao conhecimento do OAIC e resultarão em investigações. Essa certeza figura como elemento de persuasão para que as *APPs entities* adotem uma postura de cooperação e busquem viabilizar a resolução de questões por autocomposição, diretamente com o reclamante / titular de informações pessoais.

É importante observar que a postura adotada pelo reclamado (agente de tratamento de dados) antes da reclamação e enquanto a reclamação está sendo processada é considerada pelo OAIC para mensurar as determinações e a existência ou não de danos agravados. Quando o respondente age criando barreiras indevidas para a entrega de informações, para dar ao reclamante acesso a suas informações pessoais ou demonstra não respeitar ou não entender a importância das proteções do *Privacy Act 1988* (Cth), o OAIC usa seu poder para emitir uma notificação anunciando a violação do *Privacy Act 1988* (Cth), de acordo com a seção 44. Vale mencionar que, de acordo com a seção 66, diante da inércia do respondente após o recebimento do aviso mencionado, o OAIC pode buscar judicialmente a aplicação de penalidades, incluindo a possibilidade de prisão se o respondente for uma pessoa física.

Todas as decisões são autorreferenciais, ou seja, as decisões são tomadas considerando primeiramente a legislação e, em segundo lugar, os parâmetros adotados anteriormente para tratar de outros casos similares e referindo-se a princípios e parâmetros padronizados nas decisões do OAIC. Além de criar uma forma homogênea de lidar com as reclamações, isso reforça a maturidade do sistema de proteção estabelecido administrativamente. A ausência de menções a interpretações de autoridades estrangeiras e de casos estrangeiros é um ponto forte para reforçar a clareza e a coerência do sistema criado pelo *Privacy Act 1988* (Cth).

No mesmo sentido de demonstrar coesão e coerência, as decisões usam uma estrutura semelhante, o que facilita a consulta de seus tópicos. É uma prática incluir toda a legislação pertinente como anexo, além de informações sobre o direito de recorrer e como proceder para buscar a revisão da decisão. A linguagem adotada é direta, utiliza termos do *Privacy Act 1988* (Cth) e tem efeito e propósito explicativo, permitindo a compreensão da discussão necessária para esclarecer o caso em análise. Em muitas decisões, o *Commissioner* estabelece distinções entre conceitos como "uso", "divulgação", "propósito", "expectativa razoável" e outros, aplicando-os à análise caso a caso, conduzindo o leitor para as premissas adotadas e como elas resultam na conclusão. É útil esclarecer como o OAIC interpreta a lei e reiterar seus propósitos educacionais, contribuindo para a introjeção da privacidade na cultura organizacional e social. Ademais, a comunicação ao reclamante é feita por comunicação escrita sumarizando a decisão em linguagem ainda mais simples, com o inteiro teor da decisão em anexo (fato notado quando da análise das decisões do AAT e da FCA).

Outra descoberta foi que os APPs 2, 7, 8 e 9 não foram objetos de discussão em nenhuma das reclamações decididas de 2020 a 2022. O APP 2 está relacionado a anonimato e pseudoanonimato, exigindo que as entidades ofereçam aos indivíduos a opção de não se identificarem ou de usarem pseudônimos sempre que possível. Aplicam-se exceções limitadas: se a entidade do APP for obrigada ou autorizada por lei a usar a identificação, ou se utilizar os dados em decorrência de ordem de um tribunal, ou se for impraticável para a entidade do APP lidar com indivíduos que não se identificaram ou que usaram um pseudônimo. Parece ser incomum, mais aplicável a alguns serviços, como o de ouvidoria. De fato, essa possibilidade de anonimato é encontrada e aplicada principalmente para realização de reclamações junto à ouvidoria de entidades prestadoras de serviços públicos como de transporte, por exemplo. Entretanto, não é um problema para os indivíduos se, para receber feedback sobre uma reclamação, for necessário fornecer algumas informações de contato, tornando o reclamante fatalmente identificável.

O APP 7 trata de marketing direto e afirma que uma organização só pode usar ou divulgar informações pessoais para fins de marketing direto se determinadas condições forem atendidas (por exemplo, se a organização coletou as informações do indivíduo, se o indivíduo esperaria razoavelmente que a organização usasse ou divulgasse as informações para esse fim; se a organização fornecer um meio simples pelo qual o indivíduo possa facilmente solicitar o não recebimento de comunicações de marketing direto da organização; se o indivíduo não tiver feito tal solicitação para a organização; se o indivíduo tiver sido informado e consentido com o propósito; entre outras). Basicamente, apenas as informações confidenciais não podem ser divulgadas no marketing direto, uma vez que a organização oferece uma opção de exclusão ao alvo. A amplitude das exceções e a facilidade de fornecer uma opção de cancelamento do recebimento tornam o APP 7 fácil de ser alcançado pelas organizações. Provavelmente, esse é o motivo pelo qual ele não é um problema.

O APP 8 trata do compartilhamento internacional de informações pessoais e descreve as medidas que uma *APP Entity* deve tomar para proteger as informações pessoais antes que elas sejam compartilhadas transnacionalmente. Neste ponto, vale a pena lembrar que o *Privacy Act 1988* (Cth) é aplicável a organizações que coletam e mantêm informações pessoais. A interpretação predominante (de acordo com a Parte II, Seção 6 do *Privacy Act 1988* (Cth)) é que "uma entidade coleta informações pessoais somente se a entidade coletar as informações pessoais para inclusão em um registro ou publicação geralmente disponível", e que "uma entidade mantém informações pessoais se a entidade tiver posse ou controle de um registro que contenha as informações pessoais". De acordo com o OAIC[177], "manter" se estende aos registros com os quais a *APP Entity* tem o direito ou o poder de lidar, mesmo que não possua fisicamente, ou seja, que não seja proprietária da mídia na qual as informações pessoais estão armazenadas. Portanto, as organizações que apenas fornecem armazenamento de dados (como serviço de nuvem) não mantêm informações pessoais de acordo com o *Privacy Act 1988* (Cth), pois contratualmente não têm o poder de lidar com os dados, modificá-los ou usá-los. Isso é essencial para entender como a abordagem da *LGPD* é diferente, pois seu foco está nos agentes de tratamento que lidam com dados pessoais de qualquer maneira, que tratam dados pessoais, independentemente de os dados pessoais estarem em um registro físico ou armazenados digitalmente. No sistema de proteção da *LGPD* a avaliação do nível de controle sobre os dados e registros é importante apenas para definir se uma organização lida com dados pessoais como controladora ou como operadora.

[177] Veja, por exemplo, *'AAS' and Spring Hill Specialist Day Hospital (The Trustee for QFD Day Theatres Unit Trust) (Privacy) [2022] AICmr 11*,item 90.

Além disso, o APP 8 apresenta uma grande variedade de possibilidades de exceções, como, por exemplo, "se o destinatário das informações estiver sujeito a uma lei ou esquema vinculativo que tenha o efeito de proteger as informações de uma forma que, em geral, seja pelo menos substancialmente semelhante à forma como os *Australian Privacy Principles* protegem as informações" (CTH, 1988).

O APP 9 trata da adoção, do uso ou da divulgação de identificadores relacionados ao governo e descreve as circunstâncias limitadas em que uma organização pode adotar um identificador oficial de um indivíduo como seu próprio identificador ou usar ou divulgar um identificador relacionado ao governo de um indivíduo. De acordo com as *APP Guidelines*, "o objetivo do APP 9 é restringir o uso geral de identificadores relacionados ao governo por organizações para que eles não se tornem identificadores universais". Um identificador pode ser um número, letra ou símbolo, ou uma combinação de qualquer uma dessas coisas ou de todas elas, usado para identificar o indivíduo ou para verificar a identidade do indivíduo, por exemplo, o registro geral no Brasil (RG), o número de identificação fiscal e outros. O OAIC explica que essa prática "pode comprometer a privacidade ao permitir que informações pessoais de diferentes fontes sejam combinadas e vinculadas de maneiras com as quais um indivíduo pode não concordar ou esperar". Portanto, o APP 9 funciona mais como uma recomendação, porque muitas exceções podem ser aplicadas e alguns identificadores são obrigatórios em alguns campos (por exemplo, para pagar os salários de seus funcionários, uma organização precisa usar seus números de identificação fiscal - ou CPF no Brasil - para permitir que o estado colete contribuições).

No entanto, mesmo soando como uma recomendação, o APP 9 é muito relevante em termos de proteção de dados, tendo em vista o alerta feito por Carissa Véliz (2021) quando a autora menciona como a uniformização no uso de dados pessoais, como o excesso de registros pelo governo, ou o uso unificado de um mesmo identificador pode expor a segurança dos indivíduos. Véliz discorre sobre dois exemplos ocorridos durante o Terceiro Reich, o que aconteceu na Holanda, onde estava em funcionamento um serviço unificado de registro de cidadãos, o que facilitou aos nazistas encontrarem judeus, resultando no maior nível de extermínio em toda a Europa (73% dos judeus da Holanda foram executados). Por outro lado, na França, onde esse sistema de registro não existia, muitos judeus tiveram a chance de escapar da perseguição do regime nazista (VÉLIZ, 2021, p. 156-161)

Também vale a pena enfatizar a relevância do APP 9 se considerarmos o *Projeto Aadhaar*, em execução na Índia e em funcionamento desde 2009 (UNIQUE

IDENTIFICATION AUTHORITY OF INDIA, 2022[178]). O projeto criou a primeira identidade on-line do mundo, combinando todos os dados pessoais relevantes dos cidadãos indianos, incluindo dados biométricos, dados demográficos e mapeamento da íris (SUPREME COURT OF INDIA, *writ petition* (civil) nº. 494 de 2012, 2018, p. 49[179]). O apelo para a formação da base de dados da Aadhaar foi a ideia de controle para evitar a exclusão e promover a inclusão na economia[180]. A coleta massiva de dados pessoais é frequentemente envolvida, especialmente pelo discurso da indústria da vigilância, em uma relação discursiva com a segurança, e foi outro argumento para o Cartão Aadhaar. Inicialmente, o governo pretendia tornar obrigatória a apresentação da identificação on-line, usando-a como condição para o acesso a serviços e benefícios públicos (ela passou a ser exigida até mesmo para a abertura de contas bancárias e para a matrícula de crianças na escola, por exemplo). O projeto foi amplamente criticado e, em 2013, uma decisão da Suprema Corte indiana determinou que não seriam negados benefícios, serviços e subsídios sociais a nenhuma pessoa por não possuir um número Aadhaar. Após uma longa discussão na Suprema Corte sobre questões de privacidade e outros riscos, o cartão Aadhaar foi considerado válido, mas não obrigatório para comprar cartões SIM e acessar serviços públicos[181]. Imagine o risco e a vulnerabilidade desses cidadãos se a Índia fosse alvo de uma guerra (e a vulnerabilidade do governo indiano, já que na sociedade informacional as batalhas pelo poder entre as nações são travadas no espaço cibernético, tendo os bancos de dados soberanos como um alvo importante).

Portanto, embora a noção de privacidade do *Privacy Act 1988* (Cth) esteja desatualizada se considerarmos o contexto da sociedade informacional e se o objetivo legal for a proteção dos direitos da personalidade, a política de regulação implementada pelo OAIC é consistente e madura para o objetivo proposto até o momento. Como mencionado anteriormente, é possível defender que o *Privacy Act 1988* (Cth) é uma lei voltada para a segurança informacional (e não para a proteção individual). Também é uma forma de os indivíduos acessarem informações pessoais, ou explicações sobre qualquer recusa, e solicitarem correções quanto às suas informações. Vale a pena mencionar que o APP 12 é uma das bases mais frequentes para reclamações. De acordo com o APP 12, relacionado ao acesso a informações pessoais, e com as *APP Guidelines*, quando uma solicitação de acesso às informações pessoais é feita com base no APP 12, a *APP Entity* tem várias obrigações atreladas ao acesso, como fornecer acesso a

[178] Disponível em: https://uidai.gov.in/en/. Acesso em 2 Jun. 2023.
[179] Disponível em https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf. Acesso em 21 Jun. 2023.
[180] Veja https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/usage-of-aadhaar.html. Acesso em 21 Jun. 2023.
[181] Veja "*Aadhaar card: an invasion to privacy"*. Disponível em: https://www.legalserviceindia.com/legal/article-34-aadhaar-card-an-invasion-to-privacy.html. Acesso em 21 Jun. 2023.

todas as informações pessoais mantidas na forma solicitada pelo indivíduo, a menos que a modalidade de acesso solicitada não seja razoável ou seja impraticável. Além disso, todas as recusas devem ser justificadas em uma notificação por escrito, vinculando a recusa à exceção apresentada no *Privacy Act 1988* (Cth). Ademais, a recusa deve conter orientação sobre como o reclamante / titular das informações pode solicitar revisão perante o respondente/*APP Entity* e perante o OAIC. O APP 12 figura como uma ferramenta importante na estrutura do *Privacy Act 1988* (Cth), ao envolver os agentes de tratamento / regulados na difusão da cultura de conformidade com relação à privacidade.

A partir das decisões analisadas, é possível perceber que, para apresentar uma reclamação perante o OAIC, o indivíduo precisa estar atento ao fato de que todas as demandas incluídas na reclamação devem ser apresentadas anteriormente[182] ao respondente e aguardar pelo menos 30 dias para obter uma resposta[183]. Algumas decisões rejeitaram as reclamações exatamente pelo fato de a reclamação não ter sido apresentada ao respondente anteriormente. Essa exigência revela um mecanismo para evitar que o OAIC tome medidas adicionais em relação a uma reclamação que poderia ser resolvida entre as partes sem nenhuma disputa. Além disso, vale a pena mencionar que o site do OAIC contém uma grande quantidade de informações para orientar o titular de dados sobre o que é uma questão que poder ser objeto de uma reclamação, como reclamar e, se necessário, como obter um serviço de tradução e interpretação se o titular de dados for estrangeiro, não falante de inglês[184].

Outra questão interessante está relacionada à indenização por perdas e danos. As decisões são orientadas para analisar as reivindicações e o que o reclamante faz para remediar o caso, o que significa que, se o reclamante busca compensação por perdas e danos, ele deve incluir isso na reclamação. O OAIC segue rigorosamente os precedentes administrativos e judiciais como um traço do sistema jurídico de *commoon law*. O *Commissioner* tem o poder discricionário, de acordo com a Seção 5, de fazer várias declarações, inclusive lidar com qualquer perda ou dano sofrido devido à interferência na privacidade e tem o poder discricionário de resolver a situação concedendo compensações por essas perdas e danos. Os danos não econômicos podem incluir mágoa, humilhação e danos à sua saúde mental.

---

[182] Consulte as orientações fornecidas pelo OAIC sobre a necessidade de reclamar primeiro com a organização ou agência que detém as informações pessoais. Disponível em https://www.oaic.gov.au/privacy/privacy-complaints/complain-to-an-organisation-or-agency. Acesso em 21 jun. 2023. Veja também https://www.oaic.gov.au/privacy/privacy-complaints/what-you-can-complain-about. Acessado em 21 Jun. 2023.

[183] https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=APC_PC&tmFormVersion. Acesso em 21 Jun. 2023.

[184] https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us#help-lodging-a-complaint. Acesso em 21 Jun. 2023.

Para conceder indenizações, o OAIC sempre considera as provas produzidas pelo reclamante e como elas apresentam a perda ou o dano devido à interferência na privacidade. Vale a pena enfatizar que o nexo causal entre a conduta ou o ato do respondente e o dano ou prejuízo é crucial para a concessão da indenização. Tendo provas sobre a existência de danos ou perdas resultantes dos atos ou condutas do respondente, o OAIC segue os princípios estabelecidos em *Rummery e Federal Privacy Commissioner [2004] AATA 1221*: quando uma reclamação for fundamentada e houver perda ou dano, a legislação contempla alguma forma de reparação no curso normal; as concessões devem ser restritas, mas não mínimas; ao medir a compensação, os princípios de danos aplicados na lei de responsabilidade civil ajudarão, embora o guia final sejam as palavras da lei; em um caso apropriado, danos agravados podem ser concedidos; e a compensação deve ser avaliada levando-se em conta a reação do reclamante e não a reação percebida da maioria da comunidade ou de uma pessoa razoável em circunstâncias semelhantes. O último princípio demonstra uma preocupação com relação aos direitos da personalidade e uma concepção empática do impacto emocional.

É interessante observar que a interferência na privacidade em si não é uma causa para a concessão de indenização. Em muitos casos, o *Commissioner* decide determinar ações específicas que não implicam em medidas pecuniárias, como mencionado, tais como: enviar um pedido de desculpas por escrito reconhecendo a interferência na privacidade, fornecer um certificado atestando que todas as informações pessoais mantidas foram enviadas ao reclamante, fornecer um certificado atestando que todas as informações pessoais mantidas foram destruídas, entre outras.

5.3.2 Privacidade nas decisões do *Administrative Appeal Tribunal* - AAT

Na busca por decisões relativas ao *Privacy Act 1988* (Cth), foram encontradas apenas 11[185] decisões para todo o período (de 2020 a 2022). A partir das análises, foi inesperado e surpreendentemente notar que o *Privacy Act 1988* (Cth) não está no centro dos pedidos de

[185] Lista de decisões encontradas: *Garret and Other [2020] AATA 1726*; *Knight and Commonwealth Ombudsman (Freedom of information) [2021] AATA 2504*; *Martinovic and Australian Capital Territory (Compensation) [2021] AATA 3435*; *Bradford and Australian Federal Police (Freedom of information) [2021] AATA 3984*; *AUSTRALIAN ELECTORAL COMMISSION AND COMCARE [2022] AATA 138*; *LMKY and Indigenous Business Australia (Freedom of Information) [2022] AATA 428*; *Lim and Secretary, Department of Home Affairs [2022] AATA 1526*; *Lever and Australian Nuclear Science and Technology Organisation [2022] AATA 2259*; *Bradley and National Disability Insurance Agency [2022] AATA 2884*; [2022] AATA 2884; *XCFB and National Disability Insurance Agency [2022] AATA 4121*; e *Sitki and Comcare (Compensation) [2022] AATA 4435*.

revisão, seu uso foi feito apenas para mencionar o conceito de "informações pessoais" (que é aplicado no mesmo sentido nos casos relativos ao *Freedom of Information Act 1982* (Cth), central no debate em muitos casos[186], e sob o *Migration Act 1958* (Cth)[187]), e para justificar que o APP 6 permite o uso de informações pessoais (principalmente em casos que discutem objeções processuais à divulgação adicional de registros médicos relativos a tratamento psicológico, na maioria dos casos[188] relacionados a solicitações nos termos da *Safety, Rehabilitation and Compensation Act 1988* (Cth)), mesmo informações sensíveis, devido a uma obrigação legal ou quando determinado por um Tribunal. Portanto, em todas as decisões analisadas, o *Privacy Act 1988* (Cth) é simplesmente citado ou mencionado para resolver questões laterais no pedido de revisão, o que significa que não foram encontrados casos de revisão referente a decisões tomadas pelo OAIC nos termos do *Privacy Act 1988* (Cth).

O resultado revela um elevado nível de satisfação com a forma como o OAIC lidou com os casos em que a interferência na privacidade é a questão principal. Mesmo sob o argumento razoável de que isso também pode revelar que a privacidade não é um tópico importante que mereça o pedido de revisão, vale lembrar que o pedido de revisão pode ser feito sem custo para o titular dos dados, prevalecendo a suposição de que a efetividade da solução fornecida pelo OAIC pode ser a principal razão para o baixo índice de pedidos de revisão de mérito. De qualquer forma, a maneira como o *Privacy Act 1988* (Cth) é mencionado para auxiliar na fundamentação das decisões analisadas reafirma a importância do APP 6 (relativo ao uso e divulgação de informações pessoais) e sua transversalidade em demandas concretas, especialmente no que tange às exceções ali dispostas.

---

[186] Por exemplo, *Bradford and Australian Federal Police (Freedom of information) [2021] AATA 3984*; *Knight and Commonwealth Ombudsman (Freedom of information) [2021] AATA 2504*; *Lever and Australian Nuclear Science and Technology Organisation [2022] AATA 2259*; *Lim and Secretary, Department of Home Affairs [2022] AATA 1526*; e *LMKY and Indigenous Business Australia (Freedom of Information) [2022] AATA 428.*

[187] Veja, por exemplo, *Lim and Secretary, Department of Home Affairs [2022] AATA 1526*, caso envolvendo uma aplicação para revisão feita com base no *Freedom of Information Act 1982 (Cth)* para acesso a informações sobre as entradas e saídas do país de um terceiro.

[188]Por exemplo, *Martinovic and Australian Capital Territory (Compensation) [2021] AATA 3435*; *AUSTRALIAN ELECTORAL COMMISSION AND COMCARE [2022] AATA 138* e *Sitki and Comcare (Compensation) [2022] AATA 4435*.

5.3.3 Privacidade nas decisões da *Federal Court of Australia* - FCA

A pesquisa usando o indexador "Privacy Act 1988 (Cth)" resultou em 11 decisões tomadas em 2020[189], 4 decisões tomadas em 2021[190] e 15 decisões tomadas em 2022[191] pela FCA. A maioria das decisões pertinentes focadas no *Privacy Act 1988* (Cth), ou seja, que tratavam de questões atinentes à privacidade como centrais, foram tomadas em 2022. Somente em 2022, é possível notar a atuação da FCA para revisar as decisões tomadas pelo OAIC[192]. Em todos os casos em que os requerentes buscavam a revisão de decisões tomadas pelo *Information Commissioner* ou seus delegados nos termos do *Privacy Act 1988* (Cth), a decisão contestada foi tomada nos termos da Seção 41 (1)[193] da Lei, que permite que o *Information*

---

[189] Lista de decisões analisadas de 2020: *Application by Flexigroup Limited (nº. 2) [2020] ACompT; Australian Competition and Consumer Commission v Panthera Finance Pty Ltd [2020] FCA 340; Australian Information Commissioner v Facebook Inc [2020] FCA 531*(well known as "Facebook nº. 1"); *Australian Information Commissioner v Facebook Inc [2020] FCA 1307* (Facebook nº. 2); *Knowles v Secretary, Department of Defence [2020] FCA 1328; Palmer v State of Western Australia (nº. 4) [2020] FCA 1221; Lee v Fair Work Commission [2020] FCA 1204; Siemens Industry Software Inc v Telstra Corporation Limited [2020] FCA 901, Gollant, in the matter of OT Markets Pty LTd (in liquidation) [2020] FCA 207; Pathmanathan v Healthscope Operations Pty Ltd [2020] FCA 65;* e *PIA Mortgage Services Pty Ltd v King [2020] FCAFC 15.*

[190] Lista de decisões analisadas de 2021: *Australian Competition and Consumer Commission v Fuji Xerox Australia Pty Ltd [2021] FCA 153; Knowles v Secretary, Department of Defence [2021] FCAFC 215; Rana v Registrar Cridland [2021] FCA 848;* e *Rothfield v Office of the Australian Information Commissioner [2021] FCA 1524.*

[191] Lista de decisões analisadas de 2022: *Boulos v M.R.V.L. Investments Pty Ltd (nº. 3) [2022] FCA 307; Rana v Australian Information Commissioner [2022] FCA 817; Puopolo v Queensland Electricity Transmition Corporation Limited T/A Powerlink Queensland [2022] FCA 400; Philipsen v Astora Women's Health, LLC [2022] FCA 196; Luck v Secretary of Services Australia [2022]FCAFC 195; Traverse Alpine Operations Pty Ltd v Simpson [2022] FCA 1365; Facebook Inc v Australian Information Commissioner [2022] FCAFC 9; Jaworski v Australian Information Commissioner [2022] FCA 1400; Skiba v Australian Information Commissioner [2022] FCA 1171; Saffari v Australian Information Commissioner [2022] FCA 1016; Ross v Australian Information Commissioner [2022] FCA 243; Ogawa v Australian Information Commissioner [2022] FCA 1374; McEwan v Office of the Australian Information Commissioner [2022] FCA 955; McEwan v Office og the Australian Information Commissioner (nº. 2) [2022] FCA 1452;* e *McEwan v Office of the Australian Information Commissioner (nº. 2) [2022] FCA 1488.*

[192]Veja *Rana v Australian Information Commissioner [2022] FCA 817; Facebook Inc v Australian Information Commissioner [2022] FCAFC 9; Jaworski v Australian Information Commissioner [2022] FCA 1400; Skiba v Australian Information Commissioner [2022] FCA 1171; Saffari v Australian Information Commissioner [2022] FCA 1016; Ross v Australian Information Commissioner [2022] FCA 243; Ogawa v Australian Information Commissioner [2022] FCA 1374.*

[193] 41 Commissioner may or must decide not to investigate etc. in certain circumstances

(1) The Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under section 36 if the Commissioner is satisfied that:

(a) the act or practice is not an interference with the privacy of an individual; or

(c) the complaint was made more than 12 months after the complainant became aware of the act or practice; or

(d) the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith; or

(da) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances; or

(db) the complainant has not responded, within the period specified by the Commissioner, to a request for information in relation to the complaint; or

(dc) the act or practice is being dealt with by a recognised external dispute resolution scheme; or

Commissioner exerça um poder discricionário para não investigar mais um ato ou prática objeto de uma reclamação nos termos da Seção 36 do *Privacy Act 1988* (Cth).

Somente em *Jawoski v Australian Information Commissioner [2022] FCA 1400*, a FCA decidiu anular a decisão do *Commissioner* de não investigar mais a reclamação do requerente, revelando o baixo nível de interpretação errônea do *Privacy Act 1988* (Cth) pelo OAIC, uma vez que a FCA só pode anular as decisões do *Commissioner* com base em sua falha quanto à legalidade ou eventuais abusos. Em *[2022] FCA 1400*, o recorrente (reclamante no caso perante o OAIC) reclamou do uso indevido de suas informações pessoais pela *Chartered Accountants Australia and New Zealand (CA ANZ)* em retaliação à sua requisição de 38 moções para consideração sobre uma série de questões (divulgação nas contas financeiras da *CA ANZ*, estrutura de governança, custos de viagens ao exterior e remuneração de executivos seniores). Na decisão do OAIC, o *Information Commissioner* não considerou as opiniões expostas sobre o requerente pela *CA ANZ* como informações pessoais, considerando apenas seu nome completo como informação pessoal divulgada para todos os membros da *CA ANZ*. No entanto, as opiniões sobre as práticas do requerente deveriam ter sido consideradas como informações pessoais porque, entre os objetivos do *Privacy Act 1988* (Cth), está a promoção da privacidade dos indivíduos reconhecendo que essa proteção deve ser equilibrada com os interesses das entidades no desempenho de suas funções ou atividades. Além disso, a definição de "informações pessoais" inclui informações ou opiniões sobre um indivíduo identificado ou um indivíduo razoavelmente identificável, independentemente de as informações ou opiniões serem verdadeiras ou não (Seção 6 (1) do *Privacy Act 1988* (Cth)).

Dito isso, é crucial enfatizar que o tipo de revisão de decisões administrativas sob a jurisdição da FCA é exclusivo em relação a erros na aplicação da lei (que podem ser verificados por diferentes formatos de acordo com as *Federal Court Rules 2011* (Cth), mencionadas em muitas decisões, e que se referem a aplicações sob a Seção 5 da *Administrative Decision (Judicial Review) Act 1977* (Cth)[194]:

(dd) the act or practice would be more effectively or appropriately dealt with by a recognised external dispute resolution scheme; or

(e) the act or practice is the subject of an application under another Commonwealth law, or a State or Territory law, and the subject-matter of the complaint has been, or is being, dealt with adequately under that law; or

(f) another Commonwealth law, or a State or Territory law, provides a more appropriate remedy for the act or practice that is the subject of the complaint.

[194] (1) Uma pessoa prejudicada por uma decisão à qual esta lei se aplica, tomada após o início desta lei, pode solicitar ao Tribunal Federal ou ao Tribunal Federal de Circuito e Família da Austrália (Divisão 2) uma ordem de revisão em relação à decisão com base em um ou mais dos seguintes fundamentos

(a) que ocorreu uma violação das regras de justiça natural em relação à tomada da decisão;

(b) que não foram observados os procedimentos exigidos por lei com relação à tomada da decisão;

(1) A person who is aggrieved by a decision to which this Act applies that is made after the commencement of this Act may apply to the Federal Court or the Federal Circuit and Family Court of Australia (Division 2) for an order of review in respect of the decision on any one or more of the following grounds:
(a) that a breach of the rules of natural justice occurred in connection with the making of the decision;
(b) that procedures that were required by law to be observed in connection with the making of the decision were not observed;
(c) that the person who purported to make the decision did not have jurisdiction to make the decision;
(d) that the decision was not authorized by the enactment in pursuance of which it was purported to be made;
(e) that the making of the decision was an improper exercise of the power conferred by the enactment in pursuance of which it was purported to be made;
(f) that the decision involved an error of law, whether or not the error appears on the record of the decision;
(g) that the decision was induced or affected by fraud;
(h) that there was no evidence or other material to justify the making of the decision;
(j) that the decision was otherwise contrary to law.
(2) The reference in paragraph (1)(e) to an improper exercise of a power shall be construed as including a reference to:
(a) taking an irrelevant consideration into account in the exercise of a power;
(b) failing to take a relevant consideration into account in the exercise of a power;
(c) an exercise of a power for a purpose other than a purpose for which the power is conferred;
(d) an exercise of a discretionary power in bad faith;
(e) an exercise of a personal discretionary power at the direction or behest of another person;
(f) an exercise of a discretionary power in accordance with a rule or policy without regard to the merits of the particular case;
(g) an exercise of a power that is so unreasonable that no reasonable person could have so exercised the power;
(h) an exercise of a power in such a way that the result of the exercise of the power is uncertain; and
(j) any other exercise of a power in a way that constitutes abuse of the power.

(c) que a pessoa que supostamente tomou a decisão não tinha jurisdição para tomar a decisão;
(d) que a decisão não foi autorizada pela promulgação em conformidade com a qual supostamente foi tomada;
(e) que a tomada da decisão foi um exercício impróprio do poder conferido pela promulgação em cumprimento da qual ela supostamente foi tomada;
(f) que a decisão envolveu um erro de direito, quer o erro apareça ou não no registro da decisão;
(g) que a decisão foi induzida ou afetada por fraude;
(h) que não havia provas ou outros materiais que justificassem a tomada da decisão;
(j) que a decisão foi, de outra forma, contrária à lei.
(2) A referência no parágrafo (1)(e) a um exercício inadequado de um poder deve ser interpretada como incluindo uma referência a:
(a) levar em conta uma consideração irrelevante no exercício de um poder;
(b) deixar de levar em conta uma consideração relevante no exercício de um poder;
(c) exercício de um poder para um fim que não seja aquele para o qual o poder foi conferido;
(d) o exercício de um poder discricionário de má-fé;
(e) o exercício de um poder discricionário pessoal sob a direção ou a mando de outra pessoa;
(f) o exercício de um poder discricionário de acordo com uma regra ou política sem levar em conta os méritos do caso específico;
(g) o exercício de um poder que seja tão irracional que nenhuma pessoa razoável poderia ter exercido o poder;
(h) o exercício de um poder de tal forma que o resultado do exercício do poder seja incerto; e
(j) qualquer outro exercício de um poder que constitua abuso de poder.

Além disso, vale a pena lembrar que a interferência na privacidade é definida na Seção 6A (1) do *Privacy Act 1988* (Cth) como um ato ou prática que viola um APP ou um *código de APP* registrado. Uma violação de um APP ocorre se, e somente se, o ato ou prática for contrário ou inconsistente com esse princípio. Conforme mencionado em *Jaworski v Australian Information Commissioner [2022] FCA 1400 [48]*, " *It is apparent from the phrase "if, and only if" that s 6A (1) is intended to set out exhaustively the circumstances in which an act or practice may breach an APP*."[195] Portanto, os princípios aplicados à FCA na revisão do exercício da discricionariedade administrativa no contexto do *Privacy Act 1988* (Cth) são que toda discricionariedade legal ou poder discricionário é limitado pelo objeto, escopo e finalidade da legislação sob a qual é conferido, e toda discricionariedade legal deve ser exercida de acordo com "as regras da razão", o que exige racionalidade plausível demonstrada nas razões da decisão.

Conforme argumentado em *Jaworski v Australian Information Commissioner [2022] FCA 1400*, o exercício da discricionariedade administrativa pelo *Information Commissioner* para não investigar mais uma reclamação está condicionado ao estado de satisfação do *Information Commissioner* de que, de acordo com as regras da razão e com base nas provas apresentadas a ele, o ato ou prática reclamada não é uma interferência na privacidade do indivíduo. Portanto, o tribunal não tem o poder de substituir a decisão por sua própria opinião sobre como o tomador de decisões deve exercer seu poder discricionário. É o contrário, e o tribunal está limitado na revisão judicial a considerar apenas a legalidade da decisão. Em outras palavras, ele está limitado a verificar se o poder discricionário foi exercido de acordo com a lei. Portanto, o estado de satisfação é demonstrado objetivamente se tiver sido formado de forma lógica e racional com base em descobertas de fatos. " *Further, even if it cannot be detected that an error has occurred in the application of law or consideration of the relevant matters, if the conclusion is one which is wholly unreasonable, it can, nevertheless, be inferred that error has occurred.*"[196] (*Rana v Australian Information Commissioner [2022] FCA 817, em [58])*.

É surpreendente que não tenha sido encontrado nenhum pedido de revisão feito pelos requeridos questionando determinações envolvendo a concessão de indenizações por perdas econômicas e não econômicas. Houve um caso único em que o requerente questionou as

[195] "A frase "se, e somente se" deixa claro que a s 6A (1) pretende definir exaustivamente as circunstâncias em que um ato ou prática pode violar um APP."

[196] "Além disso, mesmo que não seja possível detectar a ocorrência de um erro na aplicação da lei ou na consideração das questões relevantes, se a conclusão for totalmente irracional, pode-se, ainda assim, inferir que houve erro."

determinações feitas pelo OAIC tentando elevar a indenização concedida, o *Saffari v Australian Information Commissioner [2022] FCA 1016*, que foi um pedido de revisão vinculado a *'XU' e Amazon Australia Services Inc (Privacy) [2021] AICmr 42.*

O único investigado que litigou contra o OAIC foi o Facebook Inc (investigado por violar o APP 6 e o APP 11, ao operar o aplicativo *This is your Digital Life e o Graph API*), tentando evitar a jurisdição australiana (*Facebook Inc v Australian Information Commissioner [2022] FCAFC 9*, recurso da decisão proferida em *Australian Information Commissioner v Facebook Inc (nº.2) [2020] FCA 1307*, na qual a Corte considerou que o *Information Commissioner* conseguiu demonstrar um caso *prima facie*). Embora o *Information Commissioner* tenha apresentado provas de que o *Facebook Inc* tem um link australiano e realiza negócios na Austrália, de modo que deve se submeter às regras do *Privacy Act 1988* (Cth) ao lidar com informações pessoais coletadas ou mantidas na Austrália, o *Facebook Inc* argumentou que não tem nenhum funcionário ou local fixo de negócios na Austrália e que, em seus Termos de Uso, deixa claro que todos os usuários localizados em países que não sejam os Estados Unidos e o Canadá têm um relacionamento com o *Facebook Ireland*. Com base no Acordo Comercial entre o *Facebook Inc* e o *Facebook Ireland*, o *Information Commissioner* demonstrou que o Facebook Inc é o único responsável pela instalação e remoção de *cookies* e *pixels* nos dispositivos de todos os usuários do *Facebook* e responsável por fornecer acesso à plataforma por meio de login[197]. Além disso, no Contrato, não havia nenhuma disposição sobre

[197] Vale colacionar as razões a decisão em *Facebook Inc v Australian Information Commissioner [2022] FCAFC 9: "*3. We are not dealing with scientific analysis here. But we are dealing with a business that is not manifested in physical or material matter or structures or goods, but as described by Perram J at [29]–[33] of his reasons, which can be described as the collection, storage, analysis, organisation, distribution, deployment and monetisation of information about people and their lives. How that monetisation takes place in relation to the activities carried on by Facebook Inc is neither clear nor the subject of this proceeding. One can be sure, however, that the acts done to collect, store, analyse, organise, distribute and deploy the information about people and their lives are integral to the methods of monetisation or extracting commercial value from the information. The business is not about the simple sale of goods whether tangible or intangible. It is about extracting value from information about people. [...]5. […] Micro-surgery is not undertaken by the physical, manual manipulation of a scalpel by the hand of a surgeon upon the body of a patient. The surgeon may be at an instrument, physically separated from the patient, controlling the minute device that effects the surgery. The act is taking place at both places: where the surgeon is and where the patient is. It can be characterised or conceived of as one act. There is no reason of logic or conceptual appreciation as to why the conclusion must be different depending upon the distance of separation between the two locations. The consideration of the matter and the proper characterisation of the act or activity is to be approached by reference to the nature of the business and the place of the act or activity within the business, and the context as to why the question is being asked, being here the operation of a statute concerned with the privacy of information concerning people.
6. […]Digital activity is not to be reduced to pressing a button, sending a signal, and recognising a discrete effect. This miscomprehends and mischaracterises, in the context of the business, what is going on. **In the context of a digital business such as Facebook Inc's described earlier, the relevant act done in Australia is the installation and operation of cookies on Australian users' devices and the making of the Facebook login available to an Australian developer in Australia.** This is so whether one abstracts or conceptualises these as bilateral or continuing acts or activities, or as acts or activities not attaining significance or not crystallising until installation

como o *Facebook Inc* é remunerado pelos serviços que deveriam ser oferecidos ao *Facebook Ireland.*

Os argumentos contrapostos pelo *Facebook Inc* tornam ainda mais claro o que Shoshana Zuboff (2019) menciona como suas estratégias para manter o ciclo de despossessão depois de ser pego em práticas erradas de uso indevido de dados pessoais como um ativo. O *Facebook* tenta tirar proveito da suposta falta de regulação para escapar e não responder às jurisdições com leis de privacidade e estruturas para fazer cumprir a lei que promove a privacidade.

5.4 Privacidade e cultura de compliance com o *Privacy Act 1988* (Cth) na Austrália

A análise das decisões administrativas e judiciais referentes ao *Privacy Act 1988* (Cth) foi feita para demonstrar como a lei de privacidade é aplicada e, com isso, como a estrutura criada pela lei protege a privacidade na Austrália. A análise possibilitou a identificação dos principais problemas que os australianos enfrentam como interferência na privacidade, qual é o perfil das organizações que estão desempenhando o papel de respondentes nas reclamações e qual é o comportamento das partes interessadas (indivíduos/reclamantes e organizações/entidades APP/respondentes) em relação à forma como o OAIC realiza as investigações e seu papel de monitorar a conformidade com o *Privacy Act 1988* (Cth).

Além disso, foi relevante ver o nível de engajamento dos indivíduos e como a privacidade é aprimorada como resultado do papel do OAIC de orientar e promover a conformidade e a eficácia da privacidade, orientando em todos os relatórios de decisão (feitos por meio de cartas) sobre como solicitar a revisão e usando uma linguagem simples e direta (as cartas são escritas diretamente para as partes, usando um discurso direto e uma descrição simples dos fatos e razões para a decisão, e mencionando no final todos os artigos relevantes da lei usados no racional, medidas que contribuem para a conscientização sobre a lei e sobre os recursos a serem procurados para solução de questões relacionadas à interferência na privacidade). A forma como o OAIC lida com as comunicações com titulares de dados e processadores de dados estimula a composição de conflitos e contribui para a difusão de informações sobre as práticas esperadas quando se está lidando com informações pessoais.

A principal motivação para fazer um estudo comparado entre o cenário brasileiro e australiano de privacidade e proteção de dados foi a intenção, conforme mencionado na

---

and operation on the device or the making of the login available to the user. The installation and operation and the making of the login available are not effects or consequences, but essential elements of the acts or activities themselves." *(Grifos nossos).*

introdução e reiterado nos capítulos, de comparar diferentes sistemas jurídicos desenvolvidos em nações que sofreram um processo de colonização e têm culturas muito diversas e povos miscigenados. Com muitas diferenças e semelhanças, outra razão para o interesse em pesquisar a estrutura de privacidade na Austrália foi o fato de o país ter uma das leis de privacidade mais antigas do mundo e, mesmo sofrendo a influência e a pressão de organizações internacionais, em vez de revogar essa lei em vigor desde 1988 e propor outra, mais adequada aos "melhores padrões globais", a Austrália apostou na revisão de sua lei, aprimorando o que já tem em termos de regras e estrutura para promover a privacidade. Além disso, superar esse propósito inicial seria produtivo para estabelecer, a partir da comparação, as características que representam pontos fortes, pontos fracos, ameaças e oportunidades para a melhoria contínua da estrutura de privacidade e proteção de dados para, de fato, proteger de forma mais efetiva os direitos da personalidade.

Entretanto, mesmo partindo dessas intenções e suposições, os resultados foram surpreendentes. Em primeiro lugar, já que se verificou que no sistema jurídico australiano, não existe o direito à privacidade nem o direito à proteção de dados. A concepção de privacidade na Austrália está desatualizada se considerados os padrões estabelecidos pela União Europeia, tomados como modelo pelos estados-nação em todo o mundo. O *Privacy Act 1988* (Cth) estabelece o direito de fazer uma reclamação perante o OAIC se um indivíduo sentir e tiver provas de que uma organização ou entidade APP interferiu em sua privacidade. É basicamente uma lei que lida com a segurança informacional e não é uma lei com o objetivo de promover a proteção de dados, a autodeterminação informativa e os direitos de personalidade (e não quer ou argumenta ser). Ela tem claramente o objetivo de promover a proteção da privacidade dos indivíduos, reconhecendo, ao mesmo tempo, que a proteção da privacidade das pessoas naturais deve ser equilibrada com os interesses das entidades no desempenho de suas funções e atividades.

Em segundo lugar, embora a percepção da privacidade possa parecer desatualizada e falha, o engajamento geral e a estrutura para aplicação da lei funcionam de forma muito mais efetiva do que na estrutura brasileira, para lidar com os incômodos experimentados pelos indivíduos e para construir um senso de conscientização sobre a regra e os valores que ela busca promover. Efetivamente, em termos de tratamento das reclamações, na forma como as organizações encaram a privacidade e a necessidade de tomar medidas razoáveis para lidar com informações pessoais de forma responsável e transparente, além de adotar uma postura proativa quando ocorre uma violação para aplicar os três fundamentos dos sistemas de compliance e governança: prevenir, detectar e remediar.

A efetividade verificada não é derivada de herança da *common law*. Ela é, de fato, resultado de uma série de reformas administrativas que ocorreram na Austrália nas últimas décadas. O objetivo das reformas, que incluíam a adoção de novas estratégias, era melhorar a aplicação da lei e das políticas; no entanto, o resultado obtido foi muito além do objetivo inicial, tornando a estrutura regulatória minimamente resistente para lidar com a realidade dinâmica da sociedade informacional. Entre as estratégias, vale a pena mencionar a metodologia ALRC, que permite que as recomendações sejam dadas para refletir as demandas captadas das contribuições recebidas em consultas, já abordadas no início deste capítulo. Além disso, a ação dos departamentos governamentais desempenha um papel significativo na "criação e modificação de regulamentos em resposta às mudanças tecnológicas em curso em sua esfera" (MOSES, 2011, p. 780)[198].

Ademais, o governo da *Commonwealth* tem uma comissão consultiva independente, a *Productivity Commission*, dedicada a, com base na perspectiva de toda a comunidade, promover a excelência das políticas públicas, melhorando a produtividade e o desempenho econômico, reduzindo regulações desnecessárias, incentivando o desenvolvimento de indústrias australianas eficientes e competitivas internacionalmente, facilitando o ajuste às mudanças estruturais, reconhecendo os interesses da comunidade em geral e de todos aqueles que possam ser afetados por suas propostas, promovendo o emprego e o desenvolvimento regional, levando em conta os compromissos internacionais da Austrália e as políticas comerciais de outros países e garantindo que a indústria australiana se desenvolva de forma ecologicamente sustentável, de acordo com o *Productivity Commission Act 1998* (Cth)[199]. As principais funções da *Productivity Commission* são a realização de investigatórios públicos e estudos de pesquisa solicitados pelo governo, a realização de pesquisas de iniciativa própria e relatórios anuais sobre produtividade, assistência e regulação, monitoramento de desempenho e benchmarking e outros serviços para órgãos do governo, além de tratar de reclamações sobre neutralidade competitiva (por meio do *Australian Government Competitive Neutrality Complaints Office*)[200].

---

[198] Sobre o assunto, Lyria Bennett Moses enfatiza que: "[...] Despite having a narrower jurisdiction, government departments have a significant role to play in creating and modifying regulations in response to ongoing technological change withing their sphere. Where a government department has jurisdiction over a particular set of laws or a particular type of technology, it will amendo r recomend changes to relevant regulations or status as appropriate. [...] Where a particular technology cuts across multiple government departments or agencies, then committees, task forces or working groups may be formed to coordinate reforms. Where a law is within the domain o fone or more government departments, they are generally faster and more responsive to needed change compared with more general institutions suvh as law reform commissions. [...]" (MOSES, 2011, p. 780).

[199] Seção 8 – *Productivity Commission Act 1998 (Cth).*

[200] Para mais detalhes consulte o website: https://www.pc.gov.au/. Acesso em 10 Jun. 2023.

Diferentemente do ALRC, que se reporta ao *Attorney-General* (Procurador-Geral), a *Productivity Commission* e se reporta ao *Treasurer*.

O *Office of Impact Analysis* - OIA (Escritório de Análise de Impacto)[201], o novo nome do antigo *Office of Best Practice Regulation* – OBPR (Escritório de Regulamentação de Melhores Práticas) desde 18 de novembro de 2022, tem uma função importante antes da implementação de uma nova política, pois "a análise de impacto ajuda os formuladores de políticas a considerarem como as propostas afetam empresas, indivíduos e organizações comunitárias, bem como impactos econômicos mais amplos e outros impactos". O objetivo do OIA é desenvolver uma análise de impacto sólida e baseada em evidências para apoiar os tomadores de decisão e garantir que "as opções de políticas sejam bem projetadas, bem direcionadas e adequadas à finalidade" (OIA, 2023, *tradução nossa*). O OIA também atua para monitorar o impacto e a eficácia das políticas em vigor, para garantir que a regulação tenha resultados eficientes e atinja seus objetivos com o menor impacto possível[202]. As revisões são necessárias a cada cinco anos "para garantir que o estoque regulatório permaneça adequado ao propósito ao longo do tempo e, em particular, que as mudanças sejam feitas para levar em conta as novas circunstâncias tecnológicas". (MOSES, 2011, p. 780, *tradução nossa*). Com esses esforços, a Austrália está alinhada com uma tendência internacional em direção a uma gestão "melhor" ou "mais inteligente" da regulação, voltada para o melhoramento contínuo e entendida como algo em constante evolução.

Por fim, acadêmicos argumentam que muitas estruturas regulatórias estabelecidas na Austrália se baseiam em insights da regulação responsiva (como a *Australian Competition and Consumer Commission* e o *Australian Tax Office*), que foi reconhecida pela OCDE como um princípio de "melhores práticas" para a política regulatória (OCDE, 2018) e *Behavioural Public Policy* (Política Pública Comportamental) (por exemplo, Australian Tax Office) (BARAK-CORREN, KARIV-TEITELBAUM, 2021, p. 165-168).

Toda a estrutura e as estratégias mencionadas conduzem ao fortalecimento da cultura social e organizacional em relação à privacidade e aos compromissos de privacidade propostos pelo *Privacy Act 1988* (Cth), reforçados pelo acesso fácil e padronizado[203] às informações. Por exemplo, a pesquisa sobre a busca de decisões no Brasil enfrentou um obstáculo em relação à

---

[201] Veja https://oia.pmc.gov.au/.

[202] Consulte a orientação para a revisão pós-implementação, disponível em: https://oia.pmc.gov.au/sites/default/files/2021-09/post-implementation-reviews.pdf. Acesso em 13 Abr. 2023.

[203] Por " padronizado" quero dizer que os sites dos órgãos e departamentos governamentais têm a mesma estrutura, o que facilita a navegação e a experiência do usuário. Além disso, com relação às decisões, todas as decisões administrativas e judiciais também estão disponíveis no mesmo formato e no mesmo site: https://www.austlii.edu.au/. Essa medida torna a pesquisa e o acesso mais fáceis e mais interpretáveis.

variedade de formas que os tribunais brasileiros usam para se referir à LGPD. Como resultado, foi necessário aplicar três indexadores diferentes ("LGPD", "Lei Geral de Proteção de Dados" e "Lei nº. 13.709/2018"). É algo simples que impacta a forma como os titulares de dados vivenciam a relevância da lei e seu sentimento de engajamento (ou não) com os valores fomentados pela política pública. Por cultura de compliance, entende-se o compartilhamento de valores, ideais e comportamentos aprendidos (GUENTER, 2004, p. 20), que se traduzem em uma relação mais próxima entre cidadãos e governo, e entre reguladores e regulados, criando uma atmosfera de comprometimento com a lei e com as políticas por ela subsidiadas.

O próximo capítulo é dedicado a analisar o papel desempenhado pelo *enforcement* para aumentar a efetividade das políticas públicas de privacidade e proteção de dados na sociedade informacional, na qual a urgência de convergência regulatória resulta na disseminação de um modelo de regulação da privacidade e da proteção de dados desenvolvido em arenas transnacionais.

6 ESTRATÉGIAS DE *ENFORCEMENT* E O MELHORAMENTO CONTÍNUO DA POLÍTICA NACIONAL DE PROTEÇÃO DE DADOS BRASILEIRA

Este capítulo argumenta que as estratégias de *enforcement* utilizadas na estrutura australiana podem ser úteis para inspirar o aprimoramento da política pública de proteção de dados brasileira. Começando pela possibilidade de fazer uma reclamação administrativa e tê-la apreciada individualmente, obtendo administrativamente compensação por perdas econômicas e não econômicas, até a existência de agências governamentais focadas em medir políticas para fazer ajustes apropriados para lidar com a dinâmica da vida na sociedade informacional. O capítulo está estruturado em quatro seções. A primeira seção analisa as estratégias de *enforcement* e destaca como e quais são aplicadas no contexto de privacidade e proteção de dados brasileiro e no australiano. A segunda seção trata dos efeitos que as estratégias de *enforcement* causam para a cultura de privacidade e proteção de dados. A terceira seção destaca características da estrutura de privacidade australiana que poderiam ser benéficas para aprimorar a política pública de proteção de dados brasileira. E a quarta seção aponta as lacunas encontradas em ambas as políticas de privacidade analisadas, do ponto de vista da proteção do titular dos dados, e da tutela do corpo digital.

O capítulo levanta reflexões sobre como as estratégias de *enforcement* influenciam a modulação das culturas organizacional, institucional e social, orientando-as para a contemplação de valores apresentados como subsídios para a regulação de determinada matéria. Isso porque, na sociedade informacional há a tendência à convergência regulatória diante de questões emergentes da dicotomia digital versus material na vida humana. Essa busca pela convergência como forma de lidar com um problema transnacional resulta na realização de "inovações" legislativas pelos Estados nacionais por emulação, adotando um modelo gerado internacionalmente e elevado ao nível de padrão, de “melhores práticas”. Como resultado, o conteúdo das normas que sustentam as políticas públicas no campo da privacidade e da proteção de dados torna-se bastante semelhante. Nesse contexto, as estratégias adotadas pelas nações para aplicar e reforçar a inteligência da norma, *enforcement*, tornam-se o diferencial para sua efetividade e para a introjeção dos valores que a norteiam a cultura regional.

No âmbito da regulação do tratamento de dados pessoais, a efetividade da proteção do corpo digital, formado pelas informações extraídas da interação dos indivíduos com as plataformas digitais, exige proatividade e responsividade dos agentes de tratamento de dados pessoais e dos titulares dos dados. No caso dos agentes de tratamento de dados, torna-se crucial a estruturação de um sistema de proteção que conduza à cooperação e à divisão de

responsabilidades entre as entidades estatais e não estatais envolvidas em cadeias de tratamento de dados. E, sob a perspectiva do titular dos dados, é fundamental que a política pública decorrente da regulação adote estratégias que resultem em verdadeiro empoderamento, na existência de mecanismos para buscar a concretização do direito à proteção de dados, e da resolução de seu problema individual, como sinal de que ele é relevante e que a proteção de dados é um valor a ser priorizado.

Por fim, o capítulo aborda alguns pontos omissos na regulação da proteção de dados no Brasil e na Austrália, como a não consideração da regulação do tratamento de dados pessoais de grupos e de dados agregados e a reflexão sobre alternativas para romper o círculo vicioso da divisão do aprendizado e do conhecimento, por meio da democratização da informação, incluindo tópicos sobre alfabetização para viver em uma sociedade informacional e o estímulo à criação de pensadores curiosos e críticos. Uma boa maneira de promover a conscientização é começar a abordar a tecnologia e todos os recursos digitais emergentes como ferramentas, evitando demonizá-la ou endeusá-la. No mesmo sentido, é imperioso encarar o uso da tecnologia sem fatalismos e generalizações acríticas, sem imposição como um "progresso" necessário na administração pública e na vida cotidiana.

6.1 Estratégias de *enforcement*

Esta seção explora diferentes tipos de *enforcement*, para demonstrar quão variada pode ser a maneira de aplicar uma norma e reforçar seus valores e objetivos, moldando o comportamento do regulado. Cumpre esclarecer que a tese utiliza a expressão em inglês (*enforcement*) ao passo que ela oferece um significado mais amplo do que sua tradução literal para o português (aplicação, execução, cumprimento). A revisão dos diferentes tipos de *enforcement* visa elucidar quais são os adotados no Brasil e na Austrália, em relação à proteção de dados, e como eles impactam para sinalizar a privacidade e a proteção de dados como prioridade, contribuindo para a introjeção na cultura. Essa abordagem é importante porque expõe que a convergência regulatória em curso não é suficiente para promover a eficácia se não for baseada em estratégias de cooperação e *enforcement* transnacionais. Como a cooperação regulatória é necessária, destaca-se que a proposta de regulação responsiva, conforme atualizada por John Braithwaite (2006), e abordada no Capítulo 3, trata exatamente desse propósito. Depois de apresentada a categorização criada por Peter Grabosky e John Braithwaite (1988), aplicada aos contextos australiano e brasileiro, foram feitas observações adicionais sobre outros tipos de *enforcement* adotados pelo OAIC e pela ANPD.

Grabosky e Braithwaite (1988, p. 183-194) descrevem dez tipos diferentes de *enforcement*: autorregulação ou corregulação, abordagem de incentivos econômicos, incentivo a litígios civis, divulgação, autorização de pré-comercialização, licenciamento, processo, injunções e diretivas, apreensões e publicidade adversa. Como é possível notar pela descrição, quando se trata de *enforcement*, não se está falando exclusivamente de penalidades ou punições. O *enforcement* está mais relacionado a como os direitos e valores inseridos na norma são aplicados e reforçados, e como as instituições e as pessoas envolvidas na política pública instituída trabalham para promover o comportamento desejado no campo regulado.

A autorregulação (*self-regulation*) ou corregulação (*co-regulation*) é a ausência de punições ou sanções para disciplinar um campo observado. Assim, o regulador apenas incentiva os regulados e as pessoas no campo a se regularem, a criarem normas internas, processos e procedimentos que impulsionem os valores contidos na regulação. Por outro lado, a abordagem de incentivos econômicos consiste na imposição de tributos sobre a concretização de danos que a regulação pretende mitigar. Entretanto, de acordo com Grabosky e Braithwaite (1988, p. 184), esse tipo de *enforcement* é muito caro, pois exige um enorme monitoramento e fiscalização constante, o que resulta na necessidade de muitos recursos para a viabilização das atividades de inspeção. Na prática, a opção de incentivos econômicos é aplicada de forma diferente, não se baseando na mensuração do dano para a imposição de tributos, mas levando em conta a demonstração de esforço para cumprir as normas como elementos para mitigar eventuais penalidades aplicadas. Em outras palavras, o incentivo econômico é comumente aplicado para dar "descontos", para aplicar penalidades mais brandas aos regulados que demonstrarem esforço, que cooperarem para atingir as metas da regulação. Essa é a forma como essa opção de *enforcement* é adotada no Brasil e na Austrália com relação à proteção de dados.

Outra forma de *enforcement* é incentivar o litígio civil (*civil litigation*). A ação de Cortes judiciais reafirmando direitos e aplicando penalidades por violações é uma maneira importante de reafirmar a lei e buscar o comportamento desejado. Grabosky e Braithwaite (1988, p. 185) enfatizam que alguns estudiosos, como Posner, acreditam que essa é uma das opções mais eficazes de *enforcement* da regulação. Essa estratégia não tem apoio na Austrália com relação à proteção criada pelo *Privacy Act 1988* (Cth), e é a principal ferramenta de *enforcement* na estrutura da LGPD. Para funcionar, essa opção exige uma causa para ação, o estabelecimento de um direito por lei. É, de fato, uma estratégia válida, porém, se isolada, se não houver outras opções para pleitear a concretização do direito, a dependência do litígio pode ter um efeito reverso em termos de modulação da cultura. Isso porque, repercute a ideia de que o direito ou o valor focado na lei não é importante o suficiente para criar um sistema de proteção na esfera

administrativa. Além disso, gera outros problemas em termos de celeridade para concretizar o direito e o custo para o sujeito de direito, fazendo com que a concretização do direito seja menos democrática e abrangente.

A estratégia denominada por Grabosky e Braithwaite como divulgação ou *disclosure* (1988, p. 186) consiste na imposição de transparência (por exemplo, rotulagem de ingredientes, data de consumo seguro para alimentos, provisões para rotulagem de cuidados com roupas na indústria têxtil, entre outros), para conscientizar as pessoas sobre a forma como o regulado trabalha e os eventuais riscos de lidar com ele. Assim, os sujeitos podem optar por interagir ou não com o regulado. Isso é muito comum em áreas relacionadas a alimentos e cuidados médicos. Essa estratégia foi encontrada em ambos os sistemas de proteção, *LGPD* e *Privacy Act 1988* (Cth). Na LGPD, o princípio da transparência (art. 6º, VI) é mencionado expressamente como um guia para o tratamento legítimo de dados, e é inferido do art. 18, que traz os direitos dos titulares de dados., do art. 19, e dos arts. 50 e 51, que tratam das boas práticas de governança para a proteção de dados. O *Privacy Act 1988* (Cth) trata diretamente da transparência por meio do APP 1, e indiretamente por meio de todos os outros APPs.

A liberação prévia de comercialização – *pre-marketing clearance* (GRABOSKY, BRAITHWAITE (1988, p. 186) – consiste em uma imposição de aprovação prévia de um produto ou serviço a ser oferecido no mercado. É muito comum na regulação de segurança de medicamentos e transportes, também encontrada no setor de produtos elétricos e farmacêuticos. O seu objetivo é evitar danos, em vez de corrigi-los. Embora as regulações de privacidade e proteção de dados no Brasil e na Austrália apelem para a prevenção, essa não é uma estratégia aplicada em sua estrutura.

O licenciamento (*licensing*) é a aprovação prévia da pessoa ou organização que será responsável pela atividade regulada. Por exemplo, em vez de exigir a aprovação prévia do governo para cada tipo de apólice de seguro que pode ser subscrita por uma seguradora, o governo simplesmente emite licenças apenas para as empresas com reservas, controles prudenciais e competência gerencial que podem ser confiadas para elaborar suas próprias apólices para o público; em vez de exigir a aprovação do governo para cada operação de detonação em uma mina antes que ela possa ser realizada, a exigência é que a detonação só possa ser realizada sob a supervisão de uma pessoa com um certificado de competência como detonador. Grabosky e Braithwaite (1988, p. 187) mencionam que o uso mais comum do licenciamento ante a uma violação da norma é lidar com a suspensão (em vez do cancelamento), porque é uma punição menos severa e permite que o regulado mitigue o dano e corrija os erros. O licenciamento não é aplicado nos contextos brasileiro e australiano de privacidade e proteção

de dados, tampouco o fechamento compulsório de um agente de tratamento (que seria o análogo ao cancelamento de licenciamento). No Brasil, é possível suspender o acesso a um banco de dados em caso de violação da LGPD, mas não é possível a suspensão do agente de tratamento.

O processo judicial (*prosecution*) é a ferramenta regulatória mais conhecida e a mais utilizada de todas as ações regulatórias formais (GRABOSKY, BRAITHWAITE, 1988, p. 189), que consiste em um litígio judicial contra o regulado. Outra estratégia muito comum é por meio de injunções e diretivas (GRABOSKY, BRAITHWAITE, 1988, p. 189), realizadas por meio da orientação e do estabelecimento de padrões mínimos para determinadas atividades, ordenando também medidas de precaução. Ambas as regulações examinadas usam *prosecution* e a emissão de injunções e diretrizes como formas de *enforcement*.

A publicidade adversa (*adverse publicity*) é utilizada tanto na estrutura australiana quanto na brasileira, de maneiras diferentes. Enquanto a LGPD trata da publicidade adversa como uma espécie de punição (art. 52, IV), o *Privacy Act 1988* (Cth) utiliza essa estratégia de forma indireta, pois todas as decisões proferidas em processos administrativos contra regulados que não sejam pessoas físicas mencionam o nome do reclamado e ficam disponíveis para consulta *on-line*. Quando o regulado reclamado é pessoa física, somente as suas iniciais constam nas decisões publicizadas. Além disso, em casos de grandes violações de dados, o OAIC trabalha para informar e orientar os titulares de dados, criando conteúdo que menciona a entidade em que o *data breach* ocorreu. Com a notícia da primeira punição aplicada pela ANPD em virtude de processo administrativo disciplinar, em 05 de julho de 2023 (abordada com mais vagar no Capítulo 4), há que se observar que essa publicidade adversa acontece também de forma indireta, mesmo quando não contemplada nas sanções aplicadas. Os dados da empresa punida, (no caso mencionado, a *Telekall Inforservice)*, ficam acessíveis com a publicidade dada as decisões no Diário Oficial da União. A notícia da primeira punição administrativa aplicada pela ANPD repercutiu na mídia, ampliando o potencial de perda de capital reputacional pela penalizada.

Por fim, os autores mencionam *seizure*, estratégia que se concretiza com a apreensão de mercadorias, é um tipo de *enforcement* amplamente utilizado nas regulação das indústrias de alimentos e de pesca. Entretanto, o *recall* voluntário de alimentos contaminados ou com rótulos incorretos é muito mais utilizado do que a apreensão. Esse tipo de *enforcement* não é aplicado na regulação de privacidade e da proteção de dados nos sistemas analisados.

Além disso, outra ferramenta de *enforcement* é a adoção de compromissos executáveis (GUNASEKARA, 2021, p. 34), para promover a cooperação proativa para remediar danos e riscos. Isso é adotado pelo OAIC e provavelmente também será percebido pela atuação

fiscalizatória da ANPD, com base nas regras para aplicação de sanções administrativas (*Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023 - Regulamento de Dosimetria e Aplicação de Sanções Administrativas*). Todos os compromissos executórios e injunções diretas são feitos pelo OAIC e previstos para realização pela ANPD após a finalização de investigações e processos administrativos contra processadores de dados submetidos ao *Privacy Act 1988* (Cth) e à LGPD, respectivamente. Todas as medidas de *enforcement que* implicam em punição direta ou indireta somente têm lugar após a finalização de processos administrativos.

No campo da regulação da privacidade, promover o controle pelo titular dos dados é essencial, então ter diferentes maneiras de buscar a concretização correta da proteção é extremamente relevante. Conforme mencionado por Ann Cavoukian (2017, p. 330), "privacidade é igual a controle: controle pessoal sobre os usos de seus dados pessoalmente identificáveis". Portanto, as estratégias de *enforcement* desempenham um papel crucial na educação e persuasão dos alvos da política pública (regulados e sujeitos de direito). Elas funcionam como moeda de troca e como estímulos, moldando o comportamento dos titulares de dados e dos agentes de tratamento de dados com seus resultados. Além disso, a maneira como os reguladores aplicam as opções de *enforcement* é decisiva para obter responsividade, proatividade e cooperação, posturas necessárias para a efetividade das políticas públicas sobre privacidade e proteção de dados no contexto da sociedade informacional.

6.2 O *enforcement* e a modulação da cultura de privacidade e proteção de dados

Conforme demonstrado no Capítulo 3, há uma adoção mundial de normas de proteção de dados semelhantes com relação ao seu conteúdo essencial. A maioria delas é baseada em princípios que podem ser resumidos conforme demonstrado no Capítulo 3 (tabela 1). Isso acontece devido a uma necessidade de convergência regulatória para lidar com questões emergentes na sociedade informacional que demandam esforço transnacional. Devido à convergência regulatória, a forma como a lei é aplicada desempenha um papel fundamental na efetividade da regulação e, no que diz respeito aos mecanismos disponíveis para o titular de dados para buscar a tutela dos seus direitos. A importância do *enforcement* também está ligada ao fortalecimento da cultura de privacidade e proteção de dados.

Como pode ser observado nos capítulos anteriores, o *enforcement* não é promovido apenas por instituições públicas. No mesmo sentido, sua realização nunca gera um bem puramente privado ou público, ou resulta em benefícios exclusivamente individuais ou coletivos, separadamente (JOHNS, 2019, p. 546-548; DEANGELO, HUMPHREYS,

REIMERS, 2017). Conforme demonstrado nos Capítulos 4 e 5, embora a Austrália ainda não tenha um direito à privacidade ou um direito autônomo à proteção de dados formalmente reconhecidos, ela estabeleceu um sistema democrático e efetivo de *enforcement* do *Privacy Act 1988* (Cth). Vale lembrar que a tese trata da efetividade do ponto de vista da proteção ao indivíduo, de como ele pode ter seu direito à autodeterminação informacional coberto, de como pode buscar a concretização do seu direito à proteção de dados pessoais.

Sob essa perspectiva, no Brasil ocorre o contrário: a lei é extremamente detalhada em termos de como prescreve os direitos e reconhece a importância dos dados pessoais. No entanto, o *enforcement* desses direitos depende do litígio judicial, pois o titular de dados não tem outra forma de buscar uma solução para seu próprio problema. No contexto brasileiro, todas as petições e denúncias feitas à ANPD são agregadas e utilizadas para orientar seu planejamento de investigações e fiscalizações. Além disso, as penalidades financeiras da LGPD, quando aplicadas, são revertidas para um fundo em favor dos direitos difusos. A única forma administrativa de tratar um problema de privacidade é se a questão estiver coberta pelo *Código de Defesa do Consumidor* (*Lei Federal nº. 8.078/1990*). Mesmo considerando que a reversão de penalidades para um fundo público tem o objetivo teórico de aumentar a ressonância coletiva da privacidade, ela produz um efeito dissuasivo sobre os titulares de dados para que busquem a concretização de seus direitos de privacidade e proteção de dados. Junto com isso, é necessário observar que os direitos de privacidade são concebidos no mundo ocidental a partir de uma perspectiva individual (RODOTÀ, 2008). A individualidade é enfatizada pelos valores e pontos de vista predominantes na sociedade informacional.

Essas duas perspectivas diferentes de *enforcement* (brasileira e australiana) resultam em impactos distintos na cultura de privacidade. Do ponto de vista do titular dos dados, sentir-se motivado a denunciar violações e a fazer petições exige uma recompensa direta. É difícil entender a importância da política pública para a comunidade, pois a concepção da lei é construída em uma abordagem individual. Portanto, ter uma opção sem custo para buscar a realização correta para o indivíduo do seus direitos à privacidade e proteção de dados é essencial para aumentar o engajamento e promover a privacidade coletivamente. Quanto mais os indivíduos estiverem engajados, mais eles atuarão como multiplicadores da aplicação da inteligência da LGPD e dos valores da política pública por ela subsidiada. Portanto, quanto mais os indivíduos estiverem comprometidos com a política, mais eles exigirão dos agentes de tratamento de dados o respeito aos seus direitos. Então, do ponto de vista dos agentes de tratamento de dados, se o aumento no número de petições diretas não ampliar a compreensão sobre a necessidade de se adaptar aos requisitos da LGPD, o aumento no número de demandas

administrativas contra eles (com a possibilidade de serem aplicadas compensações financeiras) será incluído como um risco tangível para a sustentabilidade dos negócios, aumentando o nível de conformidade com a lei. Haveria impacto, ainda, no que tange a disponibilidade para cooperar ao responder a uma investigação administrativa.

A dependência de judicialização, de litígio civil, permite a postura do processador de dados de calcular e tolerar o risco de ser cobrado e opera um efeito de dissuasão sobre os titulares de dados, que terão que arcar com custos e suportar o ônus de burocracia maior para ter sua demanda atendida. Isso envia a mensagem ao indivíduo, titular de dados, de que o direito reconhecido não é tão relevante quanto se afirma. E para os agentes de tratamento que manter suas atividades centradas no lucro viabilizado pela despossessão de dados (em vez de centradas no direito do titular de dados) vale a pena. Isso agrava um círculo vicioso de legitimação da exploração de dados pessoais, do uso de dados pessoais como um ativo e do desrespeito ao fundamento da autodeterminação informativa.

As análises de decisão feitas nos Capítulos 4 e 5 apoiam as inferências de que a aplicação de compensações financeiras liderada pelo regulador aumenta a cooperação e o nível de satisfação dos titulares dos dados, consequentemente aumentando a mensagem sobre a relevância dos objetivos regulatórios. Ao longo do Capítulo 5, foi demonstrado que, na Austrália, a busca de revisão das decisões do OAIC ocorre raramente, embora o pedido de revisão de mérito perante o AAT não envolva custos financeiros para o titular de dados. Os dados revelam que o OAIC, como um tomador de decisões especializado e com foco na educação, pode conduzir os procedimentos a uma conclusão mais adequada para ambos: o titular de dados, que tem seu caso tratado individualmente e as compensações por perdas feitas, e os propósitos educacional e de estímulo à responsividade dos agentes de tratamento de dados. Além disso, diante de um decisor especializado, os titulares de dados apresentam demandas focadas em questões de privacidade e proteção de dados, colaborando para o desenvolvimento de um entendimento claro e robusto da regulação. No Brasil, as demandas judiciais relativas à privacidade muitas vezes têm esse tema como uma questão orbital. Isso dificulta ainda mais a definição do que se espera dos agentes de tratamento de dados e sobre os limites entre um tratamento legítimo e uma violação à proteção de dados pessoais.

Gehan Gunesekara (2021), em uma pesquisa baseada na comparação de quatro modelos de aplicação da regulamentação da privacidade (da Austrália, Nova Zelândia, Reino Unido e Hong Kong) de 2013 a 2018, concluiu que é necessário um *enforcement* proativo, liderado pelo regulador, em vez do lastreamento do reforço à regulação na judicialização, como tem acontecido no Brasil. A judicialização gera decisões tomadas por juízes que não são

especializados em privacidade e proteção de dados, produzindo resultados heterogêneos que tornam os requisitos de conformidade com a regulação da privacidade e da proteção de dados confusos para os regulados, aumentando a sensação de insegurança jurídica. A sensação de insegurança jurídica também se espalha para os titulares dos dados, pois eles obtêm decisões e indenizações diversas quando litigam sobre problemas semelhantes.

Todos os pontos mencionados impactam o alcance dos objetivos regulatórios, definidos no *Planejamento Estratégico*[204] da ANPD como sendo compostos por três frentes de trabalho: primeiro, promover o fortalecimento da cultura de proteção de dados pessoais; segundo estabelecer um ambiente regulatório eficaz para a proteção de dados pessoais; terceiro, melhorar as condições para o cumprimento das competências legais. O fato de as decisões serem tomadas pela Autoridade reguladora da lei contribui para um melhor entendimento das expectativas regulatórias, fomentando o engajamento. Ter uma visão clara das expectativas e de como a Autoridade lida com os conceitos e elementos do regulamento é essencial para promover o fortalecimento da cultura de proteção de dados pessoais, não apenas para os agentes de tratamento, mas também para os titulares de dados e para as Cortes judiciais. Também é vital estabelecer um ambiente regulatório eficaz para a proteção de dados pessoais, ao passo que haveria uma forma de reivindicar os direitos de proteção de dados acessível a todos os titulares de dados. A judicialização, mesmo sendo uma forma válida, não é democrática e resulta em inconsistências na eficácia da política pública. Por fim, ter recursos suficientes para viabilizar a análise individual de petições e denúncias seria um grande avanço para melhorar as condições da ANPD de exercer suas competências legais.

A próxima seção explora como a transparência, a abordagem dialógica e a possibilidade de compensar perdas na esfera administrativa impulsionam a aplicação da privacidade na Austrália, em relação ao *Privacy Act 1988* (Cth), mesmo com uma lei que pode ser vista como "ultrapassada" em comparação com a LGPD no contexto da sociedade informacional.

6.3 Transparência, aposta na abordagem dialógica, e possibilidade de ter perdas compensadas na esfera administrativa

Como demonstrado, na sociedade informacional, em que os Estados nacionais têm seu poder modificado, especialmente no que diz respeito ao exercício legislativo autoral, resultando

[204] Disponível em https://www.gov.br/anpd/pt-br/acesso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf. Acesso em 10 Jul. 2023.

em uma tendência de adoção de padrões internacionais para se manterem pertencentes e adequados ao mercado em rede, o *enforcement* é um diferencial para o sucesso ou fracasso de uma política pública.

A existência de *enforcement* público e privado também é uma característica importante para a efetividade das políticas públicas. Nesse ponto, o contexto brasileiro de privacidade e proteção de dados tem uma vantagem, em comparação com o cenário australiano. Isso porque a LGPD estabelece uma distinção entre os tipos de processadores de dados, em controladores e operadores, e atribui a todos os envolvidos em uma cadeia de tratamento a responsabilidade solidária por violações de proteção de dados, o que significa que o titular dos dados pode demandar contra qualquer pessoa na cadeia de tratamento (art. 42, LGPD). Isso visa a garantir a proteção dos titulares de dados e consiste no reconhecimento da sua vulnerabilidade e da assimetria de poder perante os agentes de tratamento de dados. A previsão de responsabilidade solidária cria uma rede para *enforcement* privada. Todos os agentes de tratamento de dados vinculados têm o dever de monitorar as práticas de privacidade de seus parceiros e fornecedores, pois seus erros podem resultar em penalidades para eles mesmos. Sob a estrutura da LGPD, os controladores, definidos como processadores de dados que determinam a finalidade do tratamento, devem fornecer orientações aos operadores e guiar suas atividades no processamento de dados pessoais. Por outro lado, os operadores, que simplesmente tratam os dados pessoais em nome do controlador, devem seguir as orientações dos controladores e a lei nos tratamentos de dados empreendidos.

O nível pessoal de culpabilidade é levado em conta para permitir o direito de recurso de um processador de dados, eventualmente cobrado em excesso, contra outro. E a responsabilidade pode ser evitada se verificada uma das circunstâncias excepcionais do art. 43, da LGPD: se comprovarem que não realizaram o tratamento de dados pessoais que lhes foram atribuídos; se demonstrarem que, embora tenham realizado o tratamento de dados pessoais que lhes foram atribuídos, não houve violação da legislação de proteção de dados; ou, ainda, que o dano experimentado pelo titular dos dados se deve à sua culpa exclusiva ou de terceiros. Com relação a uma falha de terceiros, os processadores devem provar que adotaram todas as medidas razoáveis para evitar incidentes de segurança da informação e promover a segurança dos dados, considerando o estado da técnica vigente.

Como permanece explícito na abordagem da LGPD para a responsabilidade civil dos processadores de dados, a estrutura de *enforcement* brasileira se baseia no litígio judicial para fazer valer a proteção de dados, já que a aplicabilidade das penalidades pela ANPD não é revertida em benefício direto dos titulares dos dados. Como enfatizado, a ANPD não analisa e

trata individualmente as petições e denúncias recebidas. Além disso, todas as multas aplicadas pela autoridade após a realização de procedimentos administrativos sancionatórios são destinadas a um fundo público para fomentar a defesa dos direitos difusos.

A análise agregada de petições e denúncias feita pela ANPD tende a ser conduzida por um critério nebuloso se consideradas a lista de investigações em andamento[205] e a primeira penalidade aplicada em 05 de julho de 2023. A ANPD não publica estatísticas sobre as petições e denúncias recebidas, que permitiria o controle coletivo sobre a razoabilidade dos critérios adotados para orientar suas atividades de fiscalização (ao menos até novembro de 2023). Essa falta de transparência é outra lacuna a ser abordada para aumentar a eficácia regulatória e a efetividade da política pública do ponto de vista do titular dos dados. Por exemplo, a primeira penalidade após um processo administrativo sancionatório foi aplicada a uma microempresa[206] que não está mais em atividade. Mesmo concordando com a decisão e reconhecendo o *modus operandi* nocivo do regulado penalizado, é provável que a escolha de investigar mais a fundo e sancionar a empresa tenha sido motivada pela fonte da denúncia, o Ministério Público Estadual. Os fatos que motivaram a investigação ocorreram nas eleições de 2020, sendo a demora na conclusão outro ponto fraco da abordagem da ANPD. A apontada falta de transparência é nociva à finalidade da política pública e representa uma ameaça à imagem da autoridade e à desejável imparcialidade e impessoalidade das atividades de fiscalização.

No Brasil, a única opção que resta aos titulares de dados para obterem seus danos decorrentes de violações de proteção de dados é litigar perante os tribunais (exceto quando se trata de um caso de direito do consumidor). Essa característica da estrutura brasileira de proteção de dados fragiliza a efetividade da política pública e torna seus resultados limitados em termos de abrangência. Nem todo mundo tem conhecimento e condições financeiras para arcar com uma demanda judicial. Além disso, a duração média de um processo judicial tende a ser maior do que a duração de um processo administrativo. Isso leva a uma probabilidade de que a decisão judicial tenha um efeito menos restaurador em relação ao problema apresentado pelo titular de dados. A demora em resolver o problema afeta a compreensão dos titulares dos dados sobre a importância dos direitos de privacidade (privacidade, intimidade, proteção de dados e autodeterminação informativa) e faz com que a contestação da regulação, a inércia e a

[205]Lista disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao. Acesso em 10 Jul. 2023.
[206] Consulte o site da ANPD para obter mais informações e acessar as decisões e o relatório que as fundamentou. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd Acesso em 10 Jul. 2023.

conformidade de aparência valham a pena para os agentes de tratamento de dados (entre os quais, as plataformas digitais.)

Na Austrália, por outro lado, a possibilidade de reclamar ao OAIC e de ter as perdas econômicas e não econômicas compensadas na esfera administrativa fortalece a proteção do titular de dados e incentiva todos os interessados a agir como vigilantes da privacidade. Da mesma forma, cria uma demanda para os processadores de dados, motivando-os a cumprir as normas de privacidade (como estratégia de sustentabilidade da sua atividade). Devido ao acesso mais amplo às reclamações, o número de demandas enfrentadas pelos processadores de dados tende a aumentar, criando uma pressão indireta para a conformidade a fim de evitar desvantagens financeiras e reputacionais.

O argumento de que o tratamento individual de petições pela Autoridade de Privacidade, com a possibilidade de compensar as perdas, pode aumentar o engajamento dos titulares de dados em relação ao enriquecimento sem causa só é razoável se a Autoridade aceitar petições infundadas, incentivando "aventuras" jurídicas. Entretanto, se o órgão adotar uma postura firme e um padrão rigoroso para conceder eventuais compensações, os resultados da aplicação serão mais homogêneos, consistentes, confiáveis e democráticos. Vale a pena mencionar que o padrão adotado pelo OAIC torna as indenizações de fato "razoáveis, mas não mínimas". Das decisões analisadas na tese, o valor máximo de compensação foi de AU$ 19.980 (de 2013 a 2018, Gunasekara encontrou a faixa de compensações feitas pelo OAIC de AU$ 1.000 a AU$ 20.000, apoiando o argumento da consistência do padrão decisório). Haveria menos distinção no acesso à proteção de dados com base no poder financeiro, pela necessidade de litigância judicial se tornar medida secundária e subsidiária. Analisar individualmente as petições e responder a elas também seria benéfico em termos de aumento da transparência quanto à atuação da ANPD.

A partir da análise comparativa feita, ficou claro que a adoção de uma abordagem dialógica durante a investigação e o tratamento da disputa entre o titular de dados e o agente de tratamento é benéfica para o engajamento das pessoas e do mercado com a regulamentação da privacidade e da proteção de dados. O OAIC adota esse tipo de abordagem dialógica e, ao fazê-lo, cumpre seu objetivo educativo e acaba por resolver muitos conflitos por meio da conciliação, resultando em uma solução mais rápida e menos dispendiosa para a violação encontrada. No entanto, a abordagem dialógica e a regra da primeira tentativa de conciliação estão associadas à possibilidade de escalar as sanções para multas, medidas preventivas, injunções e diretivas com o objetivo de resolver a reclamação e fazer valer a norma e o valor da privacidade.

A existência de uma escala de punições permite que o regulador lide com elas como estímulos, sendo sensível ao nível de cooperação apresentado pelo regulado. Quanto mais o

regulado cooperar e demonstrar compreensão e boa vontade em cumprir a norma, menos coercitiva será a punição aplicável. Além disso, as punições que contêm medidas para remediar as violações e evitar a recorrência são priorizadas, contribuindo para atingir os objetivos da política, obstando a reincidência na mesma violação.

Um indicador de quão satisfatória é a abordagem adotada pelo OAIC no tratamento de reclamações de privacidade para os titulares de dados é que suas decisões raramente são questionadas, conforme demonstrado pela análise das decisões tomadas no Capítulo 5. E isso acontece em um contexto em que o pedido de revisão de mérito perante o AAT não implica custos para o titular de dados (foram encontrados apenas 11 casos perante o AAT de 2020 a 2022, e nenhum deles tratava essencialmente de reclamações relativas ao *Privacy Act 1988* (Cth), a maioria deles estava relacionada ao *Freedom of Information Act 1982* (Cth) e alguns ao *Safety Rehabilitation and Compensation Act 1988* (Cth)). É importante mencionar que o relatório sobre a decisão do OAIC é sempre feito com orientações sobre como solicitar a revisão perante o AAT, mencionando o prazo para fazer uma solicitação e a eventual possibilidade de recorrer à FCA em caso de erro na aplicação da lei ou abuso na conduta do *Information Commissioner*.

Além disso, as características mencionadas são pontos fortes em favor da efetividade para satisfazer democraticamente o titular dos dados e impulsionar o comportamento cooperativo dos agentes de tratamento de dados. Não se ignora que a promoção de modificações no arcabouço brasileiro para incluir o processamento individual de petições e denúncias pela ANPD demandaria gastos para o crescimento de sua estrutura e aumento de seus recursos, especialmente no que se refere a recursos humanos. No entanto, o custo seria um investimento e resultaria em uma ampliação da efetividade da política pública de proteção de dados.

Além disso, dar transparência aos critérios adotados para orientar as atividades de inspeção é uma medida acessível e pode ser aplicada em um curto espaço de tempo, exigindo menos gastos. Seria desejável não apenas divulgar informações sobre os critérios em si, mas também colocar estatísticas e informações gerais sobre as petições e denúncias recebidas à disposição para consulta pública. Essa medida seria benéfica para endossar a razoabilidade das escolhas feitas pela ANPD e permitir o controle coletivo de suas atividades, funcionando como um canal de prestação de contas.

Lidar com políticas públicas exige uma postura mental prospectiva voltada para a melhoria contínua. E o aprimoramento exige o monitoramento e o recálculo de rotas, para melhorar a proteção e promover o engajamento com os valores promovidos pela política pública. Parte das lacunas mencionadas nas estruturas de privacidade e proteção de dados da

Austrália e do Brasil é motivada pela forma como a noção de privacidade foi desenvolvida, do ponto de vista individual. Também são resultado do fato de a privacidade ter um conceito desordenado e estar em constante modificação para acompanhar o ritmo do desenvolvimento tecnológico e as modificações contextuais dele decorrentes. A próxima seção discute tópicos a serem incluídos na regulação da proteção de dados para aumentar a proteção ao corpo digital.

6.4 Temas a serem incluídos na regulação da Proteção de Dados e na política pública

O foco desta seção é apontar as lacunas no nível normativo dos regimes regulatórios brasileiro e australiano de privacidade e proteção de dados. A privacidade é um conceito elusivo e fluido, com uma trajetória marcada por rupturas e continuidades. Mesmo que essa característica possa parecer uma falha, é necessário considerar que, para lidar com a inovação e com o surgimento de novas tecnologias, a liquidez da definição é benéfica. Até mesmo as leis baseadas em princípios são desejáveis para permitir que a regulação se adapte à mutabilidade contextual da sociedade informacional. Dito isso, é razoável reconhecer que, uma vez abordada a perspectiva vigente do direito como instrumento de regulação dos riscos que possibilitam o convívio em sociedade, as leis de privacidade e proteção de dados analisadas estão no caminho adequado quanto às suas características gerais.

Conforme diagnosticado no Capítulo 3, as leis de privacidade estão atualmente focadas na segurança da informação, em vez da proteção de direitos, dando ênfase frequente ao "nível adequado de segurança" como uma condição necessária para a "continuidade desejável dos fluxos de dados mundiais". A LGPD e o *Privacy Act 1988* (Cth) não fogem ao padrão mencionado. Mesmo considerando a atenção mais profunda da *LGPD* em termos de enumeração de direitos, em comparação com o *Privacy Act* 1988 (Cth), ambas são leis de segurança da informação, se as analisarmos de forma objetiva quanto às suas repercussões práticas. E, como tal, não abrangem a proteção total do corpo físico e informacional do titular de dados (mencionado nesta tese como corpo digital), buscando em seu conteúdo direcionar e mitigar danos. Ambas podem ser melhoradas com a adoção de uma perspectiva mais proativa para aumentar a proteção da personalidade.

Os Capítulos 2 e 3 mostraram que a perspectiva vigente da privacidade é centrada no indivíduo[207], concebida e alinhada com a tradição liberal dos direitos fundamentais, concedendo

[207] Conforme mencionado, a noção de privacidade deriva da concepção de propriedade e foi desenvolvida com o pressuposto da burguesia. Sobre isso, é interessante a citação a seguir: "[...] A realização das condições materiais

proteção teórica "*in particular, to individual self-determination, to individual decisions and behaviour at will, to one's own body, or to property*"[208] (ALBERTS, 2014, p. 217). Isso representa uma oportunidade perdida de entrar na dimensão política e social da privacidade (VÉLIZ, 2021, p. 216-219), que deve se comprometer com a proteção de informações de grupos e tratamentos de dados agregados. Assim, uma das lacunas na proteção da personalidade que são notadas em ambas as normas é a falta de tratamento da proteção de dados pessoais agregados e dados de grupos. Entretanto, a privacidade é uma questão coletiva, e a exposição de um indivíduo pode colocar em risco a privacidade de muitos que estão relacionados a ele. Por esse motivo, os tratamentos de dados pessoais feitos com dados agregados devem ser considerados pelas leis de privacidade.

Há um padrão geral relativo ao entendimento de que, assim como os dados pessoais anônimos, os dados pessoais agregados não são considerados dados pessoais para fins regulatórios, uma vez que não permitem, pelo menos em teoria, a identificação dos indivíduos. Para de fato abranger a proteção do corpo digital e os direitos da personalidade, as leis de privacidade devem cobrir o conjunto de informações sobre o indivíduo, mesmo quando não forem usadas para fins de identificação. Conforme mencionado por Carissa Véliz, os dados relativos ao DNA, por exemplo, expõem toda a família, mesmo quando submetidos à "desidentificação" ou "pseudoanonimização", pois, devido ao seu caráter personalíssimo, podem ser facilmente reidentificados, como comprovado por Bradley Malin e Latanya Sweeney, que conseguiram reidentificar de 98 a 100% dos indivíduos cujos dados genéticos anonimizados estavam disponíveis publicamente sobre doenças específicas (VÉLIZ, 2021, p.35-36). Mark Taylor (2020) usa o exemplo da pandemia da COVID-19 para enfatizar que os dados de grupos podem representar um risco de danos tangíveis. De acordo com Taylor (2020), os indivíduos afetados pelo coronavírus sofreram um risco de dano tangível derivado do tratamento de dados de grupo. Taylor dá outros exemplos de como a tecnologia aplicada às políticas públicas e à tomada de decisões pode colocar alguns grupos em risco:

> For example, algorithmic bias may result in decision support systems in health care not working as well for some groups as for others. Image recognition systems trained mostly on images of light coloured skin, such as those trained to identify skin cancer,

---

para a satisfação da necessidade de intimidade surge como um momento de um processo mais complexo, através do qual a burguesia reconhece a própria identidade no interior do corpo social. A possibilidade de aproveitar plenamente a própria intimidade é uma característica que diferencia a burguesia das demais classes e o forte componente individualista faz com que esta operação se traduza, posteriormente, em um instrumento de isolamento do indivíduo burguês em relação à sua própria classe. O burguês, em outros termos, apropria-se de um seu "espaço", com uma técnica que lembra aquela estruturada para a identificação de um direito de propriedade "solitária"". (RODOTÀ, 2008, p. 27).

[208] "em particular, à autodeterminação individual, às decisões individuais e ao comportamento por vontade própria, ao próprio corpo ou à propriedade". (ALBERTS, 2014, p. 217). *Tradução nossa.*

> have been shown to not work as well for those with darker skin due to biases in the training data. It is also possible for groups to be deliberately targeted by datadriven technological advance. An example here would be the camera reliant upon artificial intelligence to automate Uyghur identification. An existing, and already stigmatised or otherwise disadvantaged group, can thus be subject to increasingly automated discrimination by developments in data-driven technology. (TAYLOR, 2020, p. 733).[209]

Ao tratar de dados de grupo no campo da pesquisa médica, Joan McGregor (2010, p. 24) explica que o dano ao grupo pode ser classificado em dano tangível e dignitário:

> Tangible consequential harm to a group includes stereotyping or stigmatizing a group so that its members are ostracized, humiliated, or discriminated against, resulting in loss of social, economic, or political opportunities or even loss of face in the society. […] Dignitary harms to groups undermine the perceived value and worth of the group in the eyes of others and the group itself. Dignitary harms can result when treatment is disrespectful to the group, treating members and their cultural beliefs and traditions as inferior, disparaging them, or otherwise not taking them seriously. (MCGREGOR, 2010, p. 24).[210]

Assim, é relevante considerar a privacidade e a proteção de dados como um fenômeno complexo, que no contexto da sociedade informacional, considerando a atuação das plataformas digitais e o rápido desenvolvimento da computação ubíqua, deve ser concebido para além da identificabilidade do titular de dados, rompendo com a perspectiva puramente individual. Vale lembrar que dados agregados e dados de grupos, mesmo destituídos do potencial de identificabilidade, podem ser utilizados para construir informações e influenciar de forma calculada as decisões tomadas pelo grupo, o que, conforme mencionado por Brent Mittelstadt (2017, p. 481), impacta diretamente o comportamento dos membros do grupo e sua personalidade[211]. Elas também podem ser processadas para apoiar decisões sobre o grupo, afetando os objetivos coletivos e gerando desvantagens injustificadas para seus membros (por

---

[209] "Por exemplo, o viés algorítmico pode fazer com que os sistemas de apoio à decisão na área da saúde não funcionem tão bem para alguns grupos quanto para outros. Foi demonstrado que os sistemas de reconhecimento de imagens treinados principalmente em imagens de pele clara, como os treinados para identificar câncer de pele, não funcionam tão bem para pessoas com pele mais escura devido a vieses nos dados de treinamento.19 Também é possível que grupos sejam deliberadamente visados por avanços tecnológicos orientados por dados. Um exemplo seria a câmera que depende de inteligência artificial para automatizar a identificação de uigures.20 Um grupo existente e já estigmatizado ou em desvantagem pode, portanto, estar sujeito a uma discriminação cada vez mais automatizada por desenvolvimentos em tecnologia orientada por dados." (TAYLOR, 2020, p. 733). *Tradução nossa.*

[210] O dano tangível consequente a um grupo inclui estereotipar ou estigmatizar um grupo de modo que seus membros sejam condenados ao ostracismo, humilhados ou discriminados, resultando na perda de oportunidades sociais, econômicas ou políticas ou até mesmo na perda de prestígio na sociedade.
[...] Os danos à dignidade dos grupos prejudicam a percepção do valor do grupo aos olhos dos outros e do próprio grupo. Os danos à dignidade podem ocorrer quando o tratamento é desrespeitoso com o grupo, tratando os membros e suas crenças e tradições culturais como inferiores, menosprezando-os ou não os levando a sério. (MCGREGOR, 2010, p. 24). *Tradução nossa.*

[211] Usando a teoria da informação de Luciano Floridi, Mittelstadt concebe que a identidade é constituída por informações que descrevem o indivíduo ou o grupo. Então, "as violações de identidade são consideradas um ataque à pessoa que é constituída por suas informações" (*"breaches of identity are considered to attack on the person who is constituted by her information"*) (2017, p. 482), e o autor afirma que o uso da análise de dados e da tomada de decisões automatizada gera essas violações de identidade porque restringe a capacidade do grupo de moldar suas próprias informações.

exemplo, causando discriminação ou exclusão). Muitos estudiosos já estão apontando para a urgência de conceber a proteção de dados, incluindo uma vertente de privacidade de grupo (RODOTÀ, 2008; TAYLOR, 2020; MITTELSTADT, 2017; MACHADO, MENDES, 2020). Os desafios relacionados aos dados de grupo também foram abordados no Capítulo 5.

Para abranger melhor a proteção do titular de dados, uma concepção de um direito à privacidade deve ser incluída em outras emendas ao *Privacy Act 1988* (Cth). Idealmente, o direito à privacidade deveria vir acompanhado da previsão expressa do direito à proteção de dados, como uma dimensão mais específica da privacidade associada à autodeterminação informativa. A previsão explícita de direitos à privacidade e à proteção de dados criaria uma causa de ação, permitindo que os indivíduos, quando necessário, busquem os direitos perante os tribunais. A medida ampliaria a proteção já estabelecida.

Além disso, outra melhoria benéfica poderia ser a exigência de um responsável pela privacidade nomeado pelas *APP entities* na Austrália. O *Privacy Act 1988* (Cth) não exige essa nomeação, embora as *APP Guidelines* considerem a medida uma boa prática. A LGPD trata a nomeação do Encarregado de Dados como uma obrigação para todos os agentes de tratamento de dados, entretanto, os guias emitidos pela ANPD não estabelecem a necessidade de o responsável pela governança da privacidade e proteção de dados desempenhar exclusivamente esse papel na instituição. Essa lacuna resulta na nomeação de muitos profissionais que não estão preparados para desenvolver as ações esperadas, frequentemente acumulando a função com outras tarefas relacionadas à sua função original. Espera-se que o Encarregado/*Privacy Officer* atue não apenas representando a instituição perante a Autoridade de Privacidade e perante os titulares de dados, mas também como líder do programa de privacidade e proteção de dados, para orientar e zelar pela conformidade das atividades, práticas e processos realizados pelos membros da instituição com relação à regulação da privacidade. Assim, é desejável que em ambos os contextos, australiano e brasileiro, a nomeação de um *Privacy Officer* / Encarregado de Dados seja obrigatória, e o papel a ser desempenhado seja a principal função do profissional indicado. Ou seja, que haja uma obstaculização no que tange a cumulação de funções com o desempenho do cargo de Encarregado de Dados / *Privacy Officer.*

Ainda em relação ao contexto australiano, seria benéfico fazer uma emenda para submeter o uso de informações pessoais de crianças a um controle rigoroso e à confirmação dos pais ou responsáveis legais. Atualmente, o *Privacy Act 1988* (Cth) não distingue regras para o uso e processamento de informações pessoais de adultos e informações pessoais de crianças (o sistema jurídico australiano não estabelece a distinção entre crianças e adolescentes, utilizando a nomenclatura de “criança” para todos os menores de 18 anos). Considerando a imaturidade

das crianças e o fato de que elas ainda estão em desenvolvimento, e a inexistência da viabilidade de um direito de ser esquecido na sociedade informacional, os tratamentos de dados pessoais realizados durante a infância têm o potencial de afetar as chances de vida do futuro. Essas crianças podem sofrer duras consequências na vida adulta devido às interações e à exploração de dados vivenciadas no início da vida. Em relação ao contexto brasileiro, embora a estrutura da LGPD tenha regras especiais para o tratamento de dados pessoais de crianças, o entendimento estabelecido pela ANPD em relação à base legal para isso neutralizou a proteção especial (veja o *enunciado CD/ANPD nº 1, de 22 de maio de 2023*[212]). Isso porque, de acordo com o referido enunciado, os dados pessoais de crianças são tratados legitimamente sob as mesmas base legais que as informações pessoais de adultos (arts. 7º e 11 da LGPD).

Para além do plano normativo, o melhoramento de ambas as políticas passa por uma maior conscientização do titular de dados pessoais quanto ao valor desses dados, o quanto a sua exposição os vulnerabiliza e impacta a sua formação de vontade, e como a manipulação desses dados é feita para a garantia de mercados futuros. Para tanto, além de reforço às campanhas publicitárias e projetos que visem essa conscientização desde a infância (pela aplicação de oficinas desde o ensino fundamental, por exemplo). Assim como ocorre na Austrália[213] em que o currículo escolar inclui obrigatoriamente disciplinas atinentes a tecnologia (*Design and Technologies* e *Digital Technologies*), que tem por objeto, além de capacitar os alunos para criar tecnologias e pensar em soluções de problemas de maneira inovadora e utilizando a tecnologia como instrumento, possui foco na segurança, em capacitar para o entendimento sobre os riscos da tecnologia, o Brasil deveria incorporar disciplinas no mesmo sentido à Base Nacional Comum Curricular[214]. O fornecimento desse tipo de capacitação de forma democrática, implementada também em escolas públicas seria um caminho para o empoderamento desses titulares de dados e para a diminuição da distorção causada pela divisão do aprendizado.

O campo das políticas públicas é um campo multidisciplinar. Conforme demonstrado nos capítulos anteriores, o mesmo pode ser dito sobre os direitos de privacidade e de proteção de dados. Dessa forma, tanto a política pública quanto as concepções de privacidade e proteção de dados devem enfrentar transformações constantes e contínua e ser submetidas a avaliações

---

[212]Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em 10 Jun. 2023.

[213] Vide currículo disponível em: https://www.australiancurriculum.edu.au/download/DownloadF10. Acesso em 25 Nov. 2023.

[214] Vide BNCC vigente, que não conta com ensino de tecnologia. Disponível em: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf. Acesso em 25 Nov. 2023.

regulares para o seu aprimoramento contínuo. E a comparação e emulação no sentido de aprender com experiências já testadas, adaptando-as e adequando-as ao contexto vigente é uma ferramenta valiosa para a missão de melhoria progressiva das políticas públicas e dos regimes regulatórios de direitos fundamentais na sociedade informacional.

O capítulo comparou o sistema regulatório e a política pública australianos de privacidade e proteção de dados com a estrutura brasileira de privacidade e proteção de dados. Foram enfatizadas as estratégias de *enforcement* adotadas por cada regime regulatório, bem como os efeitos dessas estratégias na cultura institucional, corporativa e social, apontando quais características constituem elementos de efetividade para a proteção dos indivíduos. Por fim, o capítulo promoveu uma análise geral, especificando temas que demandam a inclusão nas estruturas australiana e brasileira para aumentar a proteção dos indivíduos e melhorar a efetividade.

7 CONCLUSÕES

As políticas públicas possuem como suporte normativo normas que delineiam como as ações governamentais coordenadas ocorrerão, quais os agentes envolvidos, e a competência de cada um. Essas normas preveem direitos para determinados sujeitos e obrigações para outros, de maneira que operacionalizam, ao mesmo tempo, a regulação do campo sobre o qual se debruçam. A norma em si, no caso da LGPD, é elemento de regulação e de suporte normativo da Política Nacional de Proteção de Dados Pessoais. Entretanto, a LGPD não esgota o sistema de regulação proposto (apenas o desenha), tampouco se confunde com a política pública que subsidia (somente delineia seus contornos gerais). A tese analisou a estrutura institucional e os atores envolvidos na regulação do tratamento de dados pessoais e na política pública de proteção de dados, em perspectiva sociojurídica, com foco na identificação dos elementos e efetividade e inefetividade, dado o contemporâneo estágio de maturidade de ambos (da regulação e da política pública).

A tese procurou apontar caminhos para o melhoramento contínuo da Política Nacional de Proteção de Dados. Para tanto, propõe que o fortalecimento e a efetividade dessa política dependem principalmente do aprimoramento dos mecanismos de *enforcement* adotados pelo sistema de proteção brasileiro. Esse aprimoramento passa pelo fortalecimento da ANPD, com o incremento da sua estrutura e dos seus recursos humanos e técnicos, de maneira a viabilizar o processamento de petições e denúncias de maneira individualizada. Ademais, é extremamente importante a ampliação dos poderes da ANPD, incluindo a possibilidade de promover compensações aos titulares de dados por danos econômicos e não econômicos derivados de violações aos direitos previstos na LGPD. As medidas de fortalecimento mencionadas resultariam em empoderamento do titular de dados e democratização do acesso aos mecanismos para a concretização da proteção de dados pessoais no Brasil. Soma-se ao incremento em democraticidade, a ampliação do protagonismo da ANPD para de fato direcionar a execução da política pública, medir os resultados e ter poder de direcionar modificações a fim de corrigir desvios do planejamento original.

A existência de uma instância administrativa para a resolução de violações aos direitos de privacidade e proteção de dados tutelados na LGPD promoveria uma modificação na visão dos agentes de tratamento quanto à adequação das suas operações envolvendo dados pessoais. À medida que esses agentes de tratamento passarem a enfrentar numerosas demandas administrativas, que os compelirão a custos para endereçá-las (caso persistam no desafio aos objetivos da política pública e da regulação do tratamento de dados pessoais, custos com

advogados, com o pagamento das compensações, com recursos humanos dedicados a responder às solicitações da ANPD, entre outros), tenderão a elencar a conformidade com as exigências de privacidade e proteção de dados como um risco intolerável, que ameaça a sustentabilidade da sua atividade. Somente assim o respeito aos direitos de privacidade e proteção de dados será elevado ao patamar de investimento, equilibrando a racionalidade de custo-benefício que orienta a gestão de riscos empresariais. Haveria um impacto de redução da tendência de judicialização apontada pelos dados analisados e no acesso a decisões e soluções mais uniformes e robustas, posto que construídas por decisores especializados no tema. Ademais, contribuiria para a construção de vigoroso entendimento e interpretação sobre a LGPD e suas exigências, cooperando com a clareza aos agentes de tratamento quanto as expectativas e parâmetros mandatórios de adequação de suas atividades, bem como quanto às repercussões de desafiá-los, incrementando a percepção de segurança jurídica (para titulares e para agentes de tratamento).

Conforme demonstrado ao longo do Capítulo 2, na sociedade informacional a ubiquidade computacional é uma realidade, fazendo com que os dados, especialmente os dados pessoais, tenham a sua natureza transmutada, passando a consistir em *commodities*. Nesse contexto, as relações humanas passam a ser intermediadas por plataformas digitais de maneira ampla, para além das relações de consumo. Essas plataformas digitais atuam como ferramentas para a concretização do ciclo da despossessão de dados pessoais, que após enriquecimento e estruturação se transformam em informação. A capacidade de processamento de informações é a modalidade de poder explorada pelas plataformas digitais para exercer influência sobre os indivíduos e garantir mercados futuros. Sendo assim, o poder exercido pelas plataformas, capitalistas de vigilância, é alicerçado na assimetria de conhecimento existente entre os indivíduos e as plataformas, e essa assimetria de conhecimento tem raízes na divisão do aprendizado. A maior vulnerabilidade do indivíduo ocorre uma vez que o capitalismo de vigilância e de plataforma opera com fluxos transnacionais de dados, mitigando o poder dos Estados nacionais no que tange o controle dessas atividades. A mitigação das barreiras comunicacionais ocorrida no âmbito da sociedade informacional, em que o material e o digital se sobrepõem e interconectam, tem impactos na soberania estatal e na soberania individual.

Consoante elucidado no Capítulo 3, ante o cenário exposto, a concepção clássica de privacidade, como um direito estático de ser deixado só passa a ser insuficiente para a proteção do indivíduo. Reconhecendo essa insuficiência, organizações internacionais tornam-se palco para o fomento da derivação da privacidade em direitos específicos: proteção de dados (entendida como o direito de controlar os dados pessoais em fluxo), e autodeterminação

informativa (direito de determinar de que maneira os dados pessoais serão tratados, com a possibilidade de se opor a tratamentos ilegais e ilegítimos). Os direitos à proteção de dados e à autodeterminação informativa são direitos fundamentais, atinentes à personalidade. A partir do estabelecimento de standards para o tratamento de dados pessoais no âmbito dessas organizações internacionais, por meio de *soft laws*, os Estados nacionais passam a regular os processamentos de dados pessoais com a incorporação das diretrizes propostas nessas instâncias supranacionais.

Com a regulação orientada para uma convergência regulatória, tanto por uma necessidade, quanto por uma imposição da economia em rede, para permitir a continuidade dos fluxos transnacionais de dados, as normas regulatórias apresentam cunho principiológico e conteúdo bastante similar. Uma vez que os princípios orientadores das normas de privacidade e proteção de dados são similares, os mecanismos de *enforcement* passam a desempenhar papel crucial para a efetividade de políticas públicas que tenham essas normas como suporte. Consoante mencionado, o sentido de efetividade adotado para a tese é o que orientou a política pública, qual seja, a proteção do indivíduo e do seu corpo digital, formado pela agregação de dados e informações pessoais extraídos de interações com plataformas digitais, assim como o estabelecimento de ambiente relacional mais respeitoso e transparente. Os objetivos que orientaram a política visam mitigar a assimetria de poder existente entre titulares de dados pessoais e agentes de tratamento.

Num contexto em que o Estado não dispõe de poder nem de meios para sozinho promover os direitos, os atores não estatais e os sujeitos de direito passam a ser conclamados a auxiliar na promoção de objetivos públicos que justificam a regulação, pela instituição da norma. Em que pese a preocupação com um plano normativo alinhado às melhores práticas seja importante para solucionar os problemas advindos da crescente interação com plataformas, há que se ter em mente que a norma isolada não tem o potencial de alterar a realidade. Somente através das políticas públicas é que o governo pode atuar fomentando direitos assegurados numa norma, impulsionado valores e implementando estrutura institucional para que a previsão normativa ganhe vida e passe a existir no cotidiano, na realidade material.

Após a contextualização da sociedade informacional e das modificações que ela ocasionou na autonomia individual (soberania individual, autodomínio sobre o próprio corpo material e digital, e sobre as próprias escolhas), e na autonomia estatal (estado nacional conectado em rede com outras economias, necessidade de se manter em paridade de competitividade e desafios regulatórios por ser ao mesmo tempo regulador e regulado no âmbito da proteção de dados), os Capítulos 4 e 5 foram dedicados ao estudo do panorama das Políticas

Públicas de Privacidade e Proteção de Dados Brasileira e Australiana (no nível do *Commonwealth)*, respectivamente. Em que pese as diferença no que toca as tradições de cada um dos sistemas jurídicos analisados, assim como da diversidade de foco dos suportes normativos estudados, note-se a LGPD elaborada com fulcro em proteção pela instituição de direitos, e o *Privacy Act 1988* (Cth) alicerçado em diretrizes de segurança da informação, ambas as normas ostentam a identidade de função. Possuem objetivos e idealizações comuns, atinentes ao empoderamento do titular de dados e na construção de ambientes relacionais mais respeitosos e transparentes, função que serviu de eixo para a comparação conduzida.

A LGPD prevê direitos fundamentais individuais com maior especificidade, estando alinhada com os standards fixados em âmbito internacional. Entretanto, no panorama brasileiro o titular de dados dispõe somente da ação judicial como meio de exercer seu direito e de ter suas demandas solucionadas, caso não resolva diretamente com o agente de tratamento. Isso porque além de a ANPD ainda não possui estrutura para analisar as petições e denúncias recebidas individualmente, a LGPD prevê que todas as penalidades financeiras aplicadas pela ANPD são direcionadas ao Fundo de Defesa dos Direitos Difusos. A impossibilidade de obter compensação pelos danos sofridos pela via administrativa resulta em efeito de dissuasão aos titulares de dados para o peticionamento à ANPD, além de implicitamente militar em desfavor do argumento pela fundamentalidade do direito à proteção de dados.

Em sentido oposto, o *Privacy Act 1988* (Cth), que em comparação com os standards internacionais pode ser considerado obsoleto por não prever explicitamente o direito à privacidade e o direito à proteção de dados, estabelece mecanismos de *enforcement* mais efetivos. Isso porque, no panorama australiano o titular de dados que não obtiver autocomposição com o agente e tratamento de dados pode fazer uma reclamação para o OAIC e ter a sua demanda endereçada, com a obtenção de compensação por danos econômicos e não econômicos derivados da interferência na sua privacidade.

Conforme restou demonstrado, a política pública brasileira baseia o seu *enforcement* em linhas gerais na judicialização, na litigância perante o Judiciário. A predominância da litigância judicial como estratégia de *enforcement* no Brasil deriva do déficit orçamentário imposto à ANPD quando da sua criação e início das suas operações, representando uma falha de execução do plano original pensado para a política. Vale lembrar que a criação da ANPD sem custos adicionais e como órgão da Presidência da República foi fruto de um veto presidencial ao texto de lei aprovado pelo Legislativo. A política pública australiana, de outro lado, pauta o sistema de proteção na atuação do OAIC, autoridade administrativa de privacidade, como mediador do conflito e tomador de decisões para endereçar os casos concretos e solucionar a demanda dos

titulares de dados, caso não cheguem a uma resolução por conciliação com os agentes de tratamento.

A escolha do panorama federal australiano decorreu (além da busca por diversidade) do destaque que o país possui em implementação de regimes regulatórios inovadores, da maior abertura à experimentação de mecanismos de *enforcement*, e pelo destaque em termos de efetividade de políticas públicas e do bom nível de transparência na operação de instituições governamentais. Esses fatores possibilitaram a coleta de dados para análise e a imersão no sistema de regulação da privacidade e da proteção de dados australiano, através da consulta a repositórios disponibilizados ao público. Soma-se ao disposto o fato de o *Privacy Act 1988* (Cth) datar de 1988, sendo a base para um aparato institucional maduro e em operação desde a década de 1990.

O Capítulo 6 é dedicado ao estudo das estratégias de *enforcement* como ferramentas para o melhoramento contínuo das políticas de privacidade e proteção de dados analisadas. Em que pese a tese concluir que nenhuma regulação de privacidade existente tem o potencial de proteger os direitos fundamentais e da personalidade absolutamente, o *enforcement* desempenha papel relevante na modulação da cultura institucional, organizacional e social, para o entendimento da fundamentalidade dos direitos. Além de ter a capacidade de impulsionar comportamentos desejáveis entre os agentes de tratamento de dados, com base em maior ou menor fluxo de demandas enfrentadas. Vale dizer, embora o fortalecimento da ANPD e ampliação dos seus poderes não resolvam plenamente o déficit de efetividade da política de proteção de dados no Brasil, consistem em medidas que forçariam os agentes de tratamento de dados a adotar postura preventiva e responsiva, contribuindo para o objetivo de estabelecimento de um ambiente de interações mais respeitoso e transparente, em proteção aos interesses dos titulares de dados. Ademais, o estabelecimento de uma jurisdição administrativa especializada resultaria em democraticidade do acesso à proteção de dados, e em resoluções de demandas mais justas, homogêneas e promovidas por decisores especializados no assunto.

O reforço à dimensão subjetiva da proteção de dados, com a ênfase no indivíduo como agente de fiscalização e de concretização do direito, é um caminho para o melhoramento contínuo dessa política e para a sua viabilidade, ante a incapacidade do Estado de sozinho atuar na fiscalização e reforço ao direito, e à necessidade de contingenciar o *enforcement* com a escassez de recursos. Para que essa tutela seja democrática, é preciso que o indivíduo, titular de dados, tenha à disposição meios de exercer o seu direito sem custo, administrativamente, e de ter sua demanda apreciada individualmente, além do acesso a compensações econômicas e não econômicas resultantes de violações sofridas. No atual estágio de maturidade das políticas

analisadas, a ênfase na dimensão subjetiva da proteção de dados é maior, entretanto o melhoramento contínuo das políticas demanda, além das medidas elencadas na seção 6.4, o fortalecimento da dimensão objetiva da proteção de dados, com a obrigação de promover a proteção, fomentando a postura preventiva e responsiva dos agentes de tratamento, não somente a remediação. Mesmo com o foco no titular, já que a proteção ao seu corpo digital é imperiosa, entende-se como imprescindível a análise e a regulação da dimensão coletiva da privacidade e da proteção de dados.

Outrossim, sob a perspectiva da política pública, a análise dos contextos brasileiro e australiano de privacidade e proteção de dados reforçou o entendimento de que a lei como suporte normativo apresenta um delineamento inicial da política. Não obstante, existe um hiato quanto à execução, cujo sucesso está intimamente ligado a questões orçamentárias que impactam a estruturação do sistema de proteção e a atuação de seus atores, atingindo a qualidade das estratégias de *enforcement.* Em que pese a efetividade de políticas públicas estar atrelada à dotação orçamentária, a sua avaliação deve ultrapassar a aplicação de parâmetros meramente econômico-financeiros, quantificáveis de forma direta. O campo de avaliação de políticas públicas precisa ser expandido para que ocorra com frequência (e não de maneira episódica e por amostragem como acontece). Há a necessidade de se construir indicadores que permitam avaliar a efetividade de resultados que não sejam aferíveis por critérios puramente econômico-financeiros.

Verificou-se, ainda, que, em que pese as leis de privacidade e proteção de dados sejam instituídas com a justificativa da necessidade de proteger o indivíduo e o livre desenvolvimento da sua personalidade, a partir do seu empoderamento, na prática essas leis instituem normas de segurança da informação. O foco na segurança da informação é inferido pelos preâmbulos que reforçam a necessidade de se assegurar a continuidade dos fluxos transnacionais de dados, e na fixação de níveis de proteção que, uma vez atingidos, autorizariam o compartilhamento legítimo desses dados entre estados. Assim, embora o valor colocado como central para a norma e para a política pública sejam o livre desenvolvimento da personalidade, e a proteção da dignidade da pessoa humana, predomina como resultado o fomento ao disciplinamento do ambiente de negócios. O resultado da política pública estabelece um panorama de estabilização aparente dos desafios do digital, pela instituição de normas que validem e incentivem a continuidade dos fluxos transfronteiriços de dados pessoais.

A ubiquidade computacional na sociedade informacional eleva a *infoesfera* das plataformas digitais ao patamar de ambiente em que os sujeitos e os grupos interagem, definindo e sendo definidos por seus dados em fluxo. A ascensão do digital como habitat do

humano impacta a formação da personalidade e da configuração social. Isso porque a construção da identidade pessoal *on-line* influencia o entendimento do indivíduo sobre si e sobre os grupos que integra. A sociedade e a cultura são afetadas pelo digital e pela dinâmica de construção dessas identidades pessoais. A presença no digital não é mais facultativa. Os seres humanos são compelidos na sociedade informacional a construir essa identidade e a utilizar as plataformas digitais como meios de interação. E a tendência é que esse fenômeno se torne mais complexo, com a rapidez da evolução tecnológica e com o acesso a melhores estruturas de conexão.

Da mesma maneira, emergem questões atinentes ao delineamento da soberania digital. Na teia da sociedade informacional esse tema já é uma questão política desafiadora, basta lançar um olhar atento ao papel político das plataformas (na mobilização da opinião pública como ocorreu em relação ao projeto de lei brasileiro para regulação de plataformas – PL nº. 2630/2020 e substitutivos, outro exemplo interessante é o embate entre o *Twitter* e Donald Trump, após as invasões ao Capitólio nos EUA em janeiro de 2021) e à impotência dos Estados nacionais para barrar o poder das empresas e tecnologia (vide decisões judiciais administrativas contra a Meta por violações à privacidade dos usuários, e a crescente onda de *ransomware* contra bancos de dados governamentais). Sem mencionar a transmutação do poder financeiro das plataformas em poder político pelo exercício do *lobby* perante as arenas transnacionais que influenciam a produção legislativa e a regulação locais.

É sabido que o melhoramento contínuo é um pressuposto no campo das políticas públicas. Em que pese a sua teórica imanência, integrando uma vertente do planejamento, a medição de resultados com posterior revisão de estratégias de ação não é aplicada sistematicamente no âmbito brasileiro. Quando realizada a medição de resultados os critérios empregados são centrados em um conceito de eficiência que demanda mensuração de custos com resultados materiais economicamente apreciáveis. Tais critérios fazem com que a aplicabilidade à Política Nacional de Proteção de Dados seja nebulosa, já que os objetivos da política não atendem aos requisitos de quantificação dos indicadores utilizados no âmbito da avaliação de políticas públicas.

A pesquisa concluída demonstra a imprescindibilidade de se traçar a linha de distinção entre lei e política pública em todas as searas, mas com especial urgência no que tange à proteção de dados pessoais. O fato de a LGPD espelhar o *GDPR*, tido como standard para a proteção de dados gera uma confusão na apreciação da Política Nacional de Proteção de Dados pelos cidadãos, e mesmo em estudiosos do campo das políticas públicas. É preciso explicitar que a política pública não se confunde com a lei que a prevê, e que essa lei somente ganhará

facticidade a partir do trabalho coordenado entre os membros do parlamento, com os membros do executivo e todos que venham a atuar na estrutura de operacionalização da política pública. No caso da proteção de dados muitos agentes não estatais (agentes de tratamento e titulares de dados) são de extrema relevância para a efetividade da política e para a concretização dos valores que ela visa promover.

Imperioso reconhecer que a Política Nacional de Proteção de Dados tem como objetivo a tutela de dois bens jurídicos diversos. De um lado, o ambiente de negócios (e as relações comerciais e políticas que envolvam o tratamento de dados pessoais), visando promover maior transparência e responsabilidade ao lidar com dados pessoais, e assegurar que o Brasil tem compromisso com o respeito aos direitos reconhecidos internacionalmente na era da sociedade informacional, possuindo nível adequado de proteção de dados, e garantindo a manutenção da competitividade das empresas brasileiras no mercado transnacional em rede. De outro lado, a dignidade dos titulares de dados pessoais, seu corpo digital, ao colocar como um dos seus objetivos a proteção ao livre desenvolvimento da personalidade.

Como forma de proteger o livre desenvolvimento da personalidade, os mecanismos de *enforcement* têm que ser pensados de maneira a empoderar o titular de dados pessoais. Esse empoderamento é medida imprescindível na sociedade informacional e ante a dinamicidade do avanço tecnológico. Isso porque o conhecimento acerca do funcionamento das novas tecnologias embedadas nas plataformas que intermediam as relações e atividades é concentrado nas mãos de poucos, em virtude da divisão do aprendizado, erigida como estratégia do capitalismo de vigilância. Como a proteção de dados foi construída com uma perspectiva individual, a proteção dos valores que a promovem e fundamentam também deveria contar com mecanismos de *enforcement* que contemplassem os interesses dos titulares individualmente, de maneira democrática e acessível para todas as pessoas naturais.

A partir do estudo comparado, nota-se que ainda como maneira de empoderar o titular, a estrutura pensada para o *enforcement* deve contar com uma instância administrativa, acessível sem custo para que o titular dos dados pessoais tenha sua denúncia ou petição analisada individualmente. Isso porque proporcionaria a análise acurada das reclamações por especialistas no tema, que compõem a ANPD, responsável por fiscalizar e fomentar o cumprimento da lei que subsidia a política pública. A contrário sensu, a delegação da análise de todas as demandas individuais envolvendo proteção de dados ao Judiciário tende a produzir resultados morosos e insatisfatórios, haja vista que não existe Corte especializada no tema, e que os julgadores não são especialistas no campo.

Para além da convergência regulatória, faz-se necessária a cooperação regulatória, e a interação de autoridades nacionais de privacidade e proteção de dados com agentes não estatais em rede, com ênfase no empoderamento do titular de dados. Assim, o melhoramento contínuo de políticas públicas voltadas para lidar com problemas emergentes da sociedade informacional passa por todos os temas mencionados, que serão aprofundados nas pesquisas futuras: regulação de novas tecnologias, regimes regulatórios na sociedade informacional, impactos das plataformas na formação da personalidade, soberania digital, capacitação dos titulares de dados para a vida no digital e dinâmicas de poder na sociedade informacional.

REFERÊNCIAS

Administrative Decision (Judicial Review) Act 1977 (Cth).

AGUIAR, Rodrigo Goulart. **Sociedade em rede e internet: direitos fundamentais em diálogo.** 2015. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica do Rio Grande do Sul, 2015. 191 fls.

ALBERS, Marion; SARLET, Ingo Wolfgang (Ed.). **Personality and Data Protection Rights on the Internet: Brazilian and German approaches.** Cham: Springer, 2022.

ALISEDA, Atocha. **Abductive reasoning: logical investigations into discovery and explanations.** México: Springer, 2006.

ALLARS, Margaret. Cross-Border Transfer of Personal Information: Evolving Privacy Regulation in Europe and Australia. In: DÖOR, Dieter; WEAVER, Russel L. (eds.). **Perspectives on Privacy: increasing regulation in the USA, Canada, Australia, and European Countries.** Berlim: De Gruyter Inc., 2014. Pp. 106-125.

ALMEIDA, Rachel Letícia Curcio Ximenes de. Os cartórios e a proteção de dados. **J² — Jornal Jurídico**. [S. l.], v. 5, n. 1, p. 049–065, 2022. Disponível em: https://revistas.ponteditora.org/index.php/j2/article/view/623. Acesso em: 16 Nov. 2023.

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. **Revista Brasileira de Segurança Pública.** Vol. 16, n. 2. 2022. Disponível em: https://revista.forumseguranca.org.br/index.php/rbsp/article/view/1377/548. Acesso em 15 Nov. 2023

ALVES, Giselle Borges; SOUZA, Rodrigo Teixeira de. Comércio digital e proteção de dados: a era do Big Data. **Revista da Defensoria Pública do Distrito Federal (Online)**. 2021, Vol.3 (1). Pp.99-122. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/2021_Periodicos/Rev-Def-Pub-DF_v.3_n.1.pdf. Acesso em 15 Nov. 2023.

ANCEL, Marc. **Utilidade e métodos do direito comparado: elementos de introdução geral ao estudo comparado dos direitos.** Tradução de Sérgio José Porto. Porto Alegre: Fabris, 1980.

ANDRADE, Aparecida de Moura; SANTANA, Héctor Valverde. Avaliação de políticas públicas versus avaliação de impacto legislativo: uma visão dicotômica de um fenômeno singular. **Revista brasileira de políticas públicas.** Volume 7. Nº. 3. Dez. 2017. Disponível em: https://publicacoes.uniceub.br/RBPP/article/view/4740. Acesso em 10 Mai. 2022.

Assembleia Geral da ONU. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: https://declaracao1948.com.br/declaracao-universal/declaracao-direitos-humanos/. Acesso em 25 Jul. 2022.

ASSY, Bethânia. **Novas fronteiras entre identidade e Direitos Humanos.** Youtube, 2019. Disponível em: https://www.youtube.com/watch?v=SsgPtNwznYM. Acesso em 10 Jan. 2021.

Attorney-General's Department (Cth), "Privacy" (Web Page, 04 November 2022). Disponível em: https://www.ag.gov.au/rights-and-protections/privacy#:~:text=The%20Privacy%20Act%201988%20(Privacy,and%20in%20the%20private%20sector. Acesso em 08 Nov. 2022.

Australian Government (Cth), "Australian Law Reform Commission" (Web Page, 29 November 2022). Disponível em: https://www.alrc.gov.au/. Acesso em 29 Nov. 2022.

Australian Information Commissioner Act 2010 (Cth).

Australian Law Reform Commission Act 1996 (Cth).

AYRES, Ian; BRAITHWAITE, John. **Responsive regulation: Transcending the deregulation debate.** Oxford: Oxford University Press, 1992.

BANK, Max; DUFFY, Felix; LEYENDECKER, Verena; SILVA, Margarida. **The lobby network: big tech's web of influence in the EU.** Bruxelas: Corporate europeu Observatory and LobbyControl e.V. Brussels and Cologne, 2021.

BARAK-CORREN, Netta; KARIV-TEITELBAUM, Yael. Behavioral responsive regulation: bringing together responsive regulation and behavioral public policy. **Regulation & Governance.** Volume 15. 2021. Pp. 163-182. Disponível em: http://onlinelibrary.wiley.com/doi/10.1111/rego.12429. Acesso em 11 Dez. 2022.

BAXI, Parul. Technologies of Disintermediation in a Mediated State Civil Society Organisations and India's Aadhaar Project. **South Asia: Journal of South Asian Studies.** 2019. Volume 42. N. 3. Pp. 554-571. Disponível em: https://doi.org/10.1080/00856401.2019.1602808. Acesso em 19 Abr. 2023.

BECK, Ulrich. **Sociedade de Risco Mundial: em busca da segurança perdida.** Lisboa: Edições 70, uma chancela de Edições Almedina S.A., 2016.

BELLARMINO, Clarissa Lopes. **A proteção ético-jurídica dos dados genéticos humanos em atividades de biobancos, à luz da Constituição Federal de 1988 e das diretrizes internacionais.** 2018. Tese (Doutorado em Direito). Pontifícia Universidade Católica do Rio Grande do Sul, 2018. 174 fls.

BENNETT, Colin J.; RAAB, Charles D.. Revisiting the governance of privacy: contemporary policy instruments in global perspective. In.: **Regulation & Governance.** 2020. Volume 14. Pp. 447-464. Disponível em: https://onlinelibrary.wiley.com/doi/pdfdirect/10.1111/rego.12222. Acesso em 27 Jan. 2023.

BERNARDES, Flávio Couto. **Direito e Políticas Públicas.** Aulas ministradas ao longo do primeiro semestre de 2022 no Programa de Pós-graduação em Direito da Pontifícia Universidade Católica de Minas Gerais. Belo Horizonte: PUC Minas, 2022.

BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção de dados genéticos.** 2016. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica do Rio Grande do Sul, 2016. 178 fls.

BIONI, Bruno Ricardo; RIELLI, Mariana Marques. A construção multisetorial da LGPD: história e aprendizados. In.: BIONI, Bruno (Org.). **Proteção de dados, contexto, narrativas e elementos fundantes.** Livro Eletrônico. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 3ª edição. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo. **Regulação e proteção de dados pessoais: o princípio da *accountability*.** Rio de Janeiro: Forense, 2022.

BOFF, Salete Oro; FORTES, Vinícius Boges. A privacidade e a Proteção de Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. In.: **Sequência Estudos Jurídicos e Políticos.** Volume 35. n. 68, pp. 109-128. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109/26949. Acesso em 05 Jan. 2022.

BOTRUGNO, Carlo. Cybersecurity, privacy, and health data protection in the digital strategy of the European Union.

BRAITHWAITE, John. Responsive Regulation and Developing Economies. **World Development.** Vol. 34. N. 5. 2006. Pp. 884-898. Disponível em: 10.1016/j.worlddev.2005.04.021. Acesso em 05 Out. 2022.

BRAITHWAITE, John. Restorative justice and responsive regulation: the question of evidence. **School of Regulation and Global Governance (RegNet).** RegNet Working Papers. Nº. 51. 2016. QUT Library Collection.

BRAITHWAITE, John. **Regulatory Capitalism: how it works, ideas for making it work better.** Cheltenham: Edward Elgar, 2008.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 04 Set. 2021.

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)** (Redação dada pela Lei nº 13.853, de 2019). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 10 Out. 2021.

BRITANNICA ACADEMIC. s.v. "Judicial activism". In.: BRITANNICA ACADEMIC. **Encyclopedia Britannica.** Chicago: Encyclopedia Britannica Inc, 2019. Disponível em: https://academic-eb-com.eu1.proxy.openathens.net/levels/collegiate/article/judicial-activism/488008. Acesso em 20 Jun. 2023.

BROWN, A. J. **Michael Kirby: paradoxes and principles.** Salisbury: The Federation Press, 2011.

BRYCE, James Bryce. **The American commonwealth.** Indianapolis: Liberty Fund, 1995.

BUCCI, Maria Paula Dallari. MÉTODO E APLICAÇÕES DA ABORDAGEM DIREITO E POLÍTICAS PÚBLICAS (DPP). In: **Revista Estudos Institucionais**, v. 5, n. 3, p. 791-832, set./dez. 2019. Disponível em: https://estudosinstitucionais.com/REI/article/view/430/447. Acesso em 10 Jan. 2020.

BUCCI, Maria Paula Dallari. O conceito de política pública em direito. In: BUCCI, Maria Paula Dallari (Org.). **Políticas públicas: reflexões sobre o conceito jurídico.** São Paulo: Saraiva, 2006.

BUCCI, Maria Paula Dallari. Quadro de Referência de uma Política Pública: primeiras linhas de uma visão jurídico-institucional. **Direito do Estado.** Ano 2016. Número 122. Disponível em: http://www.direitodoestado.com.br/colunistas/maria-paula-dallari-bucci/quadro-de-referencia-de-uma-politica-publica-primeiras-linhas-de-uma-visao-juridico-institucional. Acesso em 04 Jul. 2022.

BURRELL, Jenna; FOURCADE, Marion. The Society of Algorithms. In.: **Annual Review of Sociology.** Volume 47. 2021. P. 213-237. Disponível em: https://www.annualreviews.org/doi/pdf/10.1146/annurev-soc-090820-020800. Acesso em 05 Jan. 2023.

CAMARGO, Gabriela Capobianco; SANTOS, Alessandro Santiago dos; ARIENTE, Eduardo Altomare; GOMES, Jefferson de Oliveira. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. **Estudos Avançados.** Vol. 34. Nº. 99. Maio-Agosto de 2020. Disponível em: https://doi.org/10.1590/s0103-4014.2020.3499.011. Acesso em 11 Nov. 2023.

CASSESE, Sabino. New paths for administrative law: A manifesto. In: **International Journal of Constitutional Law** (2012). Vol. 10, nº. 3, p. 603-613. Disponível em: https://academic.oup.com/icon/article/10/3/603/673508. Acesso em 20 Mar. 2020.

CASTELLS, Manuel. **A sociedade em rede.** Tradução de Roneide Venâncio Majer. Atualização para 6ª edição: Jussara Simões. São Paulo: Paz e Terra, 2013.

CASTELVECCHI, Davide. The black box of AI. In.: **Nature – International Weekly jornal of Science.** 2016. Volume 538. Issue 7623. P. 20-23. Disponível em: https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731. Acesso em 05 Jan. 2023.

CAVALCANTI, Mario Filipe. Cookies para quem? Entre o escambo digital e os direitos à privacidade e proteção de dados. **Revista Acadêmica da Faculdade de Direito do Recife.** Vol. 93. Nº. 2. 2021. Disponível em: https://periodicos.ufpe.br/revistas/ACADEMICA/article/view/249887. Acesso em 12 Nov. 2023.

CAVOUKIAN, Ann. *Privacy by Design* and the Promise of SmartData. In.: HARVEY, Inman; CAVOUKIAN, Ann; TOMKO, George; BORRETT, Don; KWAN, Hon; HATZINAKOS, Dimitrios (Eds.). **SmartData: Privacy Meets Evolutionary Robotics.** Nova York: Springer, 2013.

CAVOUKIAN, Ann. Global privacy and security, by design: turning the “privacy vs. security” paradigm on its head. **Health and Technology.** Vol. 7. Issue 4. 2017. Pp. 329-333. Disponível em: https://link.springer.com/article/10.1007/s12553-017-0207-1. Acesso em 10 Jun. 2023.

CENTRE FOR LEGAL INNOVATION. **Episode 1 – An introduction to legal design thinking and doing.** Disponível em: https://www.youtube.com/watch?v=6msY8IdIPUs. Acesso em 10 Ago. 2021.

CENTRE FOR LEGAL INNOVATION. College of Law. Resources. Disponível em: https://www.cli.collaw.com/resource-hub. Acesso em 27 Jun. 2023.

CHAUDHURI, Abhik; CAVOUKIAN, Ann. The proactive and preventive privacy (3P) framework for IoT privacy by design. **The EDP Audit, Control, and Security Newsletter (EDPACS).** Vol. 57. Nº. 1. Pp. 1-16. Disponível em: https://doi.org/10.1080/07366981.2017.1343548. Acesso em 10 Jun. 2023.

CLARK, Giovani. **Direito e Políticas Públicas.** Aulas ministradas ao longo do primeiro semestre de 2021 no Programa de Pós-graduação em Direito da Pontifícia Universidade Católica de Minas Gerais. Belo Horizonte: PUC Minas, 2021.

CLARK, Giovani; CORRÊA, Leonardo Alves; NASCIMENTO, Samuel Pontes do. O direito econômico, o pioneirismo de Washington Peluso Albino de Souza e o desafio equilibrista: a luta histórica de uma disciplina entre padecer e resistir. **Revista da Faculdade de Direito da UFMG.** N. 73, jul. / dez. 2018. Pp. 301-324. Disponível em: 10.12818/P.0304-2340.2018v73p301. Acesso em Mar. 2021.

CONSELHO DA EUROPA. **Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais.** Roma, 1950. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf. Acesso em 25 Jul. 2022.

COULDRY, Nick; MEJIAS, Ulises A. **The costs of connection: how data is colonizing human life and appropriating it for capitalism.** Stanford: Stanford University Press, 2019.

COULDRY, Nick; MEJIAS, Ulises A.. Data Colonialism: rethinking big data’s relation to the contemporary subject. **Television and new media.** 2018. Volume 20. N. 4. Disponível em: https://journals.sagepub.com/doi/full/10.1177/1527476418796632. Acesso em 10 Abr. 2023.

CUNHA, Juliana Falci Sousa Rocha. RASTREAMENTO DE CONTATOS DURANTE A PANDEMIA: : DESAFIOS TECNOLÓGICOS E JURÍDICOS. **J² — Jornal Jurídico**, [S. l.], v. 6, n. 1, p. 19–28, 2023. Disponível em: https://revistas.ponteditora.org/index.php/j2/article/view/575. Acesso em 15 Nov. 2023.

CUNHA, Anita Spies da. **O fortalecimento da dimensão objetiva do direito fundamental à proteção de dados como caminho para sua efetividade.** Porto Alegre, 2022. Dissertação (Mestrado em Direito). Universidade Federal do Rio Grande do Sul, 2022. 104 fls.

CUPIS, Adriano de. **Os direitos da personalidade.** Traduzido por Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008.

‘Current topics’ (1986) 60(6) **Australian Law Journal 315.** Pp. 317-319.

10.1080/1323238X.2022.2134289. 2022. Disponível em: https://doi.org/10.1080/1323238X.2022.2134289. Acesso em 17 Nov. 2022.

DEANGELO, Gregory; HUMPHREYS, Brad R.; REIMERS, Imke. Are public and private enforcement complements or substitutes? Evidence from high Frequency data. **Journal of Economic Behaviour & Organization.** Nº. 141. 2017. Pp. 151-163. Disponível em: https://doi.org/10.1016/j.jebo.2017.06.009. Acesso em 10 Jul. 2023.

DE LAMBOY, Christian K. (Org.). **Manual de Compliance.** São Paulo: Instituto ARC, 2017.

DE LIMA, Cíntia Rosa Pereira. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

DENNY, Danielle Mendes Thame; LEÃO, Gabriel Augusto dos Santos Nascimento. Publicidade lotérica: uma análise das promoções comerciais sob aspectos da responsabilidade social corporativa, direito do consumidor e proteção de dados pessoais. **Revista de Direito Brasileira.** Vol. 23. Nº. 9. 2020. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5125/0. Acesso em 11 Nov. 2023.

DEMETZOU, Katerina; ZANFIR-FORTUNA, Gabriela; VALE, Sebastião Barros. The thin red line: refocusing data protection law on ADM, a global perspective with lessons from case-law. **Computer Law & Security Review.** Volume 49. 2023. Disponível em: https://doi.org/10.1016/j.clsr.2023.105806. Acesso em 10 Out. 2023.

DE MORAES, Maria Celina Bodin. LGPD: um novo regime de responsabilização civil dito proativo. In: **Revista Eletrônica de Direito Civil**. V. 8, n.3 (2019). Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448. Acesso em 10 Nov. 2020.

DIMOPOULOS, Georgina. Re-thinking privacy in Australia in the wake of Dobbs v Jackson Women's Health Organization. **Australian Journal of Human Rights.** Vol. 28. N. 2-3. 2022. Pp. 425-434. Disponível em: https://www.tandfonline.com/doi/full/10.1080/1323238X.2022.2134289. Acesso em 10 Nov. 2022.

Doc & Film International. **Everything's under control.** BOOTE, Werner (diretor). 2015. Disponível em Kanopy Streaming. Acesso via acervo da QUT em 20 Dez. 2022.

DONDA, Daniel. **Guia prático de implementação da LGPD: tudo o que a sua empresa precisa saber para estar em conformidade.** São Paulo: Labrador, 2020.

DONEDA, Danilo; MENDES, Laura Schertel. Data protection in Brazil: new developments and current challenges. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (eds.). **Reloading data protection.** Londres: Springer, 2014. Pp. 3–20.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** 2ª edição. São Paulo: Thomson Reuters Brasil Revista dos Tribunais, 2020.

DOS SANTOS, Raquel Gitirana Torquato. **A Lei Geral de Proteção de Dados Brasileira: uma política pública regulatória.** 2020. Monografia de Especialização (Especialização em

Avaliação de Políticas Públicas). Instituto Serzedello Corrêa – Escola Superior do Tribunal de Contas da União, Brasília, 2020. 200 fl.

DUDIN, Mihail Nikilaevich; SMIRNOVA, Olga Olegovna; VYSOTSKAYA, Nataliya Vladimirovna; FROLOVA, Evgenia Evgenevna; VILKOVA, Nina Grigorevna. The Deming cycle (PDCA) concept as a tool for the transition to the innovative path of the continuous quality improvement in production processes of the agro-industrial sector. **European Research Studies**. Vol. *20*. Issue 2. Pp. 283-293. Disponível em: https://www.proquest.com/scholarly-journals/deming-cycle-pdca-concept-as-tool-transition/docview/1902638105/se-2. Acesso em 26 Jun. 2023.

DWYER, Tim; MARTIN, Fiona. Sharing News online: social media News analytics and their implications for media pluralism policies. **Digital Journalism.** 2017. Vol. 5, nº. 8, pp. 1080-1100. Disponível em: https://doi.org/10.1080/21670811.2017.1338527. Acesso em 10 Dez. 2022.

EC. **DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals concerning the processing of personal data and on the free movement of such data.** Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em 07 Nov. 2022.

EKEL, Petr. **Tópicos Avançados em Tomada de Decisão em Cenários Complexos.** Aulas ministradas ao longo do primeiro semestre de 2022 no Programa de Pós-graduação em Informática da Pontifícia Universidade Católica de Minas Gerais. Belo Horizonte: PUC Minas, 2022.

EUROPEAN COMMUNITY. **DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.** Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em 07 Nov. 2022.

FACHIN, Luiz Edson; PIANOVSKI RUZYK, Carlos Eduardo. A dignidade da pessoa humana no direito contemporâneo: uma contribuição à crítica da raiz dogmática do neopositivismo constitucionalista. **Revista Trimestral de Direito Civil.** Vol. 35, Rio de Janeiro, 2008, p. 108-109.

Federal Court Rules 2011 (Cth).

FERNEDA, Arie Scherreier; ZILIOTTO, Bruna Antunes; KLEIN, Vinícius. Geopricing e Geoblocking: a geodiscriminação com base na utilização de dados à luz da defesa do consumidor. **Revista Direito em Debate.** 2023. Vol. 32. Nº. 59. Disponível em: Geopricing e Geoblocking: A geodiscriminação com base na utilização de dados à luz da defesa do consumidor e da concorrência | Revista Direito em Debate (unijui.edu.br). Acesso em 10 Nov. 2023.

FINKELSEN, Ray; HAMER, David. **LexisNexis Concise Australian Legal Dictionary**. Sydney: LexisNexis Butterworths, 2020. Disponível em:

http://ebookcentral.proquest.com/lib/qut/detail.action?docID=6473552. Acesso em 17 Nov. 2022.

FLORIDI, Luciano. The construction of personal identities online. **Minds & Machines.** 2011. Volume 21. Pp. 477-479. Disponível em: https://philarchive.org/rec/FLOTCO. Acesso em 23 Jul. 2023.

FLORIDI, Luciano. The fight for digital Sovereignty: what it is, and why it mattes, especially for the EU. **Philosophy & Technology.** 2020. Volume 33. Pp. 369-378. Disponível em: https://doi.org/10.1007/s13347-020-00423-6. Acesso em 23 Jul. 2023.

FRANK, Felipe. **Autonomia da vontade, autonomia privada e negócio jurídico.** Morrisville: Lulu Press, 2019.

Freedom of Information Act 1982 (Cth).

GARCIA, Lara Rocha; AGUILERA-FERNANDES, Edson; PEREIRA-BARRETO, Marcos Ribeiro. **Lei Geral de Proteção de Dados (LGPD): guia de implantação.** São Paulo: Editora Blucher, 2020.

GEERTZ, Clifford. Uma descrição densa: por uma Teoria Interpretativa da Cultura. Pp. 3 – 21. In: GEERTZ, Clifford. **A interpretação das culturas.** 1º ed. Rio de Janeiro: LTC, 2008.

GIERKE, Otto von. **The social role of private law (1889).** Lecture given by Otto von Gierke in 1889. Traduzido para o inglês por Ewan McGaughey, precedido por ensaio introdutório, "A Social Law beyond Public v Private", escrito pelo tradutor. King's College London Law School Research Paper, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2861875. Acesso em 06 Jan. 2023.

GLITZ, Gabriela Pandolfo Coelho. **Proteção de dados pessoais: uma análise sobre a aplicabilidade do legítimo interesse.** 2019. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica do Rio Grande do Sul, 2019. 111 fls.

GONÇALVES, Victor Hugo Pereira. **Proteção de dados pessoais: direitos do titular.** Rio de Janeiro: Forense, 2022.

GOMES, Orlando. Direitos da Personalidade. In.: **Revista de Informação Legislativa.** Volume 3, n. 11. Set. 1966. Pp. 39-48. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/180717/000348967.pdf?sequence=1&isAllowed=y. Acesso em 05 Jan. 2023.

GRABOSKY, Peter. Beyond Responsive Regulation: the expanding role of non-state actors in the regulatory process. **Regulation and Governance.** Volume 7. Nº. 1. 2013. Pp. 114-123. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1748-5991.2012.01147.x Acesso em 11 Dez. 2023.

GRABOSKY, Peter; BRAITHWAITE, John. **Of manners gentle: enforcement strategies of Australian business regulatory agencies.** Melbourne: Oxford University Press, 1988.

GREENLEAF, Graham. Five Years of the APEC Privacy Framework: failure or promise? **Computer Law and Security Review.** Vol. 25. 2009. Pp. 26-48. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364908001714. Acesso em 10 Nov. 2022.

GROSSI, Bernardo Menicucci. **O desafio da regulação dos dados pessoais: entre a autonomia e a heteronomia.** 198 p. Belo Horizonte, 2022. Tese (Doutorado em Direito). – Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito. 2022. 198 fls.

GUENTHER, Melissa. Security/ Privacy Compliance: Culture Change. **EDPACS.** Volume 31. N. 12. 2004. Pp. 19-24. Disponível em: https://www.proquest.com/docview/234907205?accountid=13380&forcedol=true&pq-origsite=primo. Acesso em 10 Nov. 2022.

GULART, Caroline de Melo Lima. **A proteção de dados pessoais non uso de tecnologia na relação de emprego: efeitos do compliance trabalhista nas negociações coletivas.** 2020. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica do Rio Grande do Sul, 2020. 151 fls.

GUNASEKARA, Gehan. Enforcement design for data privacy: a comparative study. **Singapore Journal of Legal Studies.** nº. Mar. 2021. Pp. 19-38. Disponível em: https://www.proquest.com/docview/2529336498?pq-origsite=primo&accountid=13380. Acesso em 02 Nov. 2022.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca. **(Re)pensando a Pesquisa Jurídica: teoria e prática.** 3ª edição. Belo Horizonte: Del Rey, 2010.

GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; LEENES, Ronald (Eds.). **Computers, privacy and data protection: an elemento of choice.** Londres: Springer, 2011.

GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul. **Reloading data protection: multidisciplinar insights and contemporary challenges.** Londres: Springer, 2014.

HEARD, John. Profile Four: Michael Kirby A C CMG. In: SYKES, Helen; FRYDENBERG, Erica.. **Australian Leadership Reader: Six Leading Australians and Their Stories.** Australian Academic Press, 2006. Pp. 55-70.

HINCAPÍE, Gabriel Méndez; SANIN-RESTREPO, Ricardo. La Constituición Encriptada: nuevas formas de emancipación del poder global. In: *Revista de Derechos Humanos y Estudios Sociales.* Ano IV. Nº. 8. Julho – Dezembro de 2012. P. 97- 120. Disponível em: http://www.derecho.uaslp.mx/Documents/Revista%20REDHES/N%C3%BAmero%208/Redhes8-05.pdf. Acesso em 10 Out. 2021.

HINDS, Joanne; JOINSON, Adam. Human and computer personality prediction from digital footprints. In.: **APS – Association for Psychological Science.** 2019. Vol. 28. N. 2. P. 204-211. Disponível em: https://journals.sagepub.com/doi/full/10.1177/0963721419827849. Acesso em 06 Jun. 2022.

HOLM, Elizabeth A.. Indefense of the black box: black boxes algorithms can be useful in Science and engineering. In.: **Science.** 2019.Volume 364. Nº. 6435. P. 26-27. Disponível em: https://www.science.org/doi/10.1126/science.aax0162. Acesso em 05 Jan. 2023.

IDP / CEDIS; JUSBRASIL. **LGPD nos tribunais.** Edições de 2021 e 2022. Disponível em: https://painel.jusbrasil.com.br/. Acesso em 05 Nov. 2022.

IRAMINA, Aline. RGPD v. LGPD: adoção estratégica da abordagem responsiva na elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, estado e Telecomunicações.** Brasília. 2020. Vol. 12. Nº. 2. Pp. 91-117. Disponível em: http://doi.org/10.26512/lstr.v12i2.34692. Acesso em 05 Nov. 2022.

JOHNS, Leslie. The design of enforcement: collective action and the enforcement of international law. **Journal of Theoretical Politics.** 2019. Vol. 31. Issue 4. Pp. 543-567. Disponível em: 10.1177/0951629819875514journals.sagepub.com/home/jtp. Acesso em 01 Jun. 2023.

JORGE, Carlos Francisco Bittencourt; OLIVEIRA, Bruno Bastos de; MACHADO, João Guilherme de Camargo Ferraz; LIMA, Marcelo Souto de; OTRE, Maria Alice Campagnoli. Proteção de dados pessoais e COVID-19: entre a inteligência epidemiológica no controle da pandemia e a vigilância digital. **Liinc em Revista.** Vol. 26. Nº. 2. 2020. Disponível em: https://revista.ibict.br/liinc/article/view/5251. Acesso em 11 Nov. 2023.

KAHNEMAN, Daniel. **Rápido e devagar: duas formas de pensar.** Tradução de Cássio de Arantes Leite. São Paulo: Objetiva, 2012.

KIRBY, Michael. Privacy in the courts. **University of New South Wales Law Journal Forum.** Vol. 24. Nº. 1. 2001. Pp. 247-255. Disponível em: https://search.informit.org/doi/abs/10.3316/agis_archive.20014129. Acesso em 30 Nov. 2022.

KIRBY, Michael. The ALRC a winning formula. **Reform (Sydney, N.S.W.).** N. 82. 2003. Pp. 58-63. Disponível em: https://search.informit.org/doi/10.3316/cinch.257498. Acesso em 30 Nov. 2022.

KITCHIN, Rob; MCARDLE, Gavin. What makes big data, big data? Exploring the ontological characteristics of 26 datasets. In.: **Big data and Society.** Jan.-Jun. Volume 3. N 1. 2016. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/2053951716631130. Acesso em 05 Mar. 2020.

KLEIN, Naomi. **Rise of disaster capitalismo.** San Francisco: Kanopy Streaming, 2015.

KLEIN, Naomi; SMITH, Neil. The Shock Doctrine: a discussion. In.: **Environmental and Planning D: Society and Space.** 2008. Volume 26. Pp. 582-595. Disponível em: https://journals.sagepub.com/doi/epdf/10.1068/d2604ks. Acesso em 12 Jan. 2023.

LAYDER, Derek. **Investigative research: theory and practice.** Londres: SAGE Publication Ltd., 2019.

LIMA JÚNIOR, Edivaldo da Costa; SILVA, José Rilton Soares da; CÂMARA, Maria Amália Arruda; RODRIGUES, Matheus Barbosa. É possível a desqualificação do agente de tratamento? Uma análise à luz da Lei Geral de Proteção de Dados. **Revista Ratio Juris.** Vol. 17. N. 35. 2022. Pp. 651-672. Disponível em: https://publicaciones.unaula.edu.co/index.php/ratiojuris/article/view/1423/1711. Acesso em 10 Nov. 2023.

LUDWIG, Marcos de Campos. O direito ao livre desenvolvimento da personalidade na Alemanha e possibilidades de sua aplicação no Direito privado brasileiro. **Revista da Faculdade de Direito da UFRGS.** Volume 19. Março/2001. Pp. 237-263.

LUZ, Igor Henrique dos Santos; BRITO, Jaime Domingues. Positivismo Jurídico e os Direitos da Personalidade Natural. In.: **Revista Brasileira de Direito.** Passo Fundo. Volume 14, n. 2. Maio-Agosto / 2018. Pp. 36-254. Disponível em: https://doi.org/10.18256/2238-0604.2018.v14i2.1812. Acesso em 20 Dez. 2021.

LYON, David. **The culture of surveillance: watching as a way of life.** Cambridge: Polity Books, 2018.

MACHADO, Fernando Inglez de Souza. **Privacidade e proteção de dados pessoais na sociedade da informação: *profiling* e risco de discriminação.** 2018. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica do Rio Grande do Sul, 2018. Disponível em https://tede2.pucrs.br/tede2/handle/tede/8002. Acesso em 12 Nov. 2023.

MACHADO, Diego Carvalho; MENDES, Laura Schertel. Tecnologias de perfilamento e dados agregados de geolocalização no combate à COVID-19 no Brasil: uma análise dos riscos individuais e coletivos à luz da LGPD. **Direitos fundamentais e justiça.** Belo Horizonte. Vol. 14. Número 1. Nov. 2020. Pp. 105-148. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1020. Acesso em 05 Jul. 2023.

MAIMONE, Flávio Henrique Caetano de Paula. **Responsabilidade Civil na LGPD: efetividade na proteção de dados pessoais.** Indaiatuba: Editora Foco, 2022.

MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada.** 4ª edição. São Paulo: Thomson Reuters Brasil, 2022.

MANN, Monique. Privacy in Australia: Brief to UN Special Rapporteur on Right to Privacy. **Australian Privacy Foundation.** 2018. Disponível em: https://privacy.org.au/2018/08/15/australian-privacy-foundation-provides-background-brief-on-all-the-privacy-omnishambles-to-un-special-rapporteur-on-privacy/. Acesso em 25 Nov. 2022.

MARELLI, Massimo. The law and practice of international organizations' interactions with personal data protection domestic regulation: at the crossroads between the international and domestic legal orders. **Computer Law & Security Review.** Volume 50. 2023. Disponível em: https://doi.org/10.1016/j.clsr.2023.105849. Acesso em 18 Out. 2023.

MARMELSTEIN, George. **Curso de Direitos Fundamentais.** 8ª ed. São Paulo: Atlas, 2019.

MARQUES, Meire Aparecida Furbino. **CASTELOS ALGORÍTIMICOS DE PODER: enclausuramento tecnofeudal dos Direitos Humanos / fundamentais?** Belo Horizonte, 2022. Tese (Doutorado em Direito). Pontifícia Universidade Católica de Minas Gerais. 354 fls.

MARTINS, Helena; FERREIRA, Katiele Gomes; CASTRO, Luciana Gouvêa Hage de; MACEDO JÚNIOR, Daniel Paiva de; LIMA, Elizandro dos Anjos Araújo. Tratamento de dados pessoais em aplicativos públicos relacionados ao coronavírus no Ceará. **Liinc em Revista.** V. 16. Nº. 2. 2020. Disponível em: https://revista.ibict.br/liinc/article/view/5387. Acesso em 11 Nov. 2023.

MARTINS, Pedro Bastos Lobo. ***Profiling* na Lei Geral de Proteção de Dados: o livre desenvolvimento da personalidade em face da governamentabilidade algorítmica.** Indaiatuba: Editora Foco, 2022.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR (Coord.). **Comentários à Lei Geral de Proteção de Dados Pessoais: Lei 13.709/2018.** Indaiatuba: Editora Foco, 2022.

MASIERO, Silvia. Explaning trust in large biometric infrastructures: a critical realist case study of India's Aadhaar Project. **The Electronic journal of information systems in developing countries.** 2018. Volume 84. N. 6. Disponível em: https://doi.org/10.1002/isd2.12053. Acesso em 19 Abr. 2023.

MATTIA, Fábio Maria de. Direitos da Personalidade: aspectos gerais. In.: **Revista de Informação Legislativa.** Volume 14. n . 56. Out./ Dez. 1977. Pp. 247-266. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/181045. Acesso em 05 Jan. 2023.

MATZ, S.C.; KOSINSKI, M.; NNAVE, G.; STILLWELL, D. J.. Psychological targeting as an effective approach to digital mass persuasion. In: **Proceedings of the National Academy of Sciences of the United States of America.** Disponível em: https://www.pnas.org/doi/10.1073/pnas.1710966114. Acesso em 05 Jun. 2022.

MBEMBE, Achile. **Bodies and Borders.** Youtube, 2019. Disponível em: https://www.youtube.com/watch?v=JqreV_1FqtU. Acesso em 10 Jan. 2021.

MCEVOY, Sebastian. 7. Descriptive and purposive categories of comparative law. In.: MONATERI, Pier Giuseppe (Ed.). **Methods of Comparative Law.** Cheltenham: Edward Elgar Publishing, 2012. Pp. 144-162.

MCGREGOR, Joan. Population Genomics and Research Ethics with Socially Identifiable Groups. **Journal of Law, Medicine & Ethics.** 2007. Volume 35. N. 3. Pp. 356-370.

MCGREGOR, Joan. Racial, ethnic, and tribal classifications in biomedical research with biological and group harm. **The American Journal of Bioethics.** 2010. Volume 10. Nº. 9. Pp. 23-24. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/15265161.2010.492888?needAccess=true. Acesso em 27 Jan. 2023.

M. D. K.. International legal notes: international protection of privacy and controls over transnational data flow. **Australian Law Journal.** 1981. Vol. 55. Nº. 3. Pp. 163-166. Acervo QUT.

MELLO, Marcos Bernardes de. **Teoria do Fato Jurídico: plano da existência.** 22ªed. São Paulo: Saraiva Educação, 2019.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista Direito Público**, Porto Alegre, Volume 16, n. 90, 2019, 39-64, Nov-Dez 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em 05 Out. 2021.

MENDOZA, Melanie Claire Fonseca; BRANDÃO, Luiz Mathias Rocha. Do direito à privacidade à proteção de dados: das teorias de suporte e a exigência da contextualização. **Revista de Direito, Governança e Novas Tecnologias.** Vol. 2. Nº. 1. 2016. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/830. Acesso em 12 Nov. 2023.

Michael Kirby: Don't Forget the Justice Bit. Film Art Media, 2010. Acesso em 30 Nov. 2022.

MICHAELS, Ralf. Chapter 13. The functional method of comparative law. In.: REIMANN, Mathias; ZIMMERMANN, Reinhard (Eds.). **The Oxford Handbook of Comparative Law.** Oxford: Oxford, 2019. Pp. 345-389.

MITTELSTADT, Brent. From individual to group privacy in big data analytics. **Philosophy & technology.** Vol. 30. Nº. 4. 2017. Pp. 475-494. Disponível em: https://doi.org/10.1007/s13347-017-0253-7. Acesso em 06 Jul. 2023.

MOREHAM, Na. Compensating for Loss of Dignity and Autonomy. In: VARUHAS, Jason N E Varuhas; MOREHAM N A(eds), **Remedies for Breach of Privacy.** Oxford: Hart Publishing, 2018. Pp. 125-142.

MOSES, Lyria Bennett. Agent of Change. **Griffith Law Review.** Volume 20. Nº. 4. 201. Pp. 763-794. Disponível em: https://doi.org/10.1080/10383441.2011.10854720. Acesso em 31 Mar. 2023.

MOUFFE, Chantal. **The democratic paradox.** Nova York: Verso, 2000.

MUÑOZ, Ricardo Alberto. A proibição da automatização decisória baseada no perfilhamento digital. **Novos Estudos Jurídicos.** 2022. Volume 27. N. 1. Pp. 206-223. Disponível em: www.univali.br/periodicos. Acesso em 10 Abr. 2023.

NEGRI, Sérgio Marcos Carvalho de Ávila; BATISTA, Nathan Paschoalini Ribeiro. Do rastreamento de contato à vigilância: um estudo sobre o TraceTogether App. **Liinc em Revista.** Vol. 17. Nº. 1. 2021. Disponível em: https://revista.ibict.br/liinc/article/view/5710. Acesso em 11 Nov. 2023.

NEVES, Marcelo. **A constitucionalização simbólica.** 3ª edição. São Paulo: Editora WMF Martins Fontes, 2011.

O dilema das redes (*The social dilemma)*. Direção: Jeff Orlowski. Roteiro: Davis Coombe; Vickie Curtis; Jeff Orlowski. EUA: Netflix, 2020.

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy.** 1ª edição. Nova York: Crown Publichers, 2016.

OECD. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980.** Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em 10 Fev. 2020.

Office of the Australian Information Commissioner (Cth), "Australian Privacy Principles Guidelines**"** (Web Page, 04 November 2022) https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines

OKIDEGBE, Ngozi. Of Afrofuturism, of algorithms. **Critical Analysis of Law.** 2022. Volume 9. N. 1. Pp. 35-48. Disponível em https://cal.library.utoronto.ca/index.php/cal/article/view/38265#:~:text=It%20imagines%20how%20applying%20an,for%20which%20they%20are%20developed.. Acesso em 01 Mar. 2023.

PALQEE. **Relatório Privacy Culture 2021.** Disponível em: https://palqee.com/resources/privacy-culture-index-brasil-2021/. Acesso em 01 Jan. 2023.

PALQEE. **Relatório Privacy Culture 2022.** Disponivel em https://palqee.com/resources/privacy-culture-index-brasil-2022/. Acesso em 01 Jan. 2023.

PANITZ, João Vicente Pandolfo. **Proteção de dados pessoais: a intimidade como núcleo do direito fundamental à privacidade e a garantia constitucional da dignidade.** 2007. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica do Rio Grande do Sul, 2007. Disponível em: ttps://repositorio.pucrs.br/dspace/bitstream/10923/2344/1/000395907-Texto%2bParcial-0.pdf. Acesso em 18 Nov. 2023.

PARISER, Eli. **O filtro invisível: o que a internet está escondendo de você.** Tradução de Diego Alfaro. Rio de Janeiro: Zahar, 2012.

PASQUALE, Frank. **Black Box Society: the secret algorithms that control Money and information.** Londres: Harvard University Press, 2015. Pp. 1-18; 213-218.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei nº. 13.709/2018 (LGPD).** 4ª edição. São Paulo: Saraiva Jur., 2023.

POUNDER, Chris. **Why the APEC Privacy Framework is unlikely to protect privacy. 2007.** Disponível em: http://cyberlawcentre.austlii.edu.au/ipp/apec_privacy_framework/0710_pounder.pdf. Acesso em 12 Dez. 2022.

Privacidade Hackeada (*The great hack*). Direção: Karim Amer; Jehane Noujaim. Produção: Karim Amer; Jehane Noujaim; Pedro Kos; Geralyn Dreyfous; Judy Korin. Roteiro: Karim Amer; Erin Bernett; Pedro Kos. EUA: Netflix, 2019.

Privacy Act 1988 (Cth).

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth).

Productivity Commission Act 1998 (Cth).

QUINTAIS, João Pedro; DE GREGORIO, Giovanni; MAGALHÃES, João C. How platforms govern users' copyright-protected content: exploring the power of private ordering and its implications. **Computer Law & Security Review.** Vol. 48. 2023. Disponível em: https://doi.org/10.1016/j.clsr.2023.105792. Acesso em 15 Out. 2023.

QUEIROZ, Renata Capriolli Zocatelli. **Encarregado de Proteção de Dados Pessoais – DPO – Regulamentação e Responsabilidade Civil.** São Paulo: Quartier Latin, 2022.

RAMOS, Lara Castro Padilha; GOMES, Ana Virgínia Moreira. Lei Geral de Proteção de Dados Pessoais e seus reflexos nas relações de trabalho. **Scientia Juris.** V. 23. N. 2. 2019. Disponível em: https://doi.org/10.5433/2178-8189.2019v23n2p127. Acesso em 12 Nov. 2023.

RANERIP, Agneta; HENRIKSEN, Helle Zinner. Digital discretion: unpacking human and technological agency in automated decision making in Sweden's Social Services. **Social Science Computer Review.** 2020. Volume 40. Issue 2. Pp. 445-461. Disponível em: https://journals.sagepub.com/doi/full/10.1177/0894439320980434. Acesso em 15 Fev. 2023.

REISACH, Ulrike. The responsability of social media in times of societal and political manipulation. **European Journal of Operational Research.** 2021. Vol. 291. Pp. 906-917. Disponível em: 10.1016/j.ejor.2020.09.020. Acesso em 10 Dez. 2022.

REVIGLIO, Urbano; AGOSTI, Claudio. Thinking outside the Black-Box: the case for "Algorithmic Sovereignty" in Social Media. **Social Media + Society.** Abr.-Jun. 2020. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2056305120915613. Acesso em 05 Jun. 2022.

RICHARDSON, Megan; BOSUA, Rachelle; CLARCK, Karin; WEBB, Jeb; AHMAD, Atif; MAYNARD, Sean. Towards responsive regulation of the Internet of Things: Australian perspectives. **Internet policy review: journal on internet regulation.** Volume 6. Nº. 1. 2017. Disponível em: https://policyreview.info/articles/analysis/towards-responsive-regulation-internet-things-australian-perspectives Acesso em 10 Dez. 2022.

RIDDER, Denise de; KROESE, Floor; GESTEL, Laurens van. Nudgeability: mapping conditions of susceptibility to nudge influence. In.: **APS – Association for Psychological Science.** Vol. 17 (2). P. 346-359. Disponível em: https://journals.sagepub.com/doi/full/10.1177/1745691621995183. Acesso em 05 Jun. 2022.

RIEMENSCHNEIDER, Patrícia Strauss; MUCELIN, Guilherme Balczarek. Internet das Coisas, Decisões Automatizadas e o Direito à Explicação. **Revista da Faculdade de Direito da Universidade Federal de Uberlândia.** V. 49. N. 1. 2021. Disponível em: Internet das Coisas, Decisões Automatizadas e o Direito à Explicação | Revista da Faculdade de Direito da Universidade Federal de Uberlândia (ufu.br). Acesso em 12 Nov. 2023.

RIMMER, Matthew. **Michael Kirby's challenge: intellectual property, HIV/AIDS, and human rights.** Medium, 2014.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Bernardo Salgado. As três tipologias do desenvolvimento-dependente na América Latina: contribuições para um debate contemporâneo. In.: **REBELA – Revista Brasileira de Estudos Latino-Americanos.** V. 10. Nº. 2. Mai. / Ago. 2020. Disponível em: https://ojs.sites.ufsc.br/index.php/rebela/article/view/4272. Acesso em 02 Jan. 2023.

RODRIGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados pessoais: as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação.** 2010. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica do Rio Grande do Sul, 2010. 153 fls.

SAAVEDRA, Giovani; MENEZES, Daniel Negao. Proteção de dados na América Latina e os desafios da COVID-19. **Revista do Programa de Pós-Graduação em Ciências Jurídicas da Universidade Federal da Paraíba.** Vol. 19. Nº. 42. 2020. Disponível em: https://periodicos.ufpb.br/index.php/primafacie/article/view/54590. Acesso em 11 Nov. 2023.

SALES, Fernando Augusto de Vita Borges de. **Manual da LGPD.** São Paulo: Editora Mizuno, 2020.

SAMPAIO, José Adércio Leite. **Direito à Intimidade e à Vida Privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SAMPAIO, José Adércio Leite. **Direitos Fundamentais.** 2ª edição. Belo Horizonte: Del Rey, 2010.

SANIN-RESTREPO, Ricardo. **Decolonizing Democracy: power in a solid state**. Nova York: Library of Congress, 2016.

SANIN-RESTREPO, Ricardo. The case against Agamben's impotence. In: **Critical Legal Thinking**. Disponível em: https://criticallegalthinking.com/2019/09/30/the-case-against-agambens-impotence/. Acesso em 10 Out. 2021.

SANIN-RESTREPO, Ricardo; ARAUJO, Marinella Machado. A Teoria da Encriptação do Poder: itinerário de uma ideia. In.: **Revista Mineira de Direito**. V. 23. N. 45. 2020. p. 1-17. Disponível em: https://periodicos.pucminas.br/index.php/Direito/issue/view/1192. Acesso em 20 Ago. 2020.

SANTOS, Rafael Menguer Bykowski dos. Reflexión sobre la protección de datos virtuales por parte del Estado brasileño a través de las modificaciones generadas por COVID-19. **Revista Justicia & Derecho de Universidad Autónoma de Chile.** Vol. 4. Nº. 2. 2021. Disponível em: https://revistas.uautonoma.cl/index.php/rjyd/article/view/1352. Acesso em 11 Nov. 2023.

SANTOS, Laura Mello dos. Privacidad e protección de dados em el contexto de fusiones y adquisiociones transfronterizas: la (possible) función cooperativa del derecho de la competência. **Revista de la Secretaría del Tribunal Permanente de Revisión.** Vol. 10. N. 19. 2022. Disponível em: https://revistastpr.com/index.php/rstpr/article/view/489. Acesso em 10 Nov. 2023

SANTOS, Washington dos. **Dicionário jurídico brasileiro.** Belo Horizonte: Del Rey, 2001.

SEPULVEDA, Antonio; BOLONHA, Carlos; DE LAZARI, Igor. Judicial Defence to Agencies' Decisions in Brazil and the United States. **The regulatory review.** 2019. Disponível em https://www.theregreview.org/2019/07/24/sepulveda-bolonha-delazari-judicial-deference-agencies-decisions-brazil-united-states/. Acesso em 20 Jun. 2023.

SIMÕES, José Augusto. Proteção de Dados e o novo regulamento geral da União Europeia. **Revista portuguesa de medicina geral e familiar.** Vol. 34. N. 5. 2018. Pp. 266-267. Disponível em: https://scielo.pt/scielo.php?script=sci_issuetoc&pid=2182-517320180005&lng=pt&nrm=iso. Acesso em 10 Nov. 2023.

SLAUGHTER, Anne-Marie. **A new world order.** Princeton: Princeton University Press, 2004.

SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva.** São Paulo: Thomson Reuters Revista dos Tribunais, 2020.

SRNICEK, Nick. **Platform Capitalism.** Cambridge: Polity Press, 2017.

STARK, Luke. Algorithmic psychometrics and the scalable subject. **Social Studies of Science.** Volume 48. Issue 2. Disponível em: https://journals.sagepub.com/doi/10.1177/0306312718772094. Acesso em 05 Jun. 2022.

TAYLOR, Mark J. Personal Information and Group Data under the Privacy Act 1988 (Cth). **Australian Law Journal**. V. 94. Nº. 10. 2020. Pp.731-742.

TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis: qualificação, tratamento e boas práticas.** Indaiatuba: Editora Foco, 2022.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Revista dos Tribunais, 2020.

The century of the self. Direção: Adam Curtis. Produção: Adam Curtis, Lucy Kelsall e Stephen Lambert. Reino Unido: BBC, 2002.

TRANTER, Kieran. Citation Practices of the Australian Law Reform Commission in Final Reports 1992-2012. **University of New South Wales Law Journal.** Vol. 38. Nº. 1. 2015. Pp. 323-366. Disponível em: https://search.informit.org/doi/abs/10.3316/agis_archive.20151465. Acesso em 20 Nov. 2022.

TRINDADE, Augusto Cançado. **Desafios e conquistas do Direito Internacional dos Direitos Humanos no início do Século XXI.** Registro de Conferências ministradas pelo autor no *XXXIII*

Curso de Direito Internacional Organizado pela Comissão Jurídica Interamericana da OEA, no Rio de Janeiro, em 18 e 21-22 de agosto de 2006. Disponível em: https://www.oas.org/dil/esp/407-490%20cancado%20trindade%20oea%20cji%20%20.def.pdf. Acesso em 25 Jul. 2022.

TRINDADE, Augusto Cançado. **Os tribunais internacionais contemporâneos.** Brasília: FUNAG, 2013.

UFMG Talks. **Inteligência Artificial.** Palestra do Prof. Nívio Ziviani em 26 de agosto de 2019. Belo Horizonte: TV UFMG. Youtube, 2019.

UNIÃO EUROPEIA. **Charter of Fundamental Rights of the European Union. 2000/ C.** Disponível em: https://www.europarl.europa.eu/charter/pdf/text_en.pdf. Acesso em 04 Set. 2021.

VALADARES, Heloisa de Carvalho Feitosa. Proteção de dados e startups. In.: PIMENTA, Eduardo Goulart; NOGUEIRA, Fernanda Araújo Couto e Melo; FONSECA, Maurício Leopoldino da (Orgs.). **Legal talks – startups à luz do direito brasileiro.** Belo Horizonte: Editora Expert, 2020. Pp. 115-150.

VALADARES, Heloisa de Carvalho Feitosa. Proteção de dados como direito humano: unicidade na fundamentalidade e contribuições para a convergência regulatória. **Anais do VII Congresso Internacional de Direitos Humanos de Coimbra.** 2022 Disponível em: https://trabalhoscidhcoimbra.com/ojs/index.php/anaiscidhcoimbra/article/view/1889. Acesso em 01 Jun. 2023.

VALADARES, Heloisa de Carvalho Feitosa. Privacidade, proteção de dados e autodeterminação informativa: entre a visão patrimonial e de direito fundamental. **Anais do III Seminário Internacional de Direitos Humanos e Sociedade e V Jornada de Produção Científica em Direitos Fundamentais e Estado.** 2021. Disponível em: https://periodicos.unesc.net/ojs/index.php/AnaisDirH. Acesso em 25 de Jul. 2023.

VALADARES, Heloisa de Carvalho Feitosa. Metaverso e o sequestro da vontade livre e discernida. In.: VIDIGAL, Viviane; KROST, Oscar (Orgs.). **Mais direito, tecnologia e trabalho.** Volume II. Leme: Mizuno, 2022. Pp. 294-308.

VÉLIZ, Carissa. **Privacidade é poder: porque e como você deveria retomar o controle de seus dados.** Tradução: Samuel Oliveira. São Paulo: Editora Contracorrente, 2021.

WALDMAN, Ari Ezra. Gender Data in the Automated Administrative State. **Columbia Law Review.** 2019. Volume 124. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4358437. Acesso em 10 Abr. 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review,** Vol. 4, nº. 5, Dec. 1890, pp. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 26 Jun. 2022.

WESTIN, A.F.. Social and Political Dimensions of Privacy. **Journal of Social Issues,** V 59, Issue 2: 2003 pp 431-453. https://doi.org/10.1111/1540-4560.00072. Disponível em:

https://spssi.onlinelibrary.wiley.com/doi/epdf/10.1111/1540-4560.00072. Acesso em 29 Nov. 2022.

Westlaw, Current Topics (1986) Volume 60, 315 Australian Law Journal 317, 319.

WILLIAMSON, Ben. The Shock Doctrine by Naomi Klein: capitalismo, calamity and technology in the American political imaginarium. **Geography.** Volume 94. Issue 2. Pp. 108-114. Disponível em: https://doi.org/10.1080/00167487.2009.12094261 . Acesso em 12 Jan. 2023.

WIMMER, Miriam; CARVALHO, Lucas Borges de. A aplicação da Lei Geral de Proteção de Dados é suficiente para gerar segurança e confiança na sociedade? In: OLIVEIRA, Carlos Alberto Arruda de; MENEZES, Heloísa Regina Guimarães de (Eds.). **Digital: o desafio da confiança e da segurança jurídica na economia digital.** Nova Lima: Fundação Dom Cabral, 2021. Pp. 33-38.

WINDHOLZ, Eric. Federalism in Australia: a concept in search of understanding. **The Journal of Contemporary Issues in Business and Government.** Volume 17. Nº. 2. 2011. Pp. 1-18. Disponível em: Federalism in Australia: A Concept in Search of Understanding by Eric Windholz :: SSRN. Acesso em 17 Nov. 2022.

WINDHOLZ, Eric. **Governing through regulation: public policy, regulation and the law.** New York: Routledge, 2018.

WITZLEB, Normann. Another Push for an Australian Privacy Tort: Context, Evaluation and Prospects. **Australian Law Journal 765.** Volume 94. Nº. 10. 2020. Disponível em: https://www.researchgate.net/publication/344488886_Another_Push_for_an_Australian_Privacy_Tort_Context_Evaluation_and_Prospects. Acesso em 10 Nov. 2022.

WITZLEB, Normann. Determinations under the Privacy Act 1988 (Cth) as a Privacy Remedy. In: VARUHAS, Jason N E; MOREHAM, N A *(eds.).* **Remedies for Breach of Privacy**. Oxford: Hart Publishing, 2018. Pp. 377- 408.

YANOFSKY, Noson S.. Towards the definition of an algorithm. **Journal of Logic and Computation**. Volume 21. Issue 2. Abril, 2011. P. 253-286. Disponível em: https://academic.oup.com/logcom/article/21/2/253/941365?login=true. Acesso em 10 Nov. 2022.

ZAROUALI, Brahim; DOBBER, Tom; PAUW, Guy de; VREESE, Claes de. Using a personality-profiling algorithm to investigate political microtargeting: assessing the persuasion effects of personality-tailored ads on social media. **Communication Research.** Volume 49. Issue 8. Disponível em: https://journals.sagepub.com/doi/10.1177/0093650220961965. Acesso em 05 Jun. 2022.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power.** Nova York: Public Affairs, 2019.