UNIVERSIDADE FEDERAL DE SANTA MARIA – UFSM
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS – CCSH
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
MESTRADO EM DIREITO

Paulo Rodrigo de Miranda

DIREITO A INFERÊNCIAS RAZOÁVEIS COMO SUBSTRATO NORMATIVO NA CONSOLIDAÇÃO DE MECANISMOS DE GOVERNANÇA ALGORÍTMICA NOS SISTEMAS AUTOMATIZADOS DE DECISÃO

Santa Maria, RS
2022

Paulo Rodrigo de Miranda

DIREITO A INFERÊNCIAS RAZOÁVEIS COMO SUBSTRATO NORMATIVO NA CONSOLIDAÇÃO DE MECANISMOS DE GOVERNANÇA ALGORÍTMICA NOS SISTEMAS AUTOMATIZADOS DE DECISÃO

Dissertação apresentada ao Programa de Pós-Graduação em Direito, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Mestre em Direito.**

Orientadora: Profa. Dra. Valéria Ribas do Nascimento

Santa Maria, RS
2022

Miranda, Paulo Rodrigo de
DIREITO A INFERÊNCIAS RAZOÁVEIS COMO SUBSTRATO NORMATIVO NA CONSOLIDAÇÃO DE MECANISMOS DE GOVERNANÇA ALGORÍTMICA NOS SISTEMAS DE DECISÃO AUTOMATIZADA / Paulo Rodrigo de Miranda.– 2022.
212 p.; 30 cm

Orientadora: Valéria Ribas do Nascimento
Dissertação (mestrado) – Universidade Federal de Santa Maria, Centro de Ciências Sociais e Humanas, Programa de Pós-Graduação em Direito, RS, 2022

1. Accountability 2. Direito a inferências razoáveis 3. LGPD 4. Sistemas automatizados de decisão 5. Transparência I. Nascimento, Valéria Ribas do II. Título.

Sistema de geração automática de ficha catalográfica da UFSM. Dados fornecidos pelo autor(a). Sob supervisão da Direção da Divisão de Processos Técnicos da Biblioteca Central. Bibliotecária responsável Paula Schoenfeldt Patta CRB 10/1728.

Declaro, PAULO RODRIGO DE MIRANDA, para os devidos fins e sob as penas da lei, que a pesquisa constante neste trabalho de conclusão de curso (Dissertação) foi por mim elaborada e que as informações necessárias objeto de consulta em literatura e outras fontes estão devidamente referenciadas. Declaro, ainda, que este trabalho ou parte dele não foi apresentado anteriormente para obtenção de qualquer outro grau acadêmico, estando ciente de que a inveracidade da presente declaração poderá resultar na anulação da titulação pela Universidade, entre outras consequências legais.

Paulo Rodrigo de Miranda

DIREITO A INFERÊNCIAS RAZOÁVEIS COMO SUBSTRATO NORMATIVO NA CONSOLIDAÇÃO DE MECANISMOS DE GOVERNANÇA ALGORÍTMICA NOS SISTEMAS AUTOMATIZADOS DE DECISÃO

Dissertação apresentada ao Programa de Pós-Graduação em Direito, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Mestre em Direito.**

Aprovado em 25 de março de 2022:

Valéria Ribas do Nascimento, Dra. (UFSM)
(Presidente/Orientadora)

Rosane Leal da Silva, Dra. (UFSM)
(Avaliadora interna)

Eduardo Magrani, Dr. (Harvard)
(Avaliador externo)

Santa Maria, RS, Brasil
2022

AGRADECIMENTOS

Encerra-se esse ciclo acadêmico, cujas etapas foram cingidas por pessoas que prestaram auxílio de suas mais diversas formas. Por essa razão, agradeço:

Aos meus tios, Ana Caraffa e Larri Carafa, que sempre me apoiaram nos estudos, fazendo esforços imensuráveis para que eu pudesse concluir minha graduação em Direito.

À professora Valéria Ribas, que tenho uma gratidão especial por ter acreditado na minha capacidade de ingressar na seleção do mestrado da UFSM e, posteriormente, por ter aceitado ser minha orientadora, acompanhando-me, nessa trajetória, sempre com paciência e disposição para novas ideias.

À minha companheira Nadine, pelo apoio incondicional nos estudos e na profissão, bem como por sua compreensão e ternura em todas as horas que não me fiz presente nos últimos meses.

À professora Rosane Leal, que tive a oportunidade de ser seu aluno no mestrado, por ter aceitado compor a banca e pelas instigações e reflexões materializadas através de seus valiosos comentários que informaram a presente dissertação.

Ao professor Eduardo Magrani, por gentilmente se dispor a compor a banca de mestrado, sendo grande referência nos temas relacionados a governança de algoritmos e proteção de dados, cujas obras e artigos alimentaram muitas das seções da presente pesquisa.

À minha amiga Isadora, por ter reavivado minha pretensão acadêmica, ao me introduzir no grupo de pesquisa e indicar os caminhos para a seleção do mestrado.

Aos meus colegas de mestrado, em especial Leonardo Trevisan, Bruna Obaldia, Pedro Witschoreck e Alexandre Krob, os quais sempre se colocaram à disposição para me ajudar no transcurso desse projeto acadêmico.

Ao meu amigo Walter pelos sábios conselhos prestados nas horas difíceis, especialmente quanto à minha resistência em encerrar a pesquisa, ponderando que o ato de escrever uma dissertação é um projeto inacabável e que estará sempre em constante evolução, tal como a vida.

Agora, a tarefa da tecnologia digital não é mais apenas facilitar o armazenamento, indexação e manipulação de coleções de dados criptografados, textuais, de áudio ou icônicos, mas revelar automaticamente a composição de circunstâncias de todos os tipos. O digital surge como um poder aletheico, uma instância destinada a mostrar aletheia, a verdade, no sentido definido pela filosofia grega antiga, entendida como a revelação, a manifestação da realidade dos fenômenos além de sua aparência.

[...]

Os dispositivos aletéicos estão destinados, por sua crescente sofisticação, a impor sua lei, orientando as situações humanas do auge de sua autoridade. E isso não de forma homogênea, mas em diferentes graus, desde um nível de incentivo, como no caso de um aplicativo de adequação que sugere um determinado suplemento alimentar, até um nível prescritivo, como no caso de um empréstimo bancário, até atingir níveis coercitivos, especialmente no campo do trabalho, com sistemas capazes de ditar as ações a serem executadas. A partir deste momento, a tecnologia passa a ter um "poder injuntivo"; o livre exercício de nossa faculdade de julgamento e ação é substituído por protocolos destinados a modificar nossas ações individuais ou impulsos individuais da realidade a fim de "infundir-nos" com a trajetória correta a seguir. A humanidade rapidamente se dota de um órgão que a despoja de si mesma, de seu direito de decidir, com consciência e responsabilidade, as coisas que lhe dizem respeito.

– Critica della ragione artificiale: Una difesa dell'umanità, Éric Sadin.

RESUMO

DIREITO A INFERÊNCIAS RAZOÁVEIS COMO SUBSTRATO NORMATIVO NA CONSOLIDAÇÃO DE MECANISMOS DE GOVERNANÇA ALGORÍTMICA NOS SISTEMAS DE DECISÃO AUTOMATIZADA

AUTOR: Paulo Rodrigo de Miranda
ORIENTADORA: Valéria Ribas do Nascimento

O presente trabalho tem por objetivo verificar a viabilidade do reconhecimento do direito a inferências razoáveis como um substrato normativo no desenvolvimento de mecanismos de governança de algoritmos em sistemas automatizados de decisão que busque o fortalecimento de abordagens *ex ante* e uma estrutura normativa permeada por uma análise de gestão de risco (*risk-basead approach*) que garantam maior transparência e *accountability* por parte dos controladores de dados. Para desenvolver o tema da dissertação foram traçados quatro capítulos contendo os objetivos específicos. O primeiro capítulo aborda questões envolvendo a sociedade de controle na era digital dentro do contexto da governamentalidade algorítmica, de modo a ensejar uma reflexão entre o poder de controle dos algoritmos nos sistemas automatizados de decisão e a liberdade de escolha dos destinatários desses sistemas, bem como análise dos riscos oriundos da implementação desses sistemas, tais como os vieses discriminatórios e a opacidade. O segundo capítulo analisa os elementos constitucionais da tutela dos dados pessoais, dentro de uma proposição de ampliação do seu âmbito de proteção para reconhecer o direito a inferências razoáveis como um desdobramento da dimensão subjetiva do direito fundamental de proteção de dados, verificando as dimensões subjetiva e objetiva do referido direito fundamental. O terceiro capítulo apresenta o direito a inferências razoáveis como substrato normativo na consolidação de mecanismos de governança. O quarto capítulo analisa o papel da governança de algoritmos, dentro de uma estrutura de corregulação e de uma abordagem baseada em risco, que busca consolidar os arranjos institucionais da LGPD no estabelecimento de diretrizes de *compliance* e *accountability* por parte dos responsáveis de tratamento de dados envolvendo sistemas automatizados de decisão. Para responder o questionamento do tema adotou-se uma abordagem dedutiva com uma generalização do tema para a retomada de uma questão particularizada. De igual modo, será utilizado o método de procedimento pesquisa bibliográfica. Conclui-se, sumariamente que o direito a inferências razoáveis pode ser compreendido como um *standard* de comportamento para o controlador de dados, tendo a capacidade para o estabelecimento de mecanismos de governança baseados na *compliance*. Essa percepção permitirá assegurar que o desenvolvimento ou implementação de sistemas automatizados de decisão sejam realizados com a adoção de medidas técnicas e organizacionais apropriados aos riscos envolvidos em suas atividades, viabilizando, o máximo possível, transparência e *accountability* nessa procedimentalização.

Palavras-chave: *Accountability.* Direito a inferências razoáveis. LGPD. Sistemas automatizados de decisão. Transparência.

ABSTRACT

RIGHT TO REASONABLE INFERENCES AS A NORMATIVE SUBSTRATE IN CONSOLIDATING ALGORITHMIC GOVERNANCE MECHANISMS IN AUTOMATED DECISION SYSTEMS

AUTHOR: Paulo Rodrigo de Miranda
GUIDELINE: Valéria Ribas do Nascimento

This study sought to verify the feasibility of recognizing the right to reasonable inferences as a normative substrate in developing algorithm governance mechanisms in automated decision-making systems that seek to strengthen *ex-ante* approaches and a normative structure permeated by a risk-based approach that ensures greater transparency and accountability on the part of data controllers. Four chapters containing the specific objectives were outlined to develop the dissertation's theme. The first chapter addresses issues involving the society of control in the digital age within the context of algorithmic governmentality to encourage reflection between the power of algorithm control in automated decision-making systems and the freedom of choice of the recipients of these systems, as well as an analysis of the risks arising from implementing these systems, including discriminatory biases and opacity. The second chapter covers the constitutional elements of the protection of personal data within a proposition of amplifying its scope of protection to recognize the right to reasonable inferences as an unfolding of the subjective dimension of the fundamental right to data protection by analyzing the subjective and objective dimensions of the referred fundamental right. The third chapter presents the right to reasonable inferences as a normative substrate in consolidating governance mechanisms. Lastly, the fourth chapter encompasses an analysis of the role of algorithm governance within a framework of co-regulation and a risk-based approach, which seeks to consolidate the institutional arrangements of the General Personal Data Protection Law in establishing compliance and accountability guidelines by data controllers involving automated decision-making systems. To answer the question of the topic, a deductive approach was employed with a generalization of the topic for the resumption of a particularized question; likewise, the bibliographical research method was used. It was possible to conclude that, summarily, the right to reasonable inferences can be understood as a standard of behavior for the data controller and having the capacity for establishing governance mechanisms based on compliance. This will enable the development or implementation of automated decision-making systems to be assured and employed by adopting technical and organizational measures that are appropriate to the risks involved in their activities, enabling, as much as possible, transparency and accountability in this proceduralization.

Keywords: Accountability. Right to reasonable inferences. LGPD. Automated decision systems. Transparency.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACLU	*American Civil Liberties Union*
AIA	*Artificial Intelligence Act*
AIRA	Avaliação de Risco da Inteligência Artificial
ANPD	Autoridade Nacional de Proteção de Dados
CCGD	Comitê Central de Governança de Dados
CF	Constituição Federal
DPIA	*Data Protection Impact Assesment*
GDPR	*General Data Protection Regulation*
IA	Inteligência Artificial
IBGE	Instituto Brasileiro de Geografia e Estatística
ICO	*Information Commissioner's Office*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
LGPD	Lei Geral de Proteção de Dados
LIA	*Legitimate Interests Assessment*
PL	Projeto de Lei
RGPD	Regulamento Geral de Proteção de Dados
RIPDP	Relatório de Impacto à Proteção de Dados
STF	Supremo Tribunal Federal
WP29	*Working Party article* 29

SUMÁRIO

1 INTRODUÇÃO

A presente dissertação tem como tema a análise do direito a inferências razoáveis como um desdobramento da dimensão subjetiva do direito fundamental de proteção de dados, lastreada na autodeterminação informacional e no livre desenvolvimento da personalidade, e a sua funcionalidade como substrato normativo na construção de mecanismos de governança voltados a implementação de transparência e *accountability* nos sistemas automatizados de decisão. Para tanto, o estudo centrou-se no reconhecimento do direito a inferências razoáveis e a sua funcionalidade como substrato normativo na consolidação de mecanismos de governança voltados a viabilizar maior transparência, responsabilização e prestação de contas dos responsáveis pelo tratamento de dados, dentro do contexto das externalidades negativas dos sistemas automatizados de decisão, que empregam métodos de análise inferencial e a criação de perfis, bem como diante da necessidade da adoção de uma estrutura de corregulação com abordagem baseada na análise de risco (*risk-basead approach*).

A construção da realidade da ordem social está sendo moldada por uma estrutura digital imperceptível e onipresente. Com o avanço da tecnologia de armazenamento de dados houve a ampliação de mecanismos de coleta e tratamento de dados pessoais otimizados por sistemas automatizados, capazes de mediar as necessidades humanas e estruturar as demandas sociais.

A expropriação, monetização e a correlação de dados por mecanismos baseados na big data revelam as garras da racionalidade econômica que alimentam os sistemas automatizados responsáveis pela engrenagem de diversos serviços, desde plataformas digitais a softwares ou aplicativos utilizadas por governos e empresas para atender demandas específicas. Contudo, quando essa estrutura digital é direcionada para fins de avaliações educacionais[1], campanhas políticas[2],

[1] Sobre o tema recomenda-se a leitura do artigo de Mônica Tiemy Fujimoto: Desafios do *compliance* de dados nas instituições de ensino básico e superior. *In*: FRAZÃO, Ana, CUEVA, Ricardo Villas Bôas (Coord.). *Compliance* e políticas de proteção de dados. São Paulo: Revista dos Tribunais, 2022.

[2] Sobre o tema recomenda-se a leitura dos seguintes artigos: CRUZ, Francisco Brito; MASSARO, Heloisa. Dados pessoais em campanhas políticas: a construção de uma ponte entre proteção de dados pessoais e regulação eleitoral. *In*: DONEDA, Danilo, et. al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021; MAGRANI, Eduardo. Hackeando o eleitorado: sobre o uso de dados pessoais em campanhas eleitorais. Berlim: Fundação Konrad Adenauer, 2020; MAGRANI, Eduardo; MIRANDA, Paulo Rodrigo de. *Social bots* e campanhas eleitorais dentro da esfera pública

seleção de candidatos a empregos, e até mesmo para a implementação de mecanismos relacionados a policiamento preditivo ou aplicação da justiça criminal, a falta de transparência em relação aos titulares dos dados ou destinatários desses sistemas, que muitas vezes não conseguem acessar ou avaliar a qualidade das inferências que são realizadas sobre eles, coloca em risco questões fundamentais inerentes à dignidade humana, em especial à autodeterminação informacional[3] e ao livre desenvolvimento da personalidade[4].

Assim, diante do exponencial progresso do uso de sistemas automatizados de decisão surgem preocupações quanto aos seus riscos aos direitos fundamentais e os meios regulatórios adequados. Portanto, o foco do presente trabalho será a análise de mecanismos de governança para contornar os problemas oriundos da predição comportamental individual (que também gera externalidades negativas transindividuais) em sistemas automatizados de decisão, na realização de inferências e criação de perfis.

Diante dessas constatações, impõe-se a ponderação a respeito dos desafios jurídicos relacionados aos meios regulatórios adequados que permitam equalizar o exponencial uso de sistemas automatizados de decisão e a proteção a direitos fundamentais. Da análise da Lei Geral de Proteção de Dados (LGPD) observa-se a existência de uma aparente lacuna no texto legal quanto ao estabelecimento de limites e responsabilidades aos controladores de dados quando o tema envolve a realização de inferências e a construção de perfis voltados a subsidiar sistemas automatizados de decisão.

Contudo, o presente trabalho propõe uma ampliação do âmbito de proteção dos dados pessoais a partir do reconhecimento do direito a inferências razoáveis como um desdobramento da dimensão subjetiva do direito fundamental da proteção de dados. A partir disso, é possível extrair da LGPD diversas orientações normativas que viabilizam a construção de uma estrutura legal que deve orientar o tratamento

---

automatizada. Fundação Konrad Adenauer, Cadernos Adenauer 4, Ano XXII, 2021. Disponível em: https://www.kas.de/pt/web/brasilien/einzeltitel/-/content/technologische-innovationen-und-ihre-auswirkungen-auf-die-brasilianische-demokratie.

[3] O princípio da autodeterminação informacional consistiria na prerrogativa de cada indivíduo decidir sobre a divulgação e a utilização de seus dados pessoais (SARLET, 2021) conforme será desenvolvido no segundo capítulo do presente trabalho.

[4] Trata-se de um princípio implícito extraído da dignidade da pessoa humana e dos valores constitucionais como a liberdade e igualdade (LUDWIG, 2001). A dignidade da pessoa humana compreende a autodeterminação consciente e responsável da própria vida, que se realizará plenamente pelo respeito dessas escolhas por parte do Estado e pela comunidade (SARLET, 2008). Esse tema será desenvolvido no segundo capítulo do presente trabalho.

de dados realizados pelos responsáveis no desenvolvimento e na implementação de tecnologias que empregam métodos de análise inferencial e criação de perfis.

Nesse panorama, o trabalho visa, igualmente, enfrentar alguns pontos estratégicos que envolvem as externalidades negativas dos sistemas automatizados de decisão, diante do risco elevado a ser considerado em razão dos vieses discriminatórios e a opacidade inerentes ao aprendizado de máquina. Ademais, a necessidade da construção de mecanismos de governança que garantam transparência e *accountability* é um dos elementos centrais que conectará todos os capítulos do trabalho.

Quando um sistema automatizado de decisão produz um resultado (*outputs*) e não é possível acessar ou avaliar como foram feitas as inferências sobre os usuários destinatários desse sistema, constata-se uma séria limitação à autodeterminação informacional e ao livre desenvolvimento da personalidade aos titulares de dados envolvidos. De igual modo, evidencia-se a existência de barreiras significativas quanto ao acesso das justificativas que se embasaram determinada decisão, ainda que injusta ou discriminatória, negando-se aos destinatários desses sistemas tecnológicos, mecanismos de defesa para se contrapor ao resultado apresentado pelos algoritmos.

A partir disso, o presente trabalho visa analisar as contribuições de Sandra Wacther e Brent Mittelstadt na construção de reflexões a respeito dos riscos da análise inferencial e da criação de perfis e da importância da adoção de mecanismos *ex ante* como forma de viabilizar a tutela do livre desenvolvimento da personalidade e da autodeterminação informacional dos destinatários dos sistemas automatizados de decisão. Assim, pretende-se defender a necessidade de se exigir dos controladores de dados que justifiquem aos reguladores ou titulares de dados informações essenciais que permitam a prestação de contas a respeito de como os sistemas automatizados de decisão produzem inferências sobre os indivíduos.

Atualmente, são os controladores de dados que definem como devem realizar o tratamento de dados e não possuem, a rigor, nenhuma obrigação legal de âmbito nacional a viabilizar a transparência do projeto, o uso de modelos de inteligência artificial e quais os dados específicos utilizados para fazer inferências e alimentar os sistemas automatizados de decisão.

A falta de transparência a respeito da lógica subjacente ao desenvolvimento dessas tecnologias é um problema sério a ser enfrentado, especialmente quando se

observa que em muitos casos os titulares dos dados ou destinatários de serviços que empregam sistemas automatizados de decisão não conseguem ter acesso ou avaliar como as inferências são processadas pelas tecnologias, inviabilizando, inclusive, o exercício do próprio direito a explicação. Ademais, inexiste qualquer previsão legal quanto a um procedimento prévio que viabilize a efetiva contestação de decisões automatizadas de alto risco que possam resultar em ameaça ou lesão a direitos fundamentais dos destinatários destes sistemas.

Dentro dessa perspectiva, serão abordadas algumas ideias que permitam circunscrever mecanismos de *compliance* e *accountability* na busca do desenvolvimento de tecnologias em conformidade com as diretrizes normativas estabelecidas pela LGPD, especialmente sua estrutura deontológica. Para tanto, tendo em vista a existência de interoperabilidade entre a legislação europeia e a brasileira, as quais possuem nítidos pontos convergentes, serão analisados em conjunto as orientações e normativas da União Europeia, em especial o Regulamento Geral de Proteção de Dados (RGPD) e as diretrizes fornecidas pelo Grupo de Trabalho do Artigo 29 (*Working Party article* 29[5]) e pelo Grupo de Especialistas de Alto Nível em Inteligência Artificial da Comissão Europeia (*High-Level Expert Groupon Artificial Intelligence – AI HLEG*).

Diante do exponencial progresso do uso de sistemas automatizados de decisão surgem preocupações quanto aos seus riscos e os meios regulatórios adequados. Nesse sentido, o problema de pesquisa envolve o questionamento a respeito da capacidade do reconhecimento do direito a inferências razoáveis como um substrato normativo suficiente para o estabelecimento de mecanismos de governança baseados na *compliance*, que permitam assegurar a transparência e *accountability* no tratamento de dados envolvendo os sistemas automatizados de decisão.

A fim de responder a referida pergunta e desenvolver os objetivos específicos, a presente pesquisa será dividida em quatro capítulos.

No primeiro capítulo, após uma reflexão entre o poder de controle dos algoritmos nos sistemas automatizados de decisão e a liberdade de escolha dos destinatários destes sistemas, será realizada uma abordagem sobre as premissas

[5] O Grupo de Trabalho do Artigo 29 foi criado pela Diretiva 95/46/CE e tratou de questões relacionadas à proteção da privacidade e dos dados pessoais até 25 de maio de 2018, data da entrada em vigor do RGPD. Disponível em: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en.

que envolvem a compreensão dos sistemas automatizados de decisão e a mediação algorítmica no cotidiano contemporâneo, dentro de uma perspectiva da governamentalidade algorítmica. Nesse panorama, serão aprofundados os riscos do uso dos sistemas automatizados de decisão lastreados nos vieses discriminatórios e na opacidade.

O segundo capítulo tem por objetivo analisar os elementos constitucionais da tutela dos dados pessoais dentro de uma proposição de ampliação do seu âmbito de proteção para reconhecer o direito a inferências razoáveis como um desdobramento da dimensão subjetiva do direito fundamental da proteção de dados. Para tanto, será apresentado um breve contexto das leis protetivas de dados e do direito fundamental de proteção de dados, com a posterior análise dos princípios constitucionais implícitos do livre desenvolvimento da personalidade e autodeterminação informacional. A partir disso, é apresentado o direito a inferências razoáveis dentro da concepção expansionista do conceito de proteção de dados, analisando as dimensões subjetiva e objetiva do direito fundamental de proteção de dados.

No terceiro capítulo, será demonstrado que os direitos a revisão e a explicação previstos na LGPD são ferramentas insuficientes na tutela de direitos e interesses dos destinatários dos sistemas automatizados de decisão, revelando-se incapazes, em uma análise isolada, de apresentarem soluções compatíveis com as complexidades decorrentes das análises inferenciais e correlações que geram perfis. Por essa razão, o presente trabalho propõe o reconhecimento de uma estrutura constituída em quatro pilares que decorrem da dimensão objetiva do direito fundamental de proteção de dados pessoais, a partir do reconhecimento de um direito a inferências razoáveis constituídos por: i) guias deontológicos; ii) regras de boa governança; iii) legítimo interesse, e iv) direito a explicação e revisão. Essas ferramentas analisadas em conjunto permitem a consolidação de mecanismos de governança baseados na *compliance* e vão dar suporte ao capítulo seguinte.

No quarto capítulo, serão enfrentados os problemas relacionados aos desafios regulatórios e os mecanismos de governança de algoritmos, buscando investigar as opções de estrutura de governança tendo a corregulação como seu eixo central. Portanto, objetiva-se analisar a abordagem baseada em risco (*risk-basead approach*) dentro dos arranjos institucionais da LGPD na busca do estabelecimento de diretrizes de *compliance* e *accountability* por parte dos responsáveis de tratamento de dados envolvendo sistemas automatizados de

decisão. Ao final, busca-se consolidar uma estrutura normativa extraída da LGPD que viabilize a implementação de diversas camadas de transparência durante o desenvolvimento, execução e fiscalização das tecnologias que usem sistemas automatizados de decisão baseadas em aprendizado de máquina de elevado risco em harmonia com o princípio da *accountability*.

O presente trabalho se adequa perfeitamente à área de concentração do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria, nível mestrado, intitulada “Direitos Emergentes na Sociedade Global”, bem como à linha de pesquisa denominada “Direitos na sociedade em rede: atores, fatores e processos na mundialização”, porquanto o reconhecimento de um direito a inferências razoáveis como substrato normativo para a consolidação de ferramentas de governança na tutela da autodeterminação informacional e do livre desenvolvimento da personalidade articula-se com os direitos na sociedade em rede, especialmente em razão da interoperabilidade entre os institutos normativos de proteção de dados da União Europeia e do Brasil.

Por fim, no que diz respeito à metodologia, será empregado a abordagem dedutiva com uma generalização do tema para a retomada de uma questão particularizada. De igual modo, será utilizado o método de procedimento pesquisa bibliográfica.

Na abordagem dedutiva serão objeto de verificação: a mediação tecnológica promovida pela governamentalidade algorítmica, os riscos dos sistemas automatizados de decisão e seus impactos sobre o livre desenvolvimento da personalidade e a autodeterminação informacional. De igual modo, serão abordados os elementos constitucionais da tutela dos dados pessoais, dentro de uma proposição de ampliação do seu âmbito de proteção, para reconhecer o direito a inferências razoáveis como um desdobramento da dimensão subjetiva do direito fundamental da proteção de dados, bem como serão analisados os mecanismos regulatórios que permitam o estabelecimento de limites e responsabilidades aos controladores de dados que realizam inferências e perfilamento para construção de sistemas automatizados de decisão. A partir dessas premissas gerais, será desenvolvida uma relação lógica entre as premissas particulares relacionadas ao direito a inferências razoáveis como substrato normativo para a construção de uma estrutura de governança de algoritmos, tendo como norte o desenvolvimento de políticas de *compliance* baseadas na corregulação e na abordagem baseada na

análise de risco. Ao final, buscar-se-á uma conclusão particular que demonstre evidências sobre a adoção de mecanismos *ex ante* como forma de viabilizar a tutela da autodeterminação informacional e garantir maior transparência e responsabilidade dos controladores de dados, tendo como diretriz a *accountability* dos responsáveis pelo tratamento de dados referente ao emprego de inferências e criação de perfis.

Para o enfrentamento da problemática central do estudo, o presente trabalho foi pautado pelas contribuições teóricas desenvolvidas por Sandra Wacther, Brent Mittelstadt, Michael Latzer, Natascha Just, Ugo Pagallo e Luciano Floridi. De igual modo, o trabalho contará com abordagens de autores brasileiros que escrevem sobre o tema na atualidade, em especial Eduardo Magrani, Danilo Doneda, Laura Schertel Mendes, Caitlin Molholland, Ana Frazão, Isabella Frajhof, Marcela Mattiuzzo, Bruno Ricardo Bioni, Rosane Leal da Silva, dentre outros cujas obras contribuíram de forma significativa para os *insights* extraídos na construção das reflexões propostas no desenvolvimento dos quatro capítulos.

Por fim, a teoria de base será construída dentro de uma reflexão entre o poder de controle dos algoritmos nos sistemas automatizados de decisão e a liberdade de escolha dos destinatários destes sistemas, que é colocada em risco na esfera automatizada. Para tanto, será realizada uma abordagem da transição da sociedade disciplinar de Foucault para a sociedade de controle de Deleuze e o panóptico digital de Byung-Chul Han. Após, serão aprofundados aspectos da sociedade de controle na era digital dentro da perspectiva de governamentalidade algorítmica produzida pelos sistemas automatizados de decisão, tendo como referência os estudos de Antoinette Rouvroy e Thomas Berns, bem como de Fernanda Bruno. O embasamento teórico busca analisar o componente técnico dentro de uma percepção filosófica, cuja abordagem será subjacente ao texto desenvolvido.

2 SOCIEDADE DE CONTROLE, GOVERNAMENTALIDADE ALGORÍTMICA E OS SISTEMAS AUTOMATIZADOS DE DECISÃO

O emprego de sistemas automatizados de decisão que usam inteligência artificial tem sido adotado com entusiasmo pelo setor privado e público em uma infinidade de áreas. Diante do crescente uso desses sistemas informatizados, a mediação algorítmica tornou-se comum no cotidiano das pessoas, despertando interesses na academia, nos indivíduos e na sociedade a respeito da mediação algorítmica.

Neste primeiro capítulo pretende-se apurar a tensão entre o poder de controle dos algoritmos e a liberdade de escolha dos destinatários dos sistemas automatizados de decisão. A autodeterminação informacional dos titulares de dados e destinatários desses sistemas é colocada em risco diante da obscuridade dos algoritmos e os vieses discriminatórios resultantes de inferências e perfilamento dentro de uma perspectiva baseada na racionalidade econômica dos dados.

Para tanto, inicialmente será realizada uma abordagem da transição da sociedade disciplinar para a sociedade de controle e, após, serão aprofundados aspectos da sociedade de controle na era digital. Em segundo momento, serão abordadas algumas premissas sobre o funcionamento dos sistemas automatizados de decisão. Por fim, serão analisados os riscos dos sistemas automatizados de decisão, o que envolve a governamentalidade algorítmica, os vieses discriminatórios e a opacidade.

2.1 A SOCIEDADE DE CONTROLE NA ERA DIGITAL

A reflexão acerca da governança por algoritmos na modulação das subjetividades dos indivíduos reverbera nas considerações sobre os regimes de poder desenvolvida por Michel Foucault, especialmente na perspectiva de um poder disciplinar. A constituição da sociedade disciplinar é caracterizada pela “existência de poderes hierarquizados, baseada em estratégias de disciplina e confinamento, nos quais o comando social é construído mediante uma rede difusa de dispositivos ou aparelhos que produzem e regulam os costumes, os hábitos e as práticas produtivas” (HARDT; NEGRI, 2006, p. 42).

A instrumentalização das disciplinas precisa da existência de instituições disciplinares, tal como a prisão, a fábrica, o asilo, o hospital e a escola, as quais têm por função docilizar e vigiar as pessoas adequando-as às necessidades de um novo modelo capitalista emergente (CASSINO, 2020). Os saberes disciplinares surgem como um mecanismo de biopoder de governamentalidade do sujeito e do social, atuando na modelização da vida dos indivíduos e contribuindo para a constituição do capitalismo industrial (HUR, 2013).

Dentro desse contexto, há a constituição de um saber normalizador que se conecta ao capitalismo e o corpo é tomado como uma máquina. Essa impressão de vigilância e confinamento que docciliza os corpos é a sensação do Panóptico de Jeremy Benthan. A ideia do panóptico é assegurar uma vigilância total sobre os corpos confinados em instituições, desenvolvendo-se um conjunto de saberes norteadores do biopoder (HUR, 2013).

Conforme pondera Fernanda Bruno (2013, p. 57), “as instituições disciplinares, que encontram seu modelo ideal no Panóptico, são máquinas de ver que produzem modos de ser”. Com efeito, os dispositivos disciplinares na perspectiva foucaultiana asseguram a opacidade do poder e ao mesmo tempo a transparência dos indivíduos.

Nesse sentido, ao abordar o poder disciplinar e a sua invisibilidade, Foucault pondera que:

> O poder disciplinar, ao contrário, se exerce tornando-se invisível: em compensação impõe aos que submete um princípio de visibilidade obrigatória. Na disciplina, são os súditos que têm que ser vistos. Sua iluminação assegura a garra do poder que se exerce sobre eles. É o fato de ser visto sem cessar, de sempre poder ser visto, que mantém sujeito o indivíduo disciplinar. E o exame é a técnica pela qual o poder, em vez de emitir os sinais de seu poderio, em vez de impor sua marca a seus súditos, capta-os num mecanismo de objetivação. (FOUCAULT, 1999, p. 211)

As redes sociais da internet conservam o diagnóstico de Foucault sobre a armadilha da visibilidade, porquanto estas redes amplificam as dinâmicas de visibilidade dos indivíduos ao mesmo tempo que ampliam a vigilância, esta, por sua vez, discreta e menos conhecida (BRUNO, 2013b). Para Fernanda Bruno (2013b), nas sociedades atuais, há um domínio de convivência ou de sobreposição de procedimentos disciplinares e procedimentos de controle quando se trata de vigilância.

Essa questão é reanalisada por Deleuze em seu importante artigo intitulado *Post-scriptum*: sobre as sociedades de controle (1990). Na sociedade de controle os mecanismos de comando se tornam cada vez mais imanentes ao campo social, distribuídos nos indivíduos de modo que os comportamentos de integração social e de exclusão próprios do mando são interiorizados nos próprios súditos (HARDT; NEGRI, 2006, p. 42).

Conforme Deleuze (2013, p. 220) alertou: “estamos entrando nas sociedades de controle, que funcionam não mais por confinamento, mas por controle contínuo e comunicação instantânea”. Assim, enquanto o poder da sociedade disciplinar se exercia através da noção de confinamento, vigilância hierárquica e a sanção normalizadora, a sociedade de controle passa a ser caracterizada pela invisibilidade e uma onipresença, sendo conduzida de forma imperceptível e em todos os lugares.

Até os anos 1970 a maior parte dos bancos de dados e arquivos sobre indivíduos era de domínio estrito dos Estados, constituindo um modelo centralizado e hierarquizado de informações (BRUNO, 2013). Contudo, atualmente o cenário é outro, há um aumento exponencial nos bancos de dados, tanto públicos como privados, bem como um cruzamento entre eles, de modo que a massa de dados circula por uma rede descentralizada e com finalidades distintas (BRUNO, 2013).

Nessa transição da sociedade disciplinar desenvolvida por Foucault para uma virtualização da figura do controle, o poder disciplinar torna-se algo muito mais sútil e impessoal, porquanto constroem-se mecanismos que permitem um controle exercido de forma invisível por sistemas tecnológicos independentemente do conhecimento dos indivíduos. Para Deleuze (1987, não paginado) o controle pode ser visualizado “como uma estrada” que não “se enclausuram pessoas”, mas sim se “multiplicam os meios de controle”. Através das estradas as pessoas podem trafegar livremente, sem a mínima clausura, e ainda assim, serem perfeitamente controladas (DELEUZE, 1987).

Segundo Antoinette Rouvroy (2020, p. 17), “com os *big data*, a ideia é gerar hipóteses e critérios de classificação a partir dos dados”. Esse processo de estratificação do indivíduo ou quantificação dos elementos informacionais que o compõem é representado na *Big Data* como datatificação (MEJIAS; COULDRY, 2019).

Para Mejias e Couldry (2019) a datatificação (*datafication*) decorre de um processo de produção de dados que possui dois elementos centrais: i) a

infraestrutura externa, responsável pela coleta, processamento e armazenamento dos dados, e ii) estruturas tecnológicas de geração de valor, que consistem basicamente na monetização dos dados e meios de controle estatal. Portanto, as informações de dados combinam a transformação da vida humana em dados através de processos de quantificação e a geração de diferentes tipos de valor a partir dos dados.

Byung-Chul Han (2020), ao analisar o contexto atual dentro da percepção foucaultiana, observa que o Panóptico disciplinar transmuda-se em um Panóptico digital mais eficiente conduzido pelas mídias sociais, livre de coerção e baseado na liberdade e na comunicação ilimitadas. A sociedade digital de controle faz uso intensivo da liberdade, porquanto os indivíduos (como internos do Panóptico digital) comunicam-se intensivamente e expõem-se por vontade própria, havendo uma entrega de dados pelos usuários desses sistemas sem necessidade de coação (HAN, 2020).

Com efeito, as novas tecnologias estabelecem mutações das sociedades disciplinares, sendo tal processo acompanhado por uma profunda transformação dos corpos sociais, formando uma nova sociedade de controle que integram os indivíduos em novas máquinas sob a forma de banco de dados, de algoritmos, de fluxos de informações (LAPOUJADE, 2015). Conforme destaca Hur (2013), a sofisticação das técnicas de gestão da vida constitui-se uma nova mecânica de controle, na qual a prática é de modulação de comportamentos (desejos e pensamentos dos coletivos), numa moldagem auto-deformante que atua em conformidade com a axiomática do capital.

A técnica deixa de ser um meio à disposição do homem, criando o próprio ambiente no interior do qual o homem sofre modificações (GALIMBERT, 2015). Desse modo, a tecnologia torna-se o ambiente do homem, “aquilo que o cerca e o constitui segundo as regras de uma racionalidade que, baseada no critério de funcionalidade e eficiência, não hesita em subordinar as próprias exigências do homem às exigências do aparato técnico” (GALIMBERT, 2001, p. 04).

Dentro dessa perspectiva observa-se que esse processo de transformação dos indivíduos em “dividuais” afeta de forma contundente a sua singularidade, reduzindo-os a amostras nos bancos de dados da *big data*. Desse modo, o foco não está mais no indivíduo em si, o qual cede espaço para a análise de seus dados, de

seus diversos perfis que lhe são atribuídos de forma automatizada pelos algoritmos responsáveis pela intermediação de seu cotidiano.

Diante disso, torna-se necessário esclarecer alguns pontos específicos que permitam uma melhor compreensão a respeito dos sistemas automatizados de decisão.

2.2 PREMISSAS SOBRE A COMPREENSÃO DOS SISTEMAS DE DECISÃO AUTOMATIZADOS

Com o avanço da big data[6] houve a ampliação do uso da inteligência artificial em diversos âmbitos da sociedade tendo como objetivo principal a predição. A predição pode ser entendida como um processo de preenchimento de informações ausentes, sendo que um determinado sistema utiliza informações disponíveis (dados) para gerar novas informações (AGRAWAL; GANS; GOLDFARB, 2019). Portanto, o principal fator diferencial das novas tecnologias que empregam inteligência artificial é a predição. E essa tecnologia de predição, através do uso de algoritmos e dados disponíveis em grande quantidade, é o insumo para os sistemas automatizados de decisões.

Inicialmente cumpre registrar que a Lei Geral de Proteção de Dados (LGPD) não apresentou um conceito do que seria decisão automatizada. Contudo, tramita perante o Congresso Nacional o Projeto de Lei nº 4496 de 2019 (PL 4496/2019), de autoria do Senador Styvenson Valentim, que objetiva a alteração da LGPD para a inclusão da definição da expressão “decisão automatizada”.

Segundo o PL 4496/2019 decisão automatizada:

> [...] é o processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou escore, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, inteligência artificial, aprendizado de máquina, ou outra técnica computacional.

[6] “*Big data* é o termo em inglês que descreve o grande volume de dados gerados e armazenados, que podem se estruturados e não-estruturados. Dados estruturados são os dados organizados de alguma forma (banco de dados, planilhas eletrônicas, p. ex.) e dados não-estruturados são os dados não submetidos a uma organização definida (website, mídia, arquivo de texto, p. ex.). Estima-se que apenas 10% dos dados gerados são estruturados.” (KAUFMAN, 2019, p. 32).

Na justificativa do PL 4496/2019, o senador Styvenson Valentim aponta que o tratamento de dados para decisões automatizados abordados no artigo 20 da LGPD carece de aperfeiçoamentos para dar ao comando legal a efetividade necessária e que a lacuna quanto ao conceito da expressão “decisão automatizada” poderia ser capaz de comprometer a proteção pretendida. Conforme será exposto no terceiro capítulo dessa obra, realmente existem diversos temas que deixaram de ser regulamentados pelo legislador e criam barreiras para a efetiva aplicação dos direitos à explicação e à revisão previstos no artigo 20, caput e parágrafo primeiro.

Contudo, o conceito de “sistemas automatizados” de decisão seria o menos relevante, existindo outras questões carentes de regulamentação que são pressupostos básicos para a devida compreensão dos institutos consagrados no art. 20 da LGPD. Ademais, o PL 4496/2019 não aborda a questão do que vem a ser uma decisão “totalmente” automatizada, o que sem dúvida é uma preocupação muito mais relevante em termos de regulamentação do que o próprio conceito de “sistemas automatizados” que pode ser extraído de diversos artigos específicos sobre o tema. As ponderações sobre essa carência de regulação serão objeto de análise no terceiro capítulo do presente trabalho.

Com a evolução técnica dos computadores e o aumento exponencial da coleta de dados, houve uma melhora significativa na capacidade e no desenvolvimento de algoritmos de aprendizado de máquina essenciais na qualidade das predições. Para Agrawal, Gans e Goldfarb (2019) o aprendizado de máquina é retratado como “inteligência artificial” porquanto atualmente possui uma capacidade impressionante de predição. A predição é o componente-chave da inteligência artificial, porquanto a alta precisão de predição permite que as máquinas executem tarefas que até então estavam associadas à inteligência humana (AGRAWAL; GANS; GOLDFARB, 2019). Contudo, deve-se observar que “os algoritmos atuais não são capazes de raciocinar” (AGRAWAL; GANS; GOLDFARB, 2019, p. 40)

Nesse panorama, surge a relevância do conceito de inteligência artificial (“IA” ou *Artificial Intelligence*[7]) que, segundo McCarthy[8] (2007), pioneiro no campo de

[7]McCarthy (2007, não paginado) define inteligência artificial como “a ciência e a engenharia de fabricação de máquinas inteligentes, especialmente programas de computador inteligentes. Está relacionado à tarefa semelhante de usar computadores para entender a inteligência humana, mas a inteligência artificial não precisa se limitar a métodos que são biologicamente observáveis”.

[8] McCarthy cunhou o termo "IA" em 1956 em conexão com um workshop de verão proposto no *Dartmouth College*, do qual participaram muitos dos principais pensadores do mundo em

inteligência artificial, a definiu como uma ciência responsável pela criação de máquinas especialmente programadas por computador, com capacidade de realizar tarefas similares às praticadas por humanos, contudo, sem se limitar a métodos que são biologicamente observáveis.

Nesse sentido, pode-se afirmar que a inteligência artificial é uma “ciência multidisciplinar que possui como objetivo o desenvolvimento de técnicas computacionais que simulem o comportamento e a inteligência humana em diversas atividades” (GOLDSCHMIDT, 2010, p. 08). Desse modo, seriam programas capazes de aprender a realizar uma tarefa não a partir de instruções explícitas, como na programação tradicional, mas por meio de experiência (BIGONHA, 2018).

A respeito da funcionalidade e autonomia do *machine learning* (aprendizado de máquina) Pedro Domingos é esclarecedor:

> Todo algoritmo tem uma entrada e uma saída: os dados entram no computador, o algoritmo faz o que precisa com eles, e um resultado é produzido. O *machine learning* faz o contrário: entram os dados e o resultado desejado, e é produzido o algoritmo que transforma um no outro. Os algoritmos de aprendizado – também conhecidos como aprendizes – são aqueles que criam outros algoritmos. Com o *machine learning*, os computadores escrevem seus próprios programas, logo não precisamos mais fazê-lo. (DOMINGOS, 2015, p. 25)

Assim, quanto maior a quantidade, a qualidade e a diversidade de dados (experiências) disponíveis, mais complexas podem ser as tarefas aprendidas e executadas por esses algoritmos (BIGONHA, 2018). Por exemplo, os monitores de frequência cardíaca, tal como o *Apple Wacth*, permitem a coleta e armazenamentos de dados de entrada (*input*) de seus usuários, alimentado um banco de dados com informações sobre frequência cardíaca (AGRAWAL; GANS; GOLDFARB, 2018). Através de uma aplicação médica, tal como o *Cardiogram*, é possível o monitoramento de usuários e a predição de quais padrões de frequência cardíaca podem apresentar um ritmo considerado irregular pelo sistema que colocará o usuário no grupo de risco de pacientes com arritmia cardíaca e com probabilidade de um acidente vascular cerebral (AGRAWAL; GANS; GOLDFARB, 2019).

Nesse panorama, Agrawal, Gans e Goldfarb (2019) apontam que com a inteligência artificial os dados possuem três funções: i) dados de entrada (*input*), que servem como insumo aos algoritmos e são utilizado para gerar predições; ii) dados

---

computação. Disponível em: https://www.computerhistory.org/fellowawards/hall/john-mccarthy/. Acesso em: 23 set. 2019.

de treinamento (*training data*), responsáveis por treinar a inteligência artificial de modo que ela seja apta a realizar predições para determinadas finalidades, e; iii) dados de *feedback*, que possuem o objetivo de otimizar o desempenho dos algoritmos através da experiência.

Com efeito, a IA procura identificar padrões a partir da análise de dados por meio de uma lógica matemática. Trata-se da utilização de algoritmos[9], que, de forma singela, podem ser idealizados como uma sequência de instruções que orientam o computador sobre o que fazer. Dentre outras técnicas, a IA tem utilizado muito o aprendizado de máquinas (*machine learning*), cuja denominação tem como fundamento a ideia central da alimentação das máquinas computacionais com dados (AGRAWAL; GANS; GOLDFARB, 2019).

O "algoritmo é um conjunto de instruções matemáticas, uma sequência de tarefas para alcançar um resultado esperado e um tempo limitado" (KAUFMAN, 2019, p. 34). Por sua vez, o aprendizado de máquina (*machine learning*) é considerado uma ciência multidisciplinar, que possui como objetivo o desenvolvimento de técnicas computacionais que simulem o comportamento e a inteligência humana em diversas atividades (GOLDSCHMIDT, 2010).

A aprendizagem automática basicamente pode ser supervisionada ou não supervisionada. A aprendizagem de máquina supervisionada usa um conjunto de dados rotulados, cuja abordagem de aprendizado decorre de operação de coleta de dados e uso de diversas técnicas para identificar padrões e correlações entre esses dados (DELUA, 2021). Isso é aprimorado por previsões iterativas que permitem o ajustamento para uma resposta correta após a identificação de um modelo que fornece a relação preditiva mais forte entre entradas e saídas (YEUNG, 2017).

Por sua vez, no aprendizado não supervisionado ocorre a análise e agrupamento de conjuntos de dados não rotulados, porquanto os algoritmos investigam padrões ocultos nos dados sem a necessidade de "supervisão" humana, tendo como objetivo obter insights de grandes volumes de novos dados (DELUA, 2021). Esse último modelo, embora possa lidar com um número maior de dados, revela-se menos transparente. Contudo, ambos os métodos, supervisionados ou

[9] "Os algoritmos são basicamente um conjunto de instruções para realizar uma tarefa, produzindo um resultado final a partir de algum ponto de partida. Atualmente, os algoritmos embarcados em sistemas e dispositivos eletrônicos são incumbidos cada vez mais de decisões, avaliações e análises que têm impactos concretos em nossas vidas." (DONEDA; ALMEIDA, 2016, p. 01).

não, envolvem a falta de previsibilidade e transparência necessárias para que sejam considerados sistemas confiáveis e auditáveis.

Portanto, observa-se que a identificação do reconhecimento de padrões e a realização de correlações dos dados coletados é fundamental para a eficácia do aprendizado de máquina. A decisão automatizada pelos algoritmos, por sua vez, decorre de um produto de treinamento dos algoritmos através da análise de uma quantidade expressiva de dados (CORTIZ, 2020).

De forma didática Ajay Agrawal, Joshua Gans e Avi Goldfarb apresentam a anatomia de uma decisão (que pode ser levada em conta para análise de sistemas automatizados de decisão):

> Quando alguém (ou algo) toma uma decisão, usa os *dados de entrada* do mundo, que possibilitam uma *predição*. Essa predição é possível porque ocorreu um *treinamento* sobre as relações entre os diferentes tipos de dados e sobre quais se associam mais intimamente a uma situação. Combinando a predição com o *julgamento* sobre o que importa, o tomador de decisão então escolhe uma *ação*. A ação leva a um resultado (com uma recompensa ou compensação associada). O *resultado* é uma consequência da decisão. Ele é necessário para fornecer uma imagem completa. O resultado também fornece *feedback* para ajudar a melhorar a próxima predição. (AGRAWAL; GANS; GOLDFARB, 2019, p. 74)

Nesse contexto, a lógica subjacente da mediação algorítmica baseia-se na coleta de dados primários e metadados fornecidos em grande quantidade e administrados por estruturas automatizadas. Ademais, conforme pondera Morozov (2014), é o *feedback* constante em tempo real dos usuários de artefatos tecnológicos que permite que o sistema aprimore seus mecanismos de funcionamento. Acerca da regulação algorítmica em funcionamento, o referido autor esclarece que:

> Para ver a regulação algorítmica em funcionamento, basta olhar para o filtro de *spam* em seu e-mail. Em vez de se limitar a uma definição restrita de *spam*, o filtro de e-mail faz com que seus usuários o ensinem. Mesmo o Google não pode escrever regras para cobrir todas as inovações engenhosas de *spammers* profissionais. O que ele pode fazer, entretanto, é ensinar ao sistema o que constitui uma boa regra e identificar quando é hora de encontrar outra regra para encontrar uma boa regra - e assim por diante. (MOROZOV, 2014, p. 3-4)

Com efeito, é possível observar que o julgamento de decisões para várias atividades foi delegada à máquina e a experiência humana passou a constituir a matéria-prima para os sistemas automatizados de decisão que começam a fazer

parte da engrenagem social em diversos âmbitos, seja para fins de avaliações educacionais, nas campanhas políticas, na seleção de beneficiários de serviços sociais, na seleção de candidatos a empregos ou, até mesmo, na implementação de novos mecanismos na segurança pública, como policiamento preditivo ou ferramentas auxiliares na aplicação da justiça criminal.

A assunção dessa posição central nos processos de conhecimento e na gestão da realidade dos indivíduos é cunhada de racionalidade algorítmica por Fernanda Bruno (2019). A referida expressão consiste em um modelo caracterizado pela mediação das experiências dos indivíduos através de processos algorítmicos que passam a ser atores decisivos na captura e análise de dados sobre uma série de setores da vida em sociedade, gerindo, inclusive, aspectos pessoais da vida dos indivíduos e nas conduções de suas experiências individuais (BRUNO, 2019).

Dentro dessa perspectiva, serão abordados alguns problemas relacionados à mecânica e ao funcionamento dos sistemas automatizados de decisão que reforçam a necessidade de transparência e responsabilidade por parte dos controladores de dados, especialmente relacionados aos vieses discriminatórios e a opacidade dos sistemas que empregam aprendizado de máquina.

2.3 RISCOS DOS SISTEMAS AUTOMATIZADOS DE DECISÃO

O avanço da tecnologia e o advento da big data permitiram a ampliação do uso de sistemas automatizados de decisão nos meios sociais. Diante disso, vive-se em um mundo em que os algoritmos julgam decisões cada vez mais importantes na vida dos indivíduos, sendo utilizados em mecanismos de buscas, de sistemas de revisão online, avaliações educacionais, operações de mercados, a forma como as campanhas políticas são executadas e até a forma como serviços sociais como bem-estar e segurança pública são gerenciados (DIAKOPOULOS, 2017).

Uma questão inicial que deve ser esclarecida no presente trabalho é que as generalizações e inferências são aceitas pela sociedade. Segundo Mattiuzzo (2021), algumas preocupações com algoritmos devem ser reformuladas, tendo em vista que o problema com algoritmos não pode ser o simples ato de generalização. Por sua vez, nos casos em que já existiam generalizações e sua delegação para algoritmos não represente nenhuma novidade, a questão é garantir que os algoritmos apliquem corretamente os critérios adequados ao caso concreto (MATTIUZZO, 2021).

Dentro desse raciocínio, emergem questões ligadas à mecânica e funcionamento dos sistemas algorítmicos relacionados a erros nos dados capturados, tal como amostras tendenciosas que originarão vieses no resultado, correlações enganosas e até mesmo erro de engenharia, tal como um erro na própria codificação, por exemplo (MATTIUZZO, 2021).

O objetivo do presente trabalho não é aprofundar os casos específicos em que não deveria haver a aplicação dos sistemas automatizados de decisão; mas, sim, analisar os mecanismos adequados de regulação para os casos em que os usos dos algoritmos decisórios sejam aceitos. Nos usos em que são aceitos há outros problemas relacionados a eventual viés discriminatório e a ausência de transparência de como o algoritmo chegou a determinado resultado.

Assim, o perfilamento (*profiling*) e a realização de inferências produtos de sistemas que empregam aprendizagem automática são ameaças potenciais à autodeterminação informacional e ao livre desenvolvimento da personalidade e estão nitidamente relacionadas às etapas de tratamento de dados. Para Bart Schermer (2011), os riscos mais significativos associados ao uso de inferências na criação de perfis são: a discriminação, a “desindividualização” e as assimetrias de informação. Além disso, esses problemas são acentuados pela opacidade oriunda do emprego de aprendizado de máquina.

O grande problema de naturalizar a coleta massiva de dados, o consumo personalizado e a predição sobre os comportamentos dos usuários, é que se permite a criação de uma estrutura onde a modelação de comportamentos dos indivíduos passa a ocorrer de forma sutil e obscura. Ademais, o indivíduo preso dentro desse ambiente de controle digital ainda mantém a sensação de ilusão de liberdade.

Por essa razão, torna-se relevante a análise da mediação tecnológica promovida pela governamentalidade algorítmica e os riscos da desindividualização.

2.3.1 Mediação tecnológica promovida pela governamentalidade algorítmica e a “desindividualização”: *profiling* e inferências

Essa nova dinâmica de controle das ações dos indivíduos por meio de diversos dispositivos tecnológicos entra dentro da lógica da “governamentalidade algorítmica”. Para Alves (2019), a referida expressão se trata de uma estratégia de

governo por meio de algoritmos, na qual a condução das condutas dos indivíduos ocorre por meio do emprego de novas tecnologias.

Antoinette Rouvroy e Thomas Berns (2015) denominam por governamentalidade algorítmica “um certo tipo de racionalidade (a)normativa ou (a)política que repousa sobre a coleta, agregação e análise automatizada de dados em quantidade massiva de modo a modelizar, antecipar e afetar, por antecipação, os comportamentos possíveis”. Essa governamentalidade algorítmica, como uma verdadeira prática estatística, estaria decomposta em três etapas: coleta de dados e metadados em tempo real mediante monitoramento (*dataveillance*); tratamento automatizado dos dados (*data mining*), permitindo a correlação entre os dados e a criação de perfis (*profiling*), e a última etapa é a antecipação e predição dos comportamentos individuais associados aos perfis.

Fernanda Bruno (2013) pondera que a vigilância digital reside na coleta e armazenamento de dados móveis (ou circunstanciais) que consistem, dentre outros, em dados comportamentais (comunicação, consumo, deslocamento, lazer), transacionais (uso de cartão de crédito e serviços, navegações em ambientes digitais), psicológicos (declarações sobre personalidade, gosto, interesse) e sociais (comunidades e amigos em ambientes digitais).

Para Zuboff (2018), a big data tem origem no social, sendo um componente fundamental de uma nova lógica de acumulação que ela denomina capitalismo de vigilância, que consiste em prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado. O desejo de acumular dados por um número crescente de empresas compartilha uma lógica semelhante ao do lucro, ou seja, as empresas passam a ser orientadas por dados e isso impulsiona as novas maneiras de fazer negócios e governar, sendo uma questão chave para os grandes *players* econômicos (SADOWSKI, 2019).

Confirmando esse raciocínio, SADOWSKI (2019), ao citar uma publicação da revista “The Economist”, de 2017, pondera que o acúmulo de dados é um componente central da economia política no século XXI. Segundo Sadowski (2019), o extrativismo de dados atua como uma verdadeira forma de capital e que inexiste um *trade-off* justo, o que caracterizaria algo muito similar às explorações realizadas na época das colonizações. Por esse motivo, pode-se falar em um novo modo de colonialismo, um “colonialismo de dados” que se apropria da vida humana e dos

recursos sociais, extraindo informações para o benefício de interesses particulares (MEJIAS; COULDRY, 2019).

Na constatação de Zanatta e Abramovay (2019) os dados abrem três traços inéditos do capitalismo contemporâneo: o primeiro é que os objetos materiais se convertem em formas de captar e transmitir dados; o segundo é a publicidade de precisão, e o terceiro é a capacidade de antecipar os comportamentos dos cidadãos e planejar as atividades econômicas a partir daí. Nesse sentido, Frazão (2019) destaca que o capitalismo de vigilância substitui o mistério por certezas, predições e modificações comportamentais, o que compromete a premissa clássica do mercado como algo intrinsecamente insuscetível de conhecimento.

Após a coleta (ou expropriação) dos rastros digitais dos usuários da internet, há o tratamento automatizado dos dados (*data mining*) que possuem como principal objetivo a realização de inferências e correlações entre as informações obtidas e a criação de perfis (*profiling*). Com a edição dos perfis novos "saberes" são formados pelos algoritmos (através de probabilidades e estatísticas) buscando antecipar os comportamentos e produzir serviços personalizados.

A mineração ("expropriação") de dados (*data mining*) é uma técnica estatística que permite a extração de padrões que geram conhecimento (BRUNO, 2013). Contudo, esse conhecimento extraído segue processos indutivos baseados em algoritmos que extraem padrões e regras de correlação entre elementos, sendo a mais comum o tipo associativo (similaridade) entre pelo menos dois elementos (BRUNO, 2013).

Essa lógica do mercado de dados, baseado na racionalidade econômica, no qual há um *trade off* entre inovação e privacidade, revela a evidente assimetria informacional entre os agentes responsáveis pelo tratamento de dados (FRAZÃO, 2020). Isso dá em razão de um vácuo regulatório convenientemente preenchido pela autorregulação criada pelos grandes players do mercado de dados, no qual os usuários recebem "contrapartidas adequadas" pela extração de seus dados, ou seja, a possibilidade de usufruir determinado bem ou serviço colocado à sua disposição de forma "gratuita". O problema da assimetria informacional está intimamente ligado aos dilemas do consentimento informado como base legal para tratamento de dados[10].

[10] 'Em que pese a indiscutível importância do consentimento em tal cenário, fato é que a maioria dos indivíduos que efetivamente se deparam com a necessidade de renunciar – em algum grau – a seus

Segundo Bart Schermer (2011), a mineração pode ser de dados descritivos, na qual os algoritmos de mineração tentam descobrir determinadas semelhanças entre diferentes objetos e atributos, revelando correlações que podem ensejar *insights* entre objetos de dados em um conjunto de dados. Ademais, “a existência de uma correlação em um conjunto de dados não significa necessariamente que essa relação sempre ocorrerá no mundo real, nem explicar por que a correlação existe”, ou seja, “é vital não confundir correlação com causalidade quando se trata de mineração de dados descritivos” (SCHERMER, 2011, p. 46).

Por sua vez, a mineração também pode ser de dados preditivos, cuja finalidade é fazer uma previsão sobre eventos com base em padrões que foram determinados (SCHERMER, 2011). Assim, ocorre a mineração de informações sobre um indivíduo para determinar se seus dados se encaixam no perfil estabelecido, tal como, por exemplo, “dados demográficos de um conjunto de indivíduos juntos com a anotação que são conhecidos como terroristas” (SCHERMER, 2011, p. 46). Nesse tipo de mineração criam-se classes baseadas nos dados de entrada e diferentes atributos associados à classe, por exemplo, o rótulo de classe “canário” seria composto por atributos como amarelo, bico, asas, cauda, sendo que através desses atributos seria possível determinar uma probabilidade de algo pertencer a uma determinada classe (SCHERMER, 2011).

Sobre a mineração de dados, Barocas e Selbst esclarecem o seguinte:

> Em contraste com aquelas formas tradicionais de análise de dados que simplesmente retornam registros ou estatísticas resumidas em resposta a uma consulta específica, a mineração de dados tenta localizar as relações estatísticas em um conjunto de dados. Em particular, automatiza o processo de descoberta de padrões úteis, revelando regularidades nas quais a tomada de decisões subsequentes pode se basear. O conjunto acumulado de relações descobertas é comumente chamado de "modelo", e estes modelos podem ser empregados para automatizar o processo de classificar entidades ou atividades de interesse, estimar o valor de variáveis não observadas, ou prever resultados futuros. (BAROCAS; SELBST, 2016, p. 677)

---

dados para a utilização de determinado bem ou serviço, irá fazê-lo por desconhecimento dos riscos inerentes a tal ato, ou, simplesmente, por total ausência de poder de barganha com o controlador ou operador, em uma verdadeira estrutura negocial do “tudo ou nada” (*take-it-or-leave-it*).’ (FRAJHOF; MANGETH, 2020, p. 67). Para maior aprofundamento sobre o tema, que não é objeto do presente trabalho, recomenda-se a leitura do seguinte artigo: BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento válido como processo: em busca do consentimento válido. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.) BIONI, Bruno (Coord. executivo). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.

Esse sistema de automatização da descoberta de padrões úteis e na criação de modelos, permite a construção de uma arquitetura de dados que viabilizam a distinção de indivíduos e a etiqueta de qualidades que parecem estatisticamente semelhantes aos padrões encontrados, criando, dessa forma, o perfil. Por isso, é possível afirmar que as ameaças potenciais na criação dos perfis estão relacionadas ao processamento e a mineração dos dados (HILDEBRANDT, 2008).

A criação de perfis é um processo pelo qual se busca descobrir correlações entre dados que podem ser usados para identificar e representar um indivíduo ou grupo, transformando esses dados em conhecimento ou inferências, que, por sua vez, são utilizados para individuar e representar um sujeito ou para identificar um sujeito como membro de um grupo ou categoria, com a construção de prováveis atributos ou comportamentos de uma pessoa (HILDEBRANDT, 2008).

Nesse sentido, o Regulamento Geral sobre Proteção de Dados (RGPD)[11] da União Europeia define perfil (*profiling*) em seu artigo 4º, item 4, a saber:

> Definição de perfis, qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações. (UNIÃO EUROPEIA, 2016)

Nesse sentido, ao interpretar o art. 4º do RGPD e registrar que o processo de definição de perfis pode implicar um conjunto de deduções estatísticas, o extinto Grupo de Trabalho do Artigo 29 (*Working Party article 29* – WP 29)[12] esclarece que o *profiling* "é frequentemente utilizado para efetuar previsões sobre as pessoas, recorrendo a dados provenientes de várias fontes para inferir algo sobre uma pessoa, com base nas qualidades de outras pessoas que, estatisticamente, parecem semelhantes" (*EUROPEAN COMMISSION*, 2017, p. 07).

Segundo Danilo Doneda, na técnica do *profiling*:

---

[11] A *General Data Protection Regulation* (GDPR) passou a ser aplicável a partir de 25 de maio de 2018, em substituição à legislação europeia acerca da proteção de dados (substituiu a Diretiva de Proteção de Dados de 1995 – 95/46/EC). A GDPR foi projetada para: a) harmonizar as leis de privacidade de dados em toda a Europa; b) proteger e capacitar a privacidade de dados de todos os cidadãos da UE, e c) remodelar a maneira como as organizações em toda a região abordam a privacidade dos dados.

[12] O Grupo de Trabalho do Artigo 29 foi criado pela Diretiva 95/46/CE e tratou de questões relacionadas à proteção da privacidade e dos dados pessoais até 25 de maio de 2018, data da entrada em vigor do RGPD. Disponível em: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en.

> [...] os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma "metainformação", que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo. (DONEDA, 2019, pp. 151-152)

Com efeito, "a taxonomia e o conhecimento extraídos dos perfis não revelam características intrínsecas aos indivíduos, mas padrões de conduta e escolha na presença de fatores que constituem uma circunstância" (BRUNO, 2013, p. 160). Portanto, os perfis não produzem uma estrutura informativa específica a um indivíduo identificável, mas são um conjunto de informações que permitem o reconhecimento de um padrão de ocorrência dentro de um conjunto de variáveis.

Por essa razão, Hildebrandt (2008) pondera que os perfis resultantes do *data mining* são aplicados a determinadas pessoas porque seus dados coincidem com o perfil, embora o padrão de ocorrência possa ser decorrente da mineração de dados de outras pessoas. Assim, haveria a construção de perfis e sua aplicação a pessoas cujos dados não foram usados para construir o padrão de ocorrência. Esse reducionismo perde a assimetria de conhecimento entre perfis e perfilados (HILDEBRANDT, 2008).

Fernanda Bruno afirma que os perfis são simulações de identidades, porquanto são padrões estimativos que antecipam potencialidades como preferências, potenciais de consumo, valor econômico potencial, tendências e inclinações comportamentais etc. Por esse motivo, não é difícil imaginar a infinidade de perfis criados pelo uso combinado de procedimentos de rastreamento e mineração de dados (BRUNO, 2013).

Portanto, a criação de perfis e de realização de inferências no tratamento de dados, em sistema automatizados de decisão, pode acarretar o processo denominado de *de-individualisation* ("desindividualização") por Bart Schermer, consistente no "risco de que as pessoas sejam julgadas com base nas características do grupo e não em suas próprias características e méritos individuais" (SCHERMER, 2011, p. 47).

Esse processo de "desindividualização" está relacionado a criação de perfil de grupo (*group profiling*) ou agrupamento (*clustering*). "Os perfis de grupo geralmente contêm estatísticas e, portanto, as características dos perfis de grupo podem ser

válidas para o grupo e para indivíduos como membros desse grupo, embora não para indivíduos como tais" (SCHERMER, 2011, p. 47).

Portanto, no processamento de agrupamento (*clustering processes*) os indivíduos são inseridos em determinadas "categorias" e na maioria das vezes sem a possibilidade de ter ciência do que efetivamente está acontecendo (ROUVROY, 2016). Trata-se de um resultado automático, '"quase natural" do processamento estatístico de "dados", que assumem a aparência de "fatos"' (ROUVROY, 2016, p. 28).

O objetivo dos processos de criação de perfil de grupo (*group profiling*) ou agrupamento (*clustering*) é a formação de "categorias previamente desconhecidas, socialmente e visualmente imperceptíveis com base na análise de dados sem qualquer referência a informações pré-existentes sobre esses novos grupos ou categorias" (ROUVROY, 2016, p. 28). A utilização desses processos está na justificação que o processamento por agrupamento baseado na big data seria "neutro", porquanto ignorariam os processos de categorização humanos, que são inevitavelmente "tendenciosos" em razão da predisposição dos humanos ao perceber o mundo (ROUVROY, 2016).

Contudo, como não há relações sociais pré-existentes, como naquelas formados por uma categorização tradicional, "o sujeito pode ser colocado em grupos que sequer poderia imaginar que fizesse parte, junto a pessoas que nunca imaginou ter algum tipo de relação, alterando sua percepção de pertença social" (HOSNI; MARTINS, 2020, p. 83). Contudo, a grande questão é saber o que esse conhecimento todo pode dizer sobre os indivíduos (BRUNO, 2013).

Segundo Sandra Wachter:

> As plataformas não se importam necessariamente se colocam os usuários com total precisão em determinados grupos; em vez disso, o que importa é se o usuário se comporta de maneira semelhante ao grupo assumido para ser tratado como um membro do grupo [...]. As pessoas serão tratadas de forma diferente com base em sua suposta afinidade, independentemente de essa suposição ser de fato correta. (WACHTER, 2019, p. 21)

Portanto, não há uma preocupação pelos responsáveis de tratamento de dados quanto à precisão da inserção dos indivíduos em determinadas categorizações. Assim, observa-se que a racionalidade econômica de coleta de dados trabalha com uma lógica da máquina que não está preocupada com a

correlação entre verdades ou ideias, provas ou fatos, além de colocar em risco a própria capacidade reflexiva dos sujeitos de pensar por si mesmos.

Nesse contexto, torna-se importante trazer o conceito de inferências trabalhado por Sandra Wachter e Brent Mittelstadt (2019). Para os referidos autores as inferências consistem em previsões não intuitiva e inverificáveis referente aos comportamentos, preferências e informações da vida privada dos indivíduos extraída da análise da big data com o emprego da inteligência artificial. Portanto, as inferências e correlações decorrem dos processos de *data mining* (mineração de dados), consistindo em “informações, opiniões e avaliações” subjetivas e não verificáveis criadas por terceiros por meio de mais do que a mera observação do titular dos dados, porquanto envolve o trabalho de correlação de características não observadas a partir do processo de mineração da análise de dados oriundos da big data (WACHTER; MITTELSTADT, 2019).

No que diz respeito a “não verificabilidade”, os autores fornecem um exemplo para elucidar a sua acepção. Imagine um desenho de uma criança representando sua família e seu humor em relação a eles, tal desenho, embora criado pela criança, pode permitir a extração de inferências a respeito do comportamento dos pais da criança (WACHTER; MITTELSTADT, 2019). Tais inferências não são necessariamente verificáveis e são subjetivas devido à interpretação necessária para derivar as informações sobre o comportamento dos pais (WACHTER; MITTELSTADT, 2019).

Segundo Wachter e Mittelstadt (2019), os métodos de análise inferencial são usados para diversas finalidades, tais como inferir preferências do usuário, atributos confidenciais (como por exemplo, raça, gênero, orientação sexual) e opiniões (como, posições políticas), ou para prever comportamentos (como por exemplo, veicular anúncios de *marketing*). Desse modo, diante das análises da big data há uma habilidade de transformação dos dados, ampliando-se às possibilidades de “extrair, a partir dos dados, correlações, diagnósticos, padrões, inferências e associações” (FRAZÃO, 2019).

Esse grande volume de dados gerados e armazenados permitiu a inovação na capacidade de analisar grandes quantidades de dados (*Big Data analytics*), muitas vezes priorizando correlações em vez de causalidade e, portanto, sacrificando-se a exatidão para se ter acesso a tendências gerais (KAUFMAN, 2019). Desse modo, com a as análises da big data “a causalidade perde espaço

para as correlações” (MENDES, MATTIUZZO; FUJIMOTO, 2021, p. 423). A correlação está nitidamente relacionada a inferências, constituindo-se de uma “probabilidade de um evento ocorrer, caso outro evento também se realize”, portanto, trata-se de uma “relação estatística entre tais acontecimentos” (MENDES, MATTIUZZO; FUJIMOTO, 2021, p. 423).

Benanti (2020, p. 45) pondera que “o ponto em que esses sistemas são particularmente preocupantes é no fato de que os algoritmos de confiança utilizados são injustamente redutivos”, pois “não levam em com conta o contexto” (BENANTI, 2020, p. 45). Dessa forma, o reducionismo provocado pelos sistemas automatizados de decisão apresenta-se como um desafio a ser enfrentado na digitalização do mundo (BENANTI, 2020).

Nesse sentido, Éric Sadin (2019) pondera que a humanidade se dota de um órgão que a despoja de si mesma, de seu direito de decidir, com consciência e responsabilidade, as coisas que lhe dizem respeito. Dentro dessa perspectiva, os indivíduos estão perdendo a capacidade, por vezes tão saudável, de reagir reflexivamente, de exprimir recusa a certos dispositivos, quando esses representam violação da integridade e dignidade dos seres humanos (SADIN, 2019).

Segundo Rouvroy e Berns (2015), a racionalidade que repousa sobre a coleta, agregação e análise automatizada de dados em quantidade massiva de modo a modelizar, antecipar e afetar, por antecipação, os comportamentos possíveis dos indivíduos contorna e evita os sujeitos humanos como seres reflexivos. A governamentalidade algorítmica ‘se alimenta de dados “infraindividuais” insignificantes neles mesmos, para criar modelos de comportamento ou perfis supraindividuais sem jamais interpelar o sujeito, sem jamais convocá-lo a dar-se conta por si mesmo daquilo que ele é, nem daquilo que ele poderia se tornar’ (ROUVROY; BERNS, 2015, p. 42).

Portanto, há uma rarefação dos processos e ocasiões de subjetivação do indivíduo, porquanto as práticas estatísticas se contentam em analisar os cruzamentos de correlações com a big data (ROUVROY; BERNS, 2015). O livre exercício da faculdade de julgamento e ação dos indivíduos são substituídos por protocolos destinados a modificar as ações individuais ou impulsos individuais dentro de uma análise robótica responsável pela formulação instantânea de equações com o objetivo de iniciar as correspondentes trajetórias corretas a seguir (SADIN, 2019).

Nesse ponto, há um perigo da generalização de sistemas automatizados que desconsiderem a autonomia dos indivíduos ou até mesmo os tratem de forma indiferente, de modo que haja um declínio da reflexividade subjetivante e da própria possibilidade de o indivíduo contestar as produções de “saber” fundadas no *data mining* e na elaboração de perfis (ROUVROY; BERNS, 2015).

Diante disso, Paolo Benanti reforça a necessidade de pensar de maneira crítica sobre os algoritmos, porquanto:

> Se os algoritmos são a linfa vital das modernas infraestruturas tecnológicas, se tais infraestruturas modernas modelam e influenciam cada vez mais aspectos das nossas vidas, e se o discernimento e o juízo dos algoritmos de projetos são a chave a ser usada, então é importante que tenhamos a certeza de compreender como funciona esse discernimento e esse juízo. (BENANTI, 2020, p. 78)

Assim, se o emprego de algoritmos é inevitável para a evolução tecnológica, ao menos “devemos entender o que fazer para não perder as nuances que efetivamente não são partes secundárias, mas qualidades essenciais do nosso ser” (BENANTI, 2020, p. 45). Tal reflexão se impõe, pois diante da governamentalidade algorítmica “nossas possibilidades de vida se confundem com os modos de existência que a axiomática submete à nossa escolha” (LAPOUJADE, 2015, p. 268), de modo que a potência de escolher dos indivíduos seria submetida a possíveis condições preestabelecidas, na medida em que “podemos escolher, mas não podemos escolher os termos da escolha” (LAPOUJADE, 2015, p. 268).

Com efeito, a tecnologia não pode ser empregada de forma redutiva, desconsiderando as qualidades dos destinatários dos sistemas automatizados de decisão enquanto sujeitos de direito. Transposta a análise dos riscos relacionados a *de-individualisation* (desindividualização). A partir disso, serão analisados os riscos relacionados a discriminação e opacidade.

2.3.2. Externalidades negativas: vieses discriminatórios e opacidade

A discriminação “é um fenômeno comumente descrito como o ato de segmentar uma pessoa de um conjunto por causa de seu gênero, sua condição social, sua orientação sexual ou de outros fatores”, ou ainda a “exclusão de um indivíduo de um grupo de forma não justificada” (MATTIUZO, 2020, p. 117). Assim,

considerando que a categorização dos indivíduos em classificações está no centro da mineração de dados preditiva (SCHERMER, 2011), os algoritmos tendem a perpetuar injustiças, preconceitos e discriminações (AGRAWAL; GANS; GOLDFARB, 2019).

Segundo Hildebrandt (2019) um novo tipo de pensamento mágico tomou conta do imaginário do público quando envolve o tema sobre inteligência artificial, bem como pondera que é falho supor que a vida real possa ser traduzida adequadamente em dados legíveis por máquina, ainda que tal tradução possa gerar maior eficácia e ampliar as maneiras produtivas. Ademais, suposições behavioristas de aprendizagem mecânica levam consigo preocupações quanto ao impacto na identidade humana em relação à privacidade (HILDEBRANDT, 2019).

Com efeito, o algoritmo visto de uma abordagem técnica permite uma convicção generalizada que a sua atuação no mundo material é estritamente objetiva. Contudo, os referidos casos práticos demonstram que os resultados de muitos algoritmos refletem atitudes e comportamentos humanos. “A questão, no entanto, é se de fato eliminamos o viés humano ou simplesmente o camuflamos com tecnologia” (O’NEIL, 2020, p. 40).

Na literatura que aborda as preocupações referentes à automação da tomada de decisão humana, o emprego do termo “viés”[13] é aplicado com uma importância de valor moral, ou seja, o termo viés é utilizado para se referir a sistemas informáticos que discriminam de forma injusta certos indivíduos ou grupos de indivíduos em favor de outros. Nesse ponto, Burrel (2016) afirma que a suposta vantagem do algoritmo de ser mais objetivo que o ser humano, em razão de evitar inadequações ou injustiças, não pode simplesmente ser tomada pelo valor nominal. Isso se justifica porque se deve assumir que ainda há uma margem razoável de julgamento humano envolvido no projeto dos algoritmos e, portanto, há sim escolhas que se incorporam nos recursos e dados de treinamento ajustados na programação (BURREL, 2016).

No ponto do viés técnico, Selbst e Barocas (2018) explicam que a mineração de dados, muitas vezes utilizada em sistemas que empregam aprendizado de máquina, pode ser um fator crucial para o desenvolvimento de um algoritmo

[13] Friedman e Nissenbaum (1996), ao abordarem o tema do “viés em sistemas de computação”, desenvolvem três categorias sobre o tema: a) viés preexistente, que teria raízes em instituições sociais; b) viés técnico que surgiria a partir de restrições técnicas, e; c) viés emergentes surgiria no contexto de uso.

tendencioso. O objetivo da mineração de dados é fornecer uma base racional, tentando localizar relacionamentos estatísticos em um conjunto de dados. Assim, como a mineração de dados aprende pelo exemplo, o que um modelo aprende depende dos exemplos aos quais foi exposto. Os dados que funcionam como exemplos são conhecidos como “dados de treinamento”, ou seja, são os dados que treinam o modelo para se comportar de uma certa maneira e, portanto, os dados tendenciosos de treinamento levam a modelos discriminatórios (SELBST; BAROCAS, 2018).

Ao abordar o poder social dos algoritmos, Beer (2017) reforça que a incerteza sobre algoritmo pode nos levar a julgar mal seu poder, enfatizar excessivamente sua importância, conceber erroneamente o algoritmo como um ator independente isolado. O referido sociólogo (2017) destaca que desconectar o algoritmo do mundo social e vê-lo somente como um objeto técnico e independente que existe como presença distinta provavelmente será um erro.

Seguindo esse mesmo raciocínio, Kicthin (2017) registra que os algoritmos não podem ser divorciados das condições em que são desenvolvidos e implantados, ou seja, os algoritmos precisam ser entendidos como relacionais, contingentes, contextuais por natureza, enquadrados no contexto mais amplo de sua montagem sociotécnica. O que significa que o algoritmo não pode ser subestimado como uma forma técnica, objetiva, imparcial de conhecimento ou modo de operação, porquanto eles moldam como os indivíduos passam a entender o mundo (KICTHIN, 2017).

Ainda sobre o tema, o referido autor pondera que:

> Assim como os algoritmos não são expressões neutras e imparciais de conhecimento, seu trabalho não é impassível e apolítico. Algoritmos buscam, cotejam, ordenam, classificam, agrupam, analisam, criam perfis, modelam, simulam, visualizam e regulam pessoas, processos e lugares. Eles moldam como entendemos o mundo e fazem o mundo através da sua execução como software, com profundas consequências. Neste sentido, eles são profundamente performativos como eles fazem as coisas acontecerem. (KICTHIN, 2017, p. 18)

Desse modo, considerando que os algoritmos não são necessariamente neutros e podem ser desenvolvidos de forma tendenciosa, torna-se importante buscar diretrizes a respeito de quais fatores criam ambientes propícios para o surgimento desses algoritmos preconceituosos. Em uma análise panorâmica pode-se afirmar que existem vários cenários relacionados diretamente com a qualidade

dos dados, além de falhas nas metodologias estatísticas ou interpretação de resultados.

2.3.2.1 Vieses discriminatórios

Para Sandra Wachter e Brent Mittelstadt (2019, p. 01), as inferências “se baseiam em dados altamente diversos e ricos em recursos de valor imprevisível e criam novas oportunidades para perfis e tomadas de decisão discriminatórios, tendenciosos e invasores de privacidade”. Portanto, a discriminação torna-se uma externalidade negativa nos sistemas automatizados de decisão quando, mesmo sem desejo prévio de julgar as pessoas com base em características particulares, tais como etnia, gênero, religião ou preferência sexual, o algoritmo ao processar os dados, acaba de forma inadvertida discriminando determinados indivíduos ou grupos.

Tal fato geralmente ocorre quando se verifica uma base de dados tendenciosos usados para treinar o algoritmo no aprendizado de máquina, contudo, o presente trabalho propõe uma sistematização da discriminação algorítmica como uma das formas de viabilizar a construção de mecanismos de governança eficazes na promoção de uma *accountability*. Assim, para fins de sistematização dos casos que podem apresentar discriminação algorítmica, torna-se imperioso trazer alguns apontamentos desenvolvidos na doutrina nacional.

Segundo Maria Cristine Lindoso (2022), o viés associado aos dados possui dois desdobramentos que se externalizam nas possibilidades de discriminação algorítmica como consequência: a) do uso de dados e bases de dados, e b) da manipulação do algoritmo. Em relação ao primeiro ponto, a autora (2022) afirma que podem ocorrer quando: i) os dados não são suficientemente representativos; ii) os dados refletem comportamentos pretéritos que já são considerados discriminatórios – e que serão repetidos, naturalmente, pelos algoritmos; iii) pela falta de cuidado no uso de dados pessoais sensíveis, e iv) pela anonimização de dados pessoais que pode acabar sendo revertida pela leitura do algoritmo.

Por sua vez, em relação ao segundo desdobramento da discriminação algorítmica ela poderá estar presente quando: i) o desenho algorítmico, que pode prestigiar ou prejudicar, de forma injustificada, grupos específicos; ii) o modelo de treinamento do algoritmo acaba sendo ensinado a produzir *outputs* discriminatórios,

e iii) as correlações e inferências produzidas no processo de leitura dos dados apresentam resultados não condizentes com a realidade ou injustificadamente prejudiciais para determinados grupos (LINDOSO, 2022).

Seguindo o mesmo raciocínio, Laura Schertel Mendes, Marcela Mattiuzzo e Mônica Tiemy Fujimoto (2021) ponderam que a “discriminação algorítmica” pode englobar dois cenários importantes. O primeiro envolve afirmações estatisticamente inconsistentes e o segundo há uma classificação consistente sob o ponto de vista estatístico, contudo, essa classificação se mostra injusta (MENDES, MATTIUZZO, FUJIMOTO, 2021). Dentro dessa concepção, as autoras apontam quatro tipos de discriminação: i) discriminação por erro estatístico; ii) discriminação pelo uso de dados sensíveis; iii) discriminação por generalização injusta (correlação abusiva), e iv) discriminação limitadora do exercício de direitos.

Assim, na busca de harmonizar os apontamentos realizados sobre a discriminação algorítmica, o presente trabalho seguirá a construção apresentada por Mendes, Mattiuzzo e Fujimoto, com as adaptações necessárias decorrente das contribuições fornecidas por Maria Cristine Lindoso, bem como tentará combinar com as diretrizes legais constantes no inciso IX do art. 6º que prevê o princípio da não discriminação.

Partindo disso, a “discriminação por erro estatístico” pode abranger tanto dados incorretamente coletados, como problemas no código do algoritmo – por exemplo, erros na rotulagem da base de dados que antecede o aprendizado supervisionado e na própria geração de dados (KAUFMAN, 2021). No que diz respeito a esse último ponto, será melhor explorado mais a frente dentro do contexto da opacidade dos sistemas automatizados de decisão.

Referente ao primeiro ponto (coleta incorreta dos dados), este pode envolver: i) a coleta de dados que não sejam suficientemente representativos – que não representem a composição proporcional do universo objeto em questão (KAUFMAN, 2021; FRAZÃO, 2021b), e ii) dados que refletem os preconceitos na sociedade (KAUFMAN, 2021; FRAZÃO, 2021b).

Nesse sentido, em 2014 a equipe da Amazon começou a desenvolver programas com o objetivo de mecanizar a análise dos currículos dos candidatos a empregos (DASTIN, 2018). A ferramenta de contratação experimental da empresa usou inteligência artificial para dar aos candidatos pontuações. Contudo, em 2015 a Amazon percebeu que seu novo sistema não estava classificando candidatos para o

trabalho de forma neutra em termos de gênero. O sistema estava rebaixando os currículos dos candidatos que incluíssem a palavra “feminino”. Isso ocorreu porque os algoritmos foram treinados observando os padrões dos currículos enviados à empresa por um período de 10 anos anteriores, ou seja, a maioria veio de homens, diante do domínio masculino em toda a indústria de tecnologia.

Após descobrir esse viés discriminatório, os engenheiros tentaram apresentar uma solução, direcionando o sistema para tratar “feminino” de forma neutra. Contudo, a empresa acabou cancelando os estudos do projeto, porquanto os executivos teriam perdido as esperanças em corrigir o problema (DASTIN, 2018). No referido exemplo, há uma contextualização clara dos efeitos nocivos da coleta incorreta de dados como fonte de discriminação por erro estatístico, o que no caso em tela abrange tanto a ausência de dados representativos como revela o preconceito pré-existente no contexto social.

A falta de representatividade está intrinsecamente relacionada à ausência de informações suficientes relevantes sobre o contexto das mulheres, o que sem dúvida conduz que os sistemas automatizados de decisão promovam a discriminação de gênero em processos decisórios. Portanto, “se não existem dados suficientes produzidos sobre as mulheres, dificilmente as decisões automatizadas conseguirão compreender a realidade feminina de forma inclusiva e não discriminatória” (LINDOSO, 2021, p. 119)

Ademais, além da ausência de representatividade nos dados, o uso de dados históricos da empresa reforçou os vieses preexistentes decorrentes das construções anteriores à tentativa do desenvolvimento do sistema automatizado de decisão.

Nesse sentido, Maria Lindoso pondera sobre os perigos contidos na utilização de dados históricos, utilizados como *inputs* para a estruturação do aprendizado de máquina, que pode representar o emprego de dados contaminados com vieses discriminatórios:

> Nessa perspectiva, o uso de dados que reflete realidades pretéritas consegue estrutura as duas presunções do modelo utilizado pelo algoritmo para que ele possa funcionar. Uma análise preditiva automatizada sempre envolve a inserção, na base de dados, de informações que possam retratar o passado, servindo como inputs para os algoritmos compreenderem a formação de um modelo específico.
> Ocorre que os dados históricos podem guardar, de forma inerente aos desejos do programador, os preconceitos e vieses de gênero de uma determinada realidade, o que também causa impacto no resultado final do processo decisório. Isso ocorre porque, se um contexto passado for

> discriminatório, os dados irão carregar essa informação e transportá-la para o processo automatizado. (LINDOSO, 2021, pp. 125-126)

Desse modo, se houver a utilização de dados de treinamento que captem um viés de gênero, por exemplo, haverá a construção de um modelo discriminatório que poderá ensejar o desenvolvimento de softwares tendenciosos. Assim, ainda que o uso dos algoritmos nos processos de recrutamento tenha o potencial de melhorar os resultados das atividades empresariais e minimizar as discriminações humanas na seleção de candidatos, deve-se observar que muitas vezes quando se recorre ao uso de ferramentas como essas, mais difícil pode se tornar para que os candidatos "fora dos padrões" consigam obter êxito no mercado de trabalho (MENDES; MATTIUZZO; FUJIMOTO, 2021).

Desse modo, os problemas relacionados a discriminação em sistemas automatizados de decisão envolvendo o emprego de inferências e criação de perfis está intimamente conectado com "discriminação por erro estatístico". Nesse viés, torna-se importante observar, quando se fala em inferências e correlações, nem sempre as inferências serão verdadeiras, pois podem presumir informações que não existem ou podem realizar uma associação de padrões e informações não necessariamente verdadeira conforme a qualidade da coleta e uso de dados no treinamento dos modelos de aprendizado de máquina.

Diante disso, pode-se afirmar que as informações estatisticamente incorretas geram discriminação e devem ser considerado um tratamento ilícito de acordo com uma interpretação teológica da LGPD.

Segundo MATTIUZZO (2020):

> "[...] a ilicitude decorreria não de uma determinação legal expressa, mas da compreensão de que é inerentemente errado discriminar com base em dados que não refletem a realidade. Assim, nesse tipo de caso, seria necessária alguma avaliação que buscasse verificar se o algoritmo que empreendeu a análise foi programado com algum erro, por exemplo, ou se a base de dados analisada é na origem enviesada." (MATTIUZZO, 2020, p. 122)

Ademais, as correlações imperfeitas ou enganosas podem ocasionar a exclusão ou lesão de direitos dos destinatários desses sistemas automatizados de decisão, colocando em risco o livre desenvolvimento da personalidade (art. 2º, VII,

da LGPD) e o princípio da autodeterminação informativa[14] (art. 2º, II, da LGPD). Portanto, de certo modo, a "discriminação por erro estatístico" está relacionada a discriminação por generalização injusta e limitadora do exercício de direitos também, situações que reforçariam à presença da discriminação além da própria inadequação no tratamento dos dados.

Não obstante isso, ainda que as discriminações sejam estatisticamente corretas, podem representar um problema do ponto de vista jurídico, especialmente quando impuserem aos indivíduos limitações injustificadas ao exercício de direitos (MATTIUZZO, 2020). A partir disso, é possível abordar a "discriminação por generalização injusta" e a "discriminação limitadora do exercício de direitos", o que será analisada em combinação com intepretações extraídas do texto legal LGPD.

Os problemas relacionados a discriminação algorítmica e a desindividualização (tema abordado na seção anterior) são enfrentados pelo princípio da não discriminação previsto no art. 6º, inciso IX, da LGPD. No referido dispositivo é consagrado que não é possível a realização de tratamento para fins discriminatórios ilícitos ou abusivos. Portanto, uma compreensão adequada do princípio da não discriminação demanda a análise do que poderia ser considerado um tratamento de dados ilícito ou abusivo.

Segundo Marcela Mattiuzzo (2020, p. 121), "a ideia de ilicitude remete àquilo que o ordenamento jurídico define como proibido". Conforme já foi visto, a discriminação por erro estatístico é um tratamento de dados ilícito. Contudo, impõe-se registrar que essa proibição independe de um debate sobre a correção estatística da generalização, ou seja, a proibição pode existir ainda que estatisticamente a informação seja precisa MATTIUZZO (2020).

A exemplo disso, seria a vedação por lei (inciso II do §3º do art. 3º da Lei 12.414/2011 – Lei do Cadastro Positivo)[15] da utilização de dados pessoais sensíveis

[14] A delimitação conceitual e abrangência desses termos será desenvolvida no segundo capítulo do presente trabalho.

[15]'Apesar da LGPD ter trazido um conteúdo ampliado de dados pessoais sensíveis – referindo-se tanto a aspectos existenciais, como sociais – o seu tratamento jurídico já é conhecido da legislação brasileira desde a promulgação da Lei de Cadastro Positivo – Lei nº 12.414/11 – que, em seu artigo 3º, §3º, II, proíbe anotações em bancos de dados usados para análise de crédito de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" Significa dizer que para fins de análise de concessão de crédito – fundamentado no princípio da finalidade – estão vedadas inclusões nas bases de dados de quaisquer informações de natureza personalíssima e que não se relacione à finalidade almejada com a análise de crédito, com o objetivo de evitar o tratamento discriminatório – fundamento no princípio da não discriminação.' (MULHOLLAND, Caitlin. O

(pertinentes à origem social e étnica, saúde, orientação sexual, convicções políticas, religiosas e filosóficas etc.) para formar o histórico de crédito mais completo sobre um indivíduo e fornecer elementos para fins de correlações a respeito da capacidade de pagamento daquela pessoa (MATTIUZZO, 2020). Portanto, ainda que o sistema produza um resultado estatístico correto, a própria legislação entende que seu uso é proibido, portanto, ilícito.

Nesse viés, deve-se observar que a discriminação na formação de perfis e a realização de inferências não está limitada apenas aos dados sensíveis[16], que pela LGPD referem-se a dados pessoais "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II). Na verdade, a limitação para o tratamento de dados é muito mais ampla, porquanto "até mesmo dados que não são qualificados na LGPD como sensíveis podem transformar-se em sensíveis se submetidos a um determinado tratamento, revelando aspecto da personalidade de uma pessoa, que por sua vez, poderia levar a práticas de natureza discriminatória" (MULHOLLAND, 2020, p. 123).

A discriminação pela generalização injusta "é constatada em todo tipo de discriminação estatística", isso porque "o tratamento diferenciado de determinado grupo, sem que sejam levadas em conta as características e condições individuais, é a própria definição da discriminação algorítmica" (MENDES; MATTIUZZO;

---

tratamento de dados pessoais sensíveis. *In*: MULHOLLAND (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, pp. 121-122).

[16] Essa interpretação ampliada de dados sensíveis decorre da complexidade de se estabelecer um conceito seguro a respeito do tema, o que conforme será exposto no segundo capítulo do presente trabalho, deve ser analisado dentro de uma conceção expansionista, merecendo tutela da LGPD toda informação que direta ou indiretamente, identifica um sujeito, abrangendo também informações com o potencial de identificação (BIONI, 2019). Corroborando esse raciocínio, o WP 29 afirma que a proteção de dados deve ter como base uma percepção ampla do conceito de "dados pessoais" tendo em vista que merecem proteção não apenas dados que contêm informações sensíveis, mas também dados a partir dos quais podem ser concluídas informações sensíveis relativas a um indivíduo (*EUROPEAN COMMISSION*, 2011). Além disso, a criação de perfis pode transformar dados comuns em dados sensíveis a partir da combinação e transformação de dados decorrentes do emprego de metodologias de análises inferenciais e correlações (*EUROPEAN COMMISSION*, 2017). O exemplo mais comum disso é na área da publicidade direcionada. No início de maio de 2017, um jornal australiano (*The Australian*) teve acesso a um documento confidencial preparado pelo Facebook que revelou que a empresa ofereceu para um anunciante em potencial a capacidade de micro segmentar anúncios para atingir 6,4 milhões de adolescentes durante momentos de vulnerabilidade psicológica, quando estes se sentissem "inseguros", "ansiosos" ou "fracassados" (TIKU, 2017). Para maiores informações recomenda-se a leitura de Fernanda Bruno et al., denominado "Economia psíquica dos algoritmos e laboratório de plataforma: mercado, ciência e modulação do comportamento", disponível em: http://dx.doi.org/10.15448/1980-3729.2019.3.33095.

FUJIMOTO, 2021, p. 439). Como foi exposto na seção anterior, as análises da big data sacrificam a exatidão para ter acesso a tendências gerais, substituindo-se a causalidade pelas correlações.

Por sua vez, as correlações estatísticas podem ocasionar uma seletividade arbitrária das informações, pois em razão da aleatoriedade ou ausência de causalidade entre o input e o output, é possível a realização de cálculo estatístico totalmente desprovido de relação com a situação fática analisada pelo algoritmo (MENDES; MATTIUZZO; FUJIMOTO, 2021). Ademais, essa espécie de discriminação algorítmica tende a ser acentuada no processo de desindividualização relacionado a criação de perfil de grupo (*group profiling*) ou agrupamento (*clustering*), conforme abordado na seção anterior.

Nesse ponto, evidenciam-se sérios riscos de discriminação estatística dos processos algorítmicos, nos quais “o indivíduo é julgado a partir das características do grupo a que pertence, sem qualquer recurso para que possa haver uma individualização” (FRAZÃO, 2021b, p. 02). Desse modo, cria-se um verdadeiro paradoxo no qual um algoritmo processa uma série de estatísticas e fornece uma probabilidade de que determinada pessoa é um terrorista ou uma má contratação, virando a vida de alguém de ponta-cabeça, sem viabilizar mecanismos que permitam uma efetiva contraposição das evidências matemática puramente sugestivas (O’NEIL, 2020).

Assim, fica evidente como a correlação estatística, desprendida de causalidade, pode trazer grandes prejuízos aos titulares de dados. Além disso, a discriminação pela generalização injusta está intrinsecamente relacionada à discriminação limitadora do exercício de direitos. Não é por outro motivo, que Mendes, Mattiuzzo e Fujimoto (2021, p. 441) afirmam que essa última “é uma espécie da discriminação injusta (correlação abusiva), uma vez que utiliza como proxy para determinada correlação ou generalização um dado referente ao exercício de um direito”.

Um exemplo desse tipo de correlação abusiva pode ser retirada do estudo realizado, em 2019, pelo *Royal United Services Institute* (RUSI), denominado *Data Analytics and Algorithmic: bias in Policing* (Análise de dados e algorítmica: preconceito no policiamento), encomendado pelo Centro de Ética e Inovação de Dados do governo britânico, analisou o uso de sistemas automatizados envolvendo o “mapeamento preventivo de crimes” e na “avaliação de risco individual”, que

frequentemente são denominados de “policiamento preditivo”. O sistema analisado é o “*National Data Analytics Solution*” (NDAS) criado pela West Midlands Police no Reino Unido.

“O NDAS pretende legitimar e apoiar intervenções de policiamento preventivo usando grandes análises de dados e aprendizado de máquina para fazer previsões sobre o futuro potencial das ações dos indivíduos” (*BIG BROTHER WATCH*, 2020, p 11). Para tanto, o NDAS usa dados sobre indivíduos retirados de uma série de fontes públicas e privadas (*BIG BROTHER WATCH*, 2020).

O estudo abordou o viés no que se refere a: i) resultados ou processos que são sistematicamente menos favoráveis a indivíduos dentro de um determinado grupo onde não há justificativa para tal diferença, criando assim novos grupos-alvo não necessariamente vinculadas a características protegidas (dados sensíveis); ii) discriminação direta ou indireta com base em características protegidas (dados sensíveis), e; iii) desvio real ou aparente do processo de tomada de decisão de tal forma que seja ou possa parecer injusto (BABUTA; OSWALD, 2019).

No documento informativo há o registro que os algoritmos treinados em dados policiais podem replicar (e em alguns casos amplificar) os preconceitos existentes inerentes ao conjunto de dados. A exemplo disso, restou consignado que “os indivíduos de origens sociodemográficas desfavorecidas tendem a se envolver com os serviços públicos com mais frequência, o que significa que a polícia geralmente tem acesso a mais dados relacionados a esses indivíduos, o que pode, por sua vez, levá-los a serem caracterizados como de maior risco” (BABUTA; OSWALD, 2019, p. 12).

De igual modo, o estudo apontou que o uso de algoritmos preditivos pode resultar na desconsideração de informações contextuais importantes, o que pode introduzir um viés sistemático na cadeia de tomada de decisão em um esforço para “simplificar” o processo. A título de exemplo, “uma decisão sobre a detenção pós-prisão com base em uma saída preditiva pode ser distorcida se o algoritmo usar apenas dados que confirmem o risco em vez de dados que demonstrem o contrário” (BABUTA; OSWALD, 2019). Além disso, há o risco do viés da automação, no qual o operador humano tende a confiar mais em resultados automatizados, desconsiderando outras informações corretas e relevantes (BABUTA; OSWALD, 2019).

A organização de liberdades civis denominada *Big Brother Wacth, ao apresentar dados da própria* West Midlands Police, registrou que “em abril de 2019, foi relatado que os negros eram 5 vezes mais propensos do que os brancos a serem parados e revistados na área da polícia de West Midlands, enquanto os asiáticos eram 2,8 vezes mais propensos” (*BIG BROTHER WATCH*, 2020, p. 13). Reforçando a verificação desses problemas de vieses discriminatórios do sistema policial britânico, um estudante negro de 14 anos acusou a polícia metropolitana de Londres de ataques racistas, após afirmar que foi parado pela polícia acerca de 30 vezes nos últimos dois anos (TAYLOR, 2021). Em relato à revista *The Guardian* ele afirmou que foi parado inclusive quando saiu do apartamento para tão somente levar o lixo para sua mãe, sendo que em muitas oportunidades é algemado e revistado.

No mesmo sentido, Cathy O’Neil ao analisar sistemas de policiamento preditivo utilizados nas delegacias norte-americanas (tal como o software da empresa PredPol ou similares como o ComStat e o HunchLab) relata que essas tecnologias criam um ciclo nocivo de feedback, pois ao usarem critérios de georreferenciamento para “mapear” as áreas mais propensas a prática de delitos, reforçam vieses discriminatórios, com envio de recursos policias geralmente aos bairros mais empobrecidos, cuja prática de crimes é mais endêmica, especialmente a depender da estratégia da configuração dos sistemas. Esse ciclo nocivo de feedback é agravado quando os sistemas são novamente alimentados com dados dos registros de crimes nas referidas localidades mais pobres, que na maioria das vezes concentra populações negras ou hispânicas.

Desse modo, a exemplo desse ciclo nocivo de feedback o policiamento preditivo acaba se concentrando de forma desproporcional em bairros com maior índice de população negra e de minorias étnicas, demonstrando de forma clara que as correlações abusivas podem representar tanto uma discriminação pela generalização injusta, como pela limitação do exercício de direitos. Além disso, numerosas aplicações de análise de big data para fazer inferências e criar perfis demonstram-se potencialmente violadoras das liberdades e direitos fundamentais, em especial quando o algoritmo apresenta vieses discriminatórios.

Outro exemplo preocupante, pode ser extraído de uma pesquisa da Universidade de Stanford (conhecida como “*AI gaydar*”), organizada pelos pesquisadores Michal Kosinski e Yilun Wang, na qual houve a utilização de um sistema matemático sofisticado que, em tese, teria aprendido a analisar recursos

visuais com base em um grande conjunto de dados, através da seleção de milhares de fotografias de plataformas de namoro com intuito de extrair características faciais dos usuários. Nesse contexto, desenvolveu-se um algoritmo que poderia distinguir homossexuais e heterossexuais com um percentual acima de 80% (LEWIS, 2018).

O estudo, por sugerir que a IA poderia ser usada para detectar a orientação sexual, atraiu a atenção de diversos críticos. Em respostas a questionamentos realizados por dois grupos LGBTQ líderes, a *Human Rights Campaign* e GLAAD, os pesquisadores Kosinski e Wang, acabaram assumindo que havia uma correlação em que as pessoas disseram que estavam procurando por parceiros do mesmo sexo eram homossexuais (BURDICK, 2017). Ademais, alguns cientistas criticaram o estudo por motivos metodológicos, argumentando que os pesquisadores teriam usado um conjunto de dados falho, porquanto além de todos serem brancos, os usuários do site de namoro poderiam estar tendenciosos a demonstrar suas propensões sexuais de uma forma que seus pares na população geral não faziam (BURDICK, 2017).

A referida pesquisa levantou questões sobre as origens biológicas da orientação sexual, a ética da tecnologia de detecção facial e o potencial desse tipo de tecnologia violar a privacidade das pessoas ou ser utilizado para perseguir homossexuais em países, a exemplo daqueles em que homossexualidade é punível com pena de morte, tais como Irã e Arábia Saudita (LEWIS, 2018). Diante das críticas, os desenvolvedores afirmaram que a motivação inicial do *AI gaydar* era proteger os homossexuais, contudo, a iniciativa foi vista como potencial ameaça à privacidade e segurança, desencadeando protestos e cancelando a continuidade do projeto (LEWIS, 2018).

Esse último exemplo, reforça que a combinação de dados realizada pelos processos de mineração da big data podem gerar novos dados com potencial de impactar de forma significativa na autodeterminação informacional e no livre desenvolvimento da personalidade. No caso em tela houve a utilização de dados sensíveis (coleta de informações biométricas) para a produção de inferências que também podem ser enquadradas como dados sensíveis (orientação sexual) e que merecem maior proteção da lei.

Ademais, a tecnologia empregada criou uma discriminação com alto grau de individualização, explorando de forma indevida as fragilidades e vulnerabilidades de características que carregam estereótipos discriminatórios, ao permitir a utilização

de ferramentas tecnológicas que podem limitar de forma abusiva o exercício de direitos dos destinatários dos sistemas, especialmente quando empregados em países que criminalizam a homossexualidade.

Segundo Caitlin Mulholland (2020, p. 124), “o princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam inequitativos”. Por essa razão é possível atrelar o princípio da não discriminação ao princípio da equidade defendido pela Comissão Europeia[17].

A equidade é um conceito que os indivíduos são capazes de entender a um nível intuitivo, refletindo a apreciação de uma situação baseada em um conjunto de valores sociais, como a promoção da igualdade na sociedade (*KOENE*, *et al.*, 2019). Portanto, através do princípio da equidade é perfeitamente possível realizar um controle sobre a abusividade na realização de inferências ou criação de perfis que resultem em limitações injustificadas ao exercício de direitos por parte dos destinatários dos sistemas automatizados de decisão.

Através do princípio da equidade é possível apreciar os efeitos sociais dos algoritmos nas estruturas sociotécnicas e o enquadramento das ações e consequências nos valores sociais (*KOENE*, *et al.*, 2019). Trata-se da análise da equidade numa dimensão substantiva, que implica um compromisso com “a garantia de uma distribuição equitativa e justa dos benefícios e dos custos, bem como de inexistência enviesamentos injustos, discriminação e estigmatização contra pessoas e grupos” (*EUROPEAN COMMISSION*, 2019, p. 18).

Por essa razão que o Grupo de Especialistas de Alto Nível em Inteligência Artificial da Comissão Europeia propõe uma atuação preventiva para o enfrentamento dos enviesamentos injustos[18], com a adoção de processos de supervisão para analisar e abordar “a finalidade, os condicionalismos, os requisitos e as decisões do sistema de forma clara e transparente”, bem como com “o recrutamento de pessoal de diferentes origens, culturas e disciplinas pode assegurar a diversidade de opiniões e deve ser incentivado”.

---

[17] No documento denominado “Orientações Éticas para uma IA de Confiança” *(Ethic Guidelines For Trustworthy AI*), Grupo de Especialistas de Alto Nível em Inteligência Artificial da Comissão Europeia (*High-Level Expert Groupon Artificial Intelligence* – AI HLEG) defende a implementação de diversos princípios no desenvolvimento de inteligência artificial confiável e auditável, dentre os quais destaca-se o princípio da equidade.

[18] O que será explorado no terceiro capítulo do presente trabalho através da análise da gestão de risco associada a *accountability* algorítmica.

Esses casos práticos reforçam a importância do estabelecimento de mecanismos de *accountability* para o desenvolvimento e a implementação de sistemas automatizados de decisão, os quais colocam em risco a autodeterminação informacional e o livre desenvolvimento da personalidade dos destinatários desses sistemas. Dentro dessa perspectiva, advém a motivação para desenvolver-se melhores práticas no uso de ferramentas algorítmicas, alinhadas com a ética e conformidade com as leis protetivas de dados.

Por fim, torna-se relevante enfrentar o tema relacionado a opacidade dos sistemas automatizados de decisão, especialmente quando empregam aprendizado de máquina.

2.3.2.1 Opacidade

No que diz respeito à clareza dos algoritmos, Diakopoulos (2017) destaca que embora os códigos legais estejam disponíveis para leitura, os códigos algorítmicos são mais opacos, ocultos por trás de camadas de complexidade técnica. Nesse ponto, o referido autor (2017) traz alguns questionamentos sobre como pode ser caracterizado o poder que os algoritmos exercem sobre as pessoas ou como é possível compreender melhor quando os algoritmos estão prejudicando os indivíduos.

A opacidade decorre da ausência de informações de como os “dados de entrada” (*inputs*) geraram os dados de saída (*output*), e de como o sistema correlacionou as variáveis contidas nos dados e os pesos atribuídos (KAUFMAN, 2021), especialmente porque, a depender do grau de inteligência artificial (IA) empregado, o código está em constante mutação, não sendo possível, muitas vezes, compreender a relação entre os dados de entrada e os dados de saída.

Segundo Mittelstadt *et al.* (2016) ao refletirem sobre evidência inescrutável, esclarecem que quando os dados são usados ou processados para produzir evidências para uma conclusão, é razoável que a conexão entre os dados e a conclusão seja acessível, seja inteligível. Contudo, quando se trata do funcionamento de algoritmos que empregam o aprendizado de máquinas há uma nítida dificuldade inerente na interpretação de como cada um dos muitos pontos usados por um algoritmo de aprendizado contribui para o problema, para a conclusão que gera no sistema (MITTELSTADT *et al*, 2016).

Com efeito, Burrel (2016) detalha três formas de opacidade nos sistemas de aprendizado de máquina que podem apresentar desafios de responsabilidade e transparência: i) opacidade como sigilo corporativo ou estatal intencional, ii) opacidade como analfabetismo técnico e, iii) uma opacidade que surge das características dos algoritmos de aprendizado de máquina e da escala necessária para aplicá-las de maneira útil.

A opacidade como sigilo corporativo é uma forma amplamente intencional de autoproteção por empresas que pretendem manter seus segredos comerciais e vantagens competitivas (BURREL, 2016), o que de certo modo é visível na leitura do parágrafo primeiro do art. 20 da LGPD[19], que insere como exceção ao direito à explicação os casos de segredos comercial e industrial. Diante disso, torna-se interessante o questionamento levantado por Frank Pasquale (2017), o qual coloca em dúvida o "problema do conhecimento" ("*knowledge problem*") que poderia estar relacionado a uma intenção deliberadamente incentivada pelas empresas no intuito de evitar ou confundir a regulação, em vez de ser um aspecto intrínseco ao mercado.

Sobre o tema, Emre Bayamlıoglu (2021) aponta duas barreiras relacionadas aos negócios, que poderiam envolver tanto a integridade do sistema como a rivalidade econômica.

No aspecto da integridade do sistema, o autor (2021) assinala que a ocultação de informações podem ser estratégias empregadas pelos controladores de dados com a intenção de impedir que os usuários contornem ou manipulem as entradas do sistema, buscando vantagens pessoais ou prejudicando a capacidade preditiva do sistema. Por sua vez, os controladores de dados podem ser resistentes no fornecimento de uma explicação sobre o modelo de inteligência artificial empregado com receio de enfraquecer a vantagem competitiva, ponto no qual as justificativas de integridade são geralmente confundidas com argumentos relacionados à concorrência (BAYAMLIOGLU, 2021).

De outro lado, a opacidade como a maneira como os algoritmos operam na escala de aplicação está relacionada ao modo como os modelos de aprendizado de máquina operam. Nesse ponto, relacionado aos limites técnicos oriundos da

[19] "Lei 13.709/2018. Art. 20 [...] § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial." (BRASIL, 2018)

complexidade computacional e imprevisibilidade, existem três elementos essenciais que devem ser observados: i) mesmo nos modelos mais simples, quanto mais fatores forem incorporados ao modelo como *input*, mais regras serão necessárias para explicar as relações entre a entrada e saída de dados; ii) os sistemas de *machine learning* possuem capacidade de encontrar padrões que vão além da intuição humana, de modo que as relações podem ser complexas e não-intuitivas, de modo que o modelo resistirá a uma avaliação sobre a confiabilidade da decisão, e iii) nos sistemas decisórios adaptativos, o algoritmo adaptável ou não determinístico pode produzir resultados diferentes para cada instância de sua execução, sendo a regra de decisão constantemente ajustada e não podendo ser predeterminada (BAYAMLIOGLU; 2021)

Assim a opacidade está intrinsecamente relacionada com a maneira como os algoritmos operam na escala de aplicação nos modelos de aprendizado de máquina. “Em vários casos, mesmo especialistas na área ou até as próprias pessoas que programaram o sistema têm dificuldade em entender perfeitamente o passo a passo da tomada de decisão” (MATTIUZZO, 2020, p. 123), especialmente porque, em razão das previsões iterativas[20], a lógica de decisão interna do algoritmo é alterada à medida que aprende nos dados de treinamento (BURREL, 2016).

Por sua vez, um problema adicional é a opacidade como analfabetismo técnico que decorre do reconhecimento de que escrever (e ler) código e o *design* de algoritmos é uma habilidade especializada, permanecendo inacessível para a maioria da população (BURREL, 2016). Nesse sentido, Burrel (2016) reforça que para escrever para o dispositivo computacional exige muita exatidão, formalidade e completude especiais que a comunicação através de linguagens humanas não exige, o que sem dúvida aumenta ainda mais o abismo entre opacidade e transparência.

Por esse motivo, Kroll (2018) defende que qualquer inescrutibilidade ou opacidade é produto da dinâmica de poder entre os controladores de um sistema e os afetados por ele. O referido autor (2018) destaca que quando mesmo os tecnólogos levantam as mãos e dizem que “não podem” entender um algoritmo ou não sabem o porquê ele está fazendo algo, estão se limitando a considerar a ação do sistema mecanicamente. Contudo, diferentemente disso, deve-se registrar que a

[20] Que permitem o ajustamento para uma resposta correta após a identificação de um modelo que fornece a relação preditiva mais forte entre entradas e saídas (YEUNG, 2017).

responsabilidade e a ética não se ligam às especificidades de uma ferramenta técnica, mas às maneiras pelas quais essa ferramenta é usada em um contexto sociotécnico, sempre considerando quando as ferramentas são criadas (KROLL, 2018).

Em um artigo publicado em 2015 por Rich Caruana, pesquisador da Microsoft, e seus colegas, revelou que no aprendizado de máquina muitas vezes é necessário fazer uma troca de precisão por inteligibilidade. Essa troca limitaria a precisão dos modelos que podem ser empregados em aplicações críticas, tal como assistência médica, em contrapartida, permitiria uma maior avaliação e confiança no modelo de aprendizagem, fator que é essencial quando se trata de cuidados relativos à saúde dos seres humanos.

Caruana *at al (2015)* relatam que foi realizado um estudo que tinha por objetivo prever a probabilidade de morte para pacientes com pneumonia. A finalidade era facilitar a triagem dos pacientes de modo que os doentes de alto risco pudessem ser internados no hospital, enquanto que os doentes de baixo risco pudessem ser tratados como pacientes ambulatoriais. No estudo, constatou-se que o sistema de redes neurais multitarefas eram mais precisos. Contudo, era muito arriscado para o uso em pacientes, porque a falta de intelegibilidade dificultava saber eventuais problemas que o sistema precisaria de correção. Assim, preferiu-se a escolha de um modelo de aprendizado baseado em regras, embora não fosse tão preciso, ele permitia identificar as falhas no sistema (CARUANA *at al, 2015)*.

E graças a escolha desse sistema menos complexo (aprendizado baseado em regras), foi possível identificar uma falha no sistema. Este modelo entendeu que pacientes com pneumonia tinham menor risco de morrer do que a população geral. Contudo, tal erro ocorreu porque na prática os pacientes com asma eram internados diretamente nas Unidades de Terapia Intensiva, o que em dados permitia um prognóstico melhor que a média dos demais pacientes. Portanto, sem ter um elemento que permitisse o sistema fazer essa diferenciação, erroneamente o algoritmo entendia que a asma reduzia o risco, quando na verdade os asmáticos têm risco maior se não forem hospitalizados (CARUANA *at al, 2015)*.

Este estudo permite concluir que a verificação das referidas falhas do sistema apenas foi possível porque o hospital aderiu a um sistema menos complexo que permitiu maior transparência da análise das decisões dos algoritmos. Portanto, tal exemplo reforça que a falta de transparência pode ser fator preponderante na

análise dos sistemas de decisão automatizadas, especialmente quando a sua ausência possa colocar em risco os destinatários da tecnologia.

Por essa razão, Emile Loza de Siles (2021, p. 521) defende que “para eliminar o viés de IA, ou, no mínimo, torná-lo visível, é importante testar o viés em cada etapa de componente do processo de IA”. Desse modo, em cada etapa do processo no desenvolvimento de uma inteligência artificial (o que envolve os sistemas automatizados de decisão) a IA deve ser avaliada. Esse processo de avaliação prévia pelo responsável da realização do tratamento de dados está relacionado ao estabelecimento de mecanismos de governança, numa percepção de gestão de risco, e *accountability* nas decisões algorítmicas, o que será devidamente explorado no terceiro e no quarto capítulo do presente trabalho.

Por fim, pode-se afirmar que os mecanismos de processamento e tratamento de dados, através da mineração, embora possa aparentar ser um processo neutro, são capazes de influenciar os sistemas automatizados de decisão, colocando em risco o livre desenvolvimento da personalidade e a autodeterminação informativa que constituem uma camada mais densa do direito fundamental a proteção de dados.

A partir disso, passa-se para o segundo capítulo do presente trabalho, no qual será analisado o direito a inferências como um direito que pode ser extraído da dimensão subjetiva do direito fundamental de proteção de dados, bem como o papel da governança de algoritmos como estrutura essencial no estabelecimento de mecanismos capazes de tornar as decisões automatizadas passíveis de compreensão e contestação.

3 DIREITO A INFERÊNCIAS RAZOÁVEIS COMO DESDOBRAMENTO SUBJETIVO DO DIREITO FUNDAMENTAL DE PROTEÇÃO DE DADOS PESSOAIS

Conforme foi exposto no capítulo anterior deste trabalho, a governamentalidade algorítmica, ao empregar sistemas automatizados de decisão, utiliza modelos preditivos e perfis que são atribuídos a indivíduos baseados em dados fragmentados decorrentes da big data. O uso extensivo dos dados pessoais e a crescente dependência de algoritmos para analisá-los, a fim de moldar escolhas e tomar decisões, muitas vezes com pouca ou nenhuma supervisão humana, representa sérios desafios à garantia da justiça, da responsabilidade e da proteção dos direitos humanos (FLORIDI; TADDEO, 2016).

Por mais valiosos que sejam os resultados dos sistemas de decisões automatizadas, há um risco elevado a ser considerado quando estiverem presentes a ausência de transparência e responsabilidade dos controladores de dados. Isso decorre do fato que eventual uso inadequado desses sistemas coloca em perigo o direito ao livre desenvolvimento da personalidade e o direito à autodeterminação informacional.

Nesse aspecto, as inferências e perfis criados pelos controladores de dados assumem um papel relevante na colocação social dos destinatários dos sistemas automatizados de decisão. Assim, eventuais resultados anômalos podem gerar formas acentuadas de discriminação, afetando um ou vários indivíduos, que diante da assimetria informacional existente acabam inviabilizados de exercerem o contraditório e ampla defesa de resultados estatisticamente calculados pelas máquinas.

O presente capítulo iniciará com um breve contexto histórico de alguns pontos a respeito do contexto das leis protetivas de dados e a consagração do direito fundamental de proteção de dados no ordenamento jurídico brasileiro. Em um segundo momento, serão verificados os desdobramentos constitucionais na tutela dos dados pessoais envolvendo o livre desenvolvimento da personalidade e a autodeterminação informacional. Na seção seguinte, pretende-se analisar os elementos constitucionais da tutela dos dados pessoais, dentro de uma proposição de ampliação do seu âmbito de proteção para reconhecer o direito a inferências razoáveis como um desdobramento da dimensão subjetiva do direito fundamental da

proteção de dados. Para tanto, serão abordadas as dimensões subjetiva e objetiva do direito fundamental de proteção de dados. Por fim, será analisado o papel da governança dos algoritmos no contexto da LGPD, conectando o tema à estrutura da corregulação e com o princípio da *accountability*, no intuito de preparar a transição para o terceiro capítulo.

3.1 BREVE CONTEXTO DAS LEIS PROTETIVAS DE DADOS E O DIREITO FUNDAMENTAL DE PROTEÇÃO DE DADOS

No âmbito internacional diversas iniciativas orientaram o desenvolvimento das normas de direito de proteção de dados, em especial o trabalho desenvolvido pela OCDE que resultou nas *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, finalizadas em 1980, e a Convenção de Estrasburgo de 1981 (Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais) que foi a primeira a adotar normas específicas para o tratamento de dados pessoais (DONEDA, 2019).

Em 1995 deu-se início a formação do sistema europeu de proteção de dados através da edição das Diretivas 95/46/CE e 2002/58/CE, atualmente substituídas pelo Regulamento EU 2016/679, conhecido como *General Data Protection Regulation* (GDPR) e pela Diretiva 2002/28/EC, que dispõe sobre aspectos de privacidade em serviços de comunicação eletrônica. Por sua vez, no ano de 2000 o direito de proteção de dados alcançou a condição de direito fundamental de natureza autônoma ao ser consignado na Carta de Direitos Fundamentais da União Europeia. A partir de então, passou, em grande medida, a ser autoaplicável, vinculando direta e indiretamente todos os integrantes da União Europeia (SARLET, 2021).

No Brasil, a proteção de dados pessoais somente se estruturou em torno de um conjunto normativo unitário nos últimos anos (DONEDA, 2019). Contudo, “a informação, como fenômeno a ser regulado pelo Direito não passou despercebido pelo Constituinte brasileiro” (MENDES, 2018, p. 194), o qual consagrou alguns direitos e garantias fundamentais voltadas a regulamentar a informação, tais como a inviolabilidade da intimidade e da vida privada (art. 5º, X) e o sigilo da correspondência e das comunicações (art. 5º, X).

Além disso, houve a previsão de uma garantia processual denominada *habeas data*, colocado à disposição do indivíduo para que esse pudesse ter acesso ou corrigir dados constantes de registros ou bancos de dados de entidades governamentais ou de caráter público (art. 5º, LXXII)[21].

Somado a essas previsões na CF, a legislação infraconstitucional avançou de forma paulatina sobre o tema, conforme observa Vladimir Aras:

> Nesta linha, o protagonismo cabe ao art. 43 do Código de Defesa do Consumidor (Lei nº 8.078/1990), ao que seguiu a Lei nº do Habeas Data (Lei nº 9.507/1997). Merecem menção os arts. 20 e 21 do Código Civil (Lei nº 11.406/2002), sobre direitos da personalidade, a Lei do Sigilo Bancário (Lei Complementar nº 105/2001), assim como a Lei de Identificação Criminal (Lei nº 12.037/2009), a Lei do Cadastro Positivo (Lei nº 12.414/2011), o art. 31 da Lei de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014), entre outros dispositivos – como os da Lei nº 7.210/1984, da Lei nº 9.613/1998, da Lei nº 12.850/2013 e do CPP especialmente após a Lei nº 13.344/2016. (ARAS, 2022, p. 106)

No que diz respeito à legislação específica sobre a proteção de dados, registra-se que a primeira iniciativa oficial do Governo ocorreu em 30 de novembro de 2010, através do Ministério da Justiça que abriu a primeira consulta pública sobre o anteprojeto de lei de proteção de dados pessoais, de autoria de Laura Schertel e Danilo Doneda (BIONI; RIELLI; VICENTE, 2019). “O referido debate público foi promovido pelo Ministério da Justiça e realizado inteiramente pela Internet, contando com a colaboração da Fundação Getúlio Vargas – Direito Rio e do Observatório da Internet, do Comitê Gestor da Internet do Brasil” (DONEDA, 2020, p. 253).

Com as revelações de Edward Snowden, a respeito da espionagem realizada pelo governo norte-americano sobre diversas autoridades no mundo, incluindo a presidente Dilma Roussef, houve o impulsionamento para a aprovação do Marco Civil da Internet (MCI)[22], em abril de 2014, através da Lei nº 12.965/2014. “Não foi a intenção do Marco Civil da Internet suprir a ausência de uma legislação geral acerca

---

[21] CF. Art. 5º [...] LXXII - conceder-se-á "habeas-data":
a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (BRASIL, 1988)

[22] Um dos textos legais mais importantes nesta toada é, sem dúvida, o Marco Civil da Internet (MCI), de 2014, que tornou mais claros os direitos dos usuários da internet no Brasil, entre eles a inviolabilidade e o sigilo de comunicações telemáticas e a confidencialidade dos registros de conexão e acesso. Orientando-se pelos princípios da proteção da privacidade e da proteção de dados pessoais, o MCI deu maior densidade a tais direitos, regulando também a remoção de conteúdo pessoalmente ofensivo. (ARAS, 2022, 107).

da proteção de dados pessoais” (DONEDA, 2020, p. 252), o qual já acenava para uma legislação própria sobre a proteção de dados pessoais consoante expressa previsão contida no inciso III do art. 3º da Lei 12.965/2014.

Nesse contexto, realizou-se a segunda consulta pública, orquestrada pelo Ministério da Justiça, que iniciou em 28 de janeiro de 2015 e se estendeu até julho do mesmo ano (BIONI; RIELLI; VICENTE, 2019). Após o debate público, com mais de 1.100 contribuições enviadas, houve a consolidação de uma nova versão do Anteprojeto pelo Ministério da Justiça, enviando-se ao Congresso Nacional, onde foi recebido pela Câmara dos Deputados como PL 5.276/2016, que originou a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 – LGPD), promulgada em 14 de agosto de 2018.

A LGPD apresenta uma significativa simetria com o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, “tendo incorporado uma série de institutos, princípios e regras da normativa europeia” (SARLET, 2021, p. 26). Ademais, “muito embora o Brasil sequer esteja vinculado ao direito europeu em geral, nem no concernente aos direitos humanos e fundamentais, para efeitos da transferência de dados o Brasil deve atender aos parâmetros do regulamento europeu” (SARLET, 2021, pp. 26-27).

A Constituição Federal, embora faça referência ao sigilo de comunicações de dados (art. 5º, XII, CF), não contemplava expressamente um direito fundamental à proteção e livre disposição dos dados pelo seu respectivo titular, “sendo o reconhecimento de tal direito algo ainda relativamente recente na ordem jurídica brasileira” (SARLET, 2021, p. 35). Ademais, antes da promulgação da EC nº 115 de 2022, a condição de um direito fundamental explicitamente autônomo do direito à proteção dos dados pessoais era associado e reconduzido por alguns princípios e direitos fundamentais de caráter geral e especial, tais como, princípio da dignidade humana, direito fundamental ao livre desenvolvimento da personalidade (implicitamente positivado), direito geral de liberdade e direitos especiais da personalidade, sendo os mais relevantes os direitos à privacidade e à intimidade (SARLET, 2021).

Para Sarlet (2021) o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados é o direito ao livre desenvolvimento da personalidade, que assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana, o que incluiria a autodeterminação

informativa, como “o direito à livre disposição sobre os dados pessoais” (SARLET, 2021, p. 36).

Em maio de 2020 a Suprema Corte foi instada a se manifestar quanto a constitucionalidade da Medida Provisória (MP) 954/2020, que obrigava as empresas de telefonia a disponibilizarem ao Instituto Brasileiro de Geografia e Estatística (IBGE) dados pessoais dos usuários (tais como nome, número de telefone e endereço de seus consumidores). Na oportunidade o Supremo Tribunal Federal (STF) confirmou a decisão monocrática, proferida em abril de 2020, pela relatora da ADI 6387, Ministra Rosa Weber, que concedeu liminar suspendendo a eficácia da MP 954, porquanto o referido ato normativo do Executivo representava restrição ilegítima aos direitos à privacidade, intimidade e sigilo dos dados pessoais, pois tal exigência estaria em desconformidade com as diretrizes da proporcionalidade.

A decisão do STF representou um marco jurisprudencial significativo ao reconhecer o direito fundamental à proteção de dados como um direito autônomo e distinto do âmbito do direito à privacidade.

A respeito da repercussão da decisão do STF e sua importância para o Direito brasileiro, Mendes, Júnior e Fonseca ponderam que:

> O significado histórico da decisão do STF pode ser equiparado ao clássico julgamento do Tribunal Constitucional Federal alemão, em 1983, relativamente à Lei do Recenseamento. Ao fazer referência ao julgado, o STF expressamente mencionou o conceito de autodeterminação informativa, já positivado na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados), a fim de ressaltar o necessário protagonismo exercido pelo cidadão no controle do que é feito com seus dados. Assim, pôs-se em destaque a existência de finalidades legítimas para seu processamento, bem como da necessidade de implementação de medidas de segurança para tanto. (MENDES; JÚNIOR; FONSECA, 2021, p. 67)

Desse modo, pode-se observar que a decisão do STF representa um verdadeiro fortalecimento na proteção de dados no âmbito nacional. Nesse contexto, não há como negar que a decisão da Suprema Corte “emprestou urgência à tramitação do Projeto de Emenda à Constituição (PEC) n. 17/2019, que visa alterar o texto constitucional de modo a inserir “a proteção de dados pessoais” no rol dos “direitos e garantias fundamentais”’ (MENDES; JÚNIOR; FONSECA, 2021, p. 69)

Com isso, no dia 10 de fevereiro de 2022, o presidente do Congresso Nacional, senador Rodrigo Pacheco, promulgou a Emenda Constitucional nº 115, de 2022, que passou a incluir a proteção de dados pessoais entre os direitos e

garantias fundamentais previstos na Constituição Federal (art. 5º, inciso LXXIX)[23], bem como fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais (art. 22, inciso XXX, CF)[24] e a competência material exclusiva da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei (art. 21, inciso XXVI, CF)[25].

A respeito da EC 115/2022, o ministro do Superior Tribunal de Justiça Ricardo Villas Bôas Cueva, ao ponderar a respeito da inclusão da proteção dos dados pessoais no rol do art. 5º da Constituição Federal, afirmou:

> Trata-se de um marco civilizatório, que coloca o Brasil no mesmo patamar de proteção de direitos fundamentais que a Europa. Agora se completa a arquitetura legislativa da proteção de dados no Brasil. A positivação do direito fundamental à proteção de dados é fundamental para aprofundar a tutela da autodeterminação informativa no país, pois a LGPD tem caráter marcadamente instrumental. (RODAS, 2022, p. 01).

A EC 115/2022 surgiu através da PEC nº 17 de 2019 de iniciativa do senador Eduardo Gomes, que originalmente propunha alterar o inciso XII e incluir a proteção de dados pessoais ao final do dispositivo. Com o transcurso do processo legislativo, houve o aperfeiçoamento da proposta, que passou a incluir um novo inciso no art. 5º da CF. De igual modo, houve a inclusão do inciso XXVI no art. 21 que também não constava na PEC 17/2019, que passou a prever a competência material da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais.

Dito isso, torna-se oportuno a análise dos desdobramentos constitucionais na tutela dos dados pessoais relacionados à tutela da dignidade da pessoa humana, em especial o livre desenvolvimento da personalidade e o direito à autodeterminação informacional.

3.2 LIVRE DESENVOLVIMENTO DA PERSONALIDADE E AUTODETERMINAÇÃO INFORMACIONAL

[23] “CF. Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)” (BRASIL, 1988)

[24] “CF. Art. 22. Compete privativamente à União legislar sobre: [...] XXX - proteção e tratamento de dados pessoais. (Incluído pela Emenda Constitucional nº 115, de 2022)” (BRASIL, 1988)

[25] “CF. Art. 21. Compete à União: [...] XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. (Incluído pela Emenda Constitucional nº 115, de 2022)” (BRASIL, 1988)

Um dos desafios mais importantes da atualidade é estabelecer uma abordagem adequada para a proteção dos direitos cívicos no desenvolvimento de novas tecnologias (PÉREZ LUNO, 2011). Por esse motivo, Pérez Luno (2011) reforça a necessidade da concepção dos valores e direitos das pessoas como uma garantia universal a ser observada no desenvolvimento das tecnologias, o que sem dúvida inclui os sistemas automatizados de decisão.

As assimetrias de informação e a racionalidade econômica dos dados podem "influenciar a igualdade de condições entre governo e cidadãos e entre empresas e consumidores, perturbando o atual equilíbrio de poder entre as diferentes partes" (SCHERMER, 2011, p. 47). O processamento de dados através de análises da big data tem como engrenagem a coleta massiva de dados que podem ser utilizados "para desenvolver prognósticos, tanto com relação à economia, à natureza ou à política, como sobre comportamento individual" (MENDES; MATTIUZZO; FUJIMOTO, 2021, p. 423).

Assim, o valor das informações obtidas não reside apenas na capacidade de armazenamento de grande volume de dados, mas, principalmente, na possibilidade de se obterem novos elementos informativos a respeito dos cidadãos a partir do tratamento desses dados (MENDES, 2014). Portanto, a proteção de dados pessoais pode ser compreendida como uma dimensão do direito à privacidade que adquire um âmbito muito mais abrangente, embora ambas se fundamentem na proteção da personalidade e da dignidade da pessoa humana (MENDES, 2014).

Nesse ponto, a questão da assimetria informacional é exponencializada em razão da limitada transparência dos indivíduos sobre a mineração dos dados, sendo que muitas vezes os indivíduos "não conseguem saber nem mesmo os dados que são coletados", tendo "dificuldades ainda maiores para compreender as inúmeras destinações que a eles pode ser dada e a extensão do impacto destas em suas vidas" (FRAZÃO, 2020, p. 23).

Segundo Wolfgang Hoffmann-Riem:

> Os indivíduos dificilmente terão outra escolha senão a de revelar em grande medida seus dados pessoais para as empresas, caso não queiram ser excluídos desses serviços básicos. Diante da capacidade de manipulação, reprodução e das possibilidades de divulgação praticamente ilimitadas dos dados, tanto em termos de tempo como de espaço, bem como sua imprevisível capacidade de recombinação em procedimentos de processamento não transparentes por meio de algoritmos incompreensíveis,

> os indivíduos podem ser expostos a dependências de longo alcance ou condições contratuais impositivas. (HOFFMANN-RIEM, 2020, p. 46):

A assimetria informacional, a opacidade constante nos sistemas automatizados de decisão e os vieses discriminatórios (abordados no primeiro capítulo) representam uma profunda ameaça ao desenvolvimento da personalidade dos indivíduos (HOFFMANN-RIEM, 2021). Portanto, as normas de proteção da personalidade, que estão especialmente relacionadas aos direitos de liberdade e igualdade, devem servir como parâmetro para o estabelecimento de mecanismos de governança na tutela dos destinatários dos sistemas automatizados de decisão.

Ademais, segundo Danilo Doneda (2021) uma considerável parcela das liberdades individuais é concretamente exercida através de estruturas digitais, nas quais a comunicação e a informação têm papel relevante. Além disso, a criação de perfis e a realização de inferências e correlações, aliados à mineração preditiva dos dados extraídos da big data, representam sérios impactos no livre desenvolvimento da personalidade, o qual pode ser compreendido como uma garantia do exercício de liberdade e igualdade na formação do pensamento dos indivíduos.

O livre desenvolvimento da personalidade está previsto de forma expressa no artigo 22 da Declaração Universal de Direitos Humanos:

> Todos, como membros da sociedade, têm direito à segurança social e têm direito para a realização, através do esforço nacional e da cooperação internacional e em acordo com a organização e os recursos de cada Estado, da economia, direitos sociais e culturais indispensáveis à sua dignidade e ao livre desenvolvimento de sua personalidade. (*UNITED NATIONS*, 1948)

Segundo Elimar Szaniawski (2005, p. 56) “os horrores do nazismo, da Segunda Guerra Mundial, e dos regimes totalitários do segundo pós-guerra, que se caracterizam pelo desprezo pela vida humana e pela personalidade, despertaram os povos para uma nova necessidade de proteger, sob todos os aspectos, os valores da personalidade e a importância do ser humano como pessoa”. Nesse viés, a Lei Fundamental da República Federal da Alemanha, dentre os direitos de liberdade, prevê em seu artigo 2º, inciso I que “toda pessoa tem direito ao livre desenvolvimento de sua personalidade, desde que não violem os direitos dos outros e não violem a ordem constitucional ou o código moral” (*DEUTSCHLAND*, 1949).

Da leitura do dispositivo constitucional alemão é possível aferir que o ordenamento jurídico admite “liberdades individuais que não restrinjam indevidamente liberdades alheias, sob pena de tornarem-se atos de não-liberdade (LUDWIG, 2001, p. 254). O direito ao livre desenvolvimento da personalidade “advém do reconhecimento doutrinário de dois princípios fundamentais que coexistem: a liberdade e a igualdade” (LUDWIG, 2001, p. 254).

Segundo Marcos Ludwig (2001) embora não exista previsão expressa do direito ao livre desenvolvimento da personalidade na Constituição Federal (CF) brasileira, trata-se de um princípio implícito que pode ser extraído da consagração da dignidade da pessoa humana (art. 1º, III, CF), dos valores fundamentais constantes no “caput” do artigo 5º da CF, tais como vida, liberdade, igualdade, segurança e propriedade, bem como da estrutura constitucional da ordem econômica e financeira (art. 170, CF).

“A rigor, a lógica fundante dos direitos da personalidade é a tutela da dignidade da pessoa humana” (TEPEDINO, 1999, p. 29). Não é por outra razão que a LGPD catalogou o livre desenvolvimento da personalidade como um fundamento na disciplina da proteção de dados pessoais, relacionando-o aos direitos humanos, à dignidade e ao exercício da cidadania pelas pessoas naturais (art. 2º, inciso VII).

Ainda em referência ao tema em questão, Cristiano Chaves de Farias e Nelson Rosenvald (2017) ponderam que a projeção da personalidade humana é erigida através da consagração do princípio da dignidade da pessoa humana, tendo em vista que o Direito Civil deve estar em conformidade com a normatividade constitucional. Assim, da dignidade da pessoa humana defluiriam como consectários naturais: “(i) o respeito à integridade física e psíquica das pessoas; (ii) a admissão da existência de pressupostos materiais (patrimoniais, inclusive) mínimos para que se possa viver; e (iii) o respeito pelas condições fundamentais de liberdade e igualdade” (ROSENVALD; FARIAS, 2017, p. 173).

Nesse sentido, Gustavo Tepedino (1999, p. 23) pondera que a personalidade deve ser considerada como um “valor máximo do ordenamento, modelador da autonomia privada, capaz de submeter toda a atividade econômica a novos critérios de validade”. Esses novos critérios estariam condicionados à cláusula geral fixada pela CF de promoção da dignidade humana, conferindo-se prioridade a valores consagrados na tábua axiológica eleita pelo constituinte (TEPEDINO, 1999).

Reafirmando essa percepção, Szaniawski salienta que:

> O constituinte brasileiro optou por construir um sistema de tutela da personalidade, alicerçando o direito geral da personalidade pátrio a partir do princípio da dignidade da pessoa humana e de alguns outros princípios constitucionais fundamentais, espalhados em diversos Títulos, que garantem o exercício do livre desenvolvimento da personalidade humana. (SZANIAWSKI, 2005, p. 137)

Portanto, a validade dos atos jurídicos "está condicionada à sua adequação aos valores constitucionais e à sua funcionalização ao desenvolvimento e realização da pessoa humana" (TEPEDINO, 1999, p. 27), de modo que a tutela da personalidade dos indivíduos garanta o exercício do livre desenvolvimento da personalidade humana. Nesse sentido, a LGPD apresenta a autodeterminação informativa (ou informacional) como fundamento da estrutura de proteção de dados (art. 2º, II), embora deixe de fornecer um conceito mais detalhado a respeito desse instituto jurídico extraído da jurisprudência alemã.

A partir disso e em análise comparada do direito alemão, pode-se afirmar que a autodeterminação informacional (ou informativa) é um desdobramento do direito geral da personalidade (MENKE, 2014). O direito geral da personalidade se instaurou no seio da jurisprudência alemã como uma tentativa de superar os déficits e limitações da concepção da esfera privada[26] (MENDES, 2020b).

Na decisão do caso "Eppler", do ano de 1980, há uma mudança paradigmática da proteção da esfera privada para um direito da personalidade geral e abstrato, na qual a Corte constitucional alemã referendou uma tutela que transcendeu o desenvolvimento da pessoa no âmbito de sua esfera privada, alavancando-a para abranger o próprio desenvolvimento da personalidade no seio da sociedade (MENDES, 2020b).

Segundo Laura Mendes:

> A importância da decisão reside no fato de que o Tribunal Constitucional aproveitou a oportunidade para expor uma explicação minuciosa da concepção do direito geral da personalidade. Assim, explicitamente estabelecido, pela primeira vez, que esse direito da personalidade representa um "direito de liberdade indefinido", que complementaria os direitos de liberdade específicos".
> Fica, ademais, reconhecido que sua tarefa é "proteger, nos termos do princípio constitucional da 'dignidade da pessoa humana' (art. 1º, §1º, LF), a

[26] Não é a finalidade do presente trabalho aprofundar o tema a respeito dos antecedentes do direito à autodeterminação informacional na jurisprudência alemã. Para maiores informações recomenda-se a leitura do artigo publicado por Laura Schertel Mendes intitulado: "autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã".

> esfera de vida pessoal mais íntima e a conservação de suas condições básicas que não podem ser captadas de forma conclusiva pelas tradicionais garantias concretas da liberdade. (MENDES, 2020b, p. 225)

Nesse viés, o direito da personalidade passou a ter como ideia central resumida em três pontos: proteção abrangente, abstração e conceito de autodeterminação. “O direito geral de personalidade representa uma ampliação da proteção perante a concepção da esfera privada ao abranger agora não somente a estreita esfera privada, mas toda a personalidade” (MENDES, 2020b, p. 226). Por sua vez, a abstração permite que o direito geral de personalidade garanta ampla proteção, flexibilidade e adaptabilidade, sendo apresentado como um direito de liberdade indistinto, que complementa os direitos de liberdade específicos (MENDES, 2020b). Por fim, a ideia de autodeterminação representa a possibilidade de o próprio indivíduo decidir de como se apresentar em público (MENDES, 2020b).

Seguindo essa evolução conceitual, em 1983 o Tribunal Constitucional alemão, no caso da Lei do Censo, reconheceu o direito do cidadão germânico de negar informações de caráter pessoal, entendendo como uma faculdade individual consentir, ou não, na coleta, no armazenamento e no compartilhamento de dados pessoais (RUARO, 2015). Na sentença do recenseamento, a Suprema Corte alemã deixou claro que “não importava mais se as informações coletadas dos cidadãos eram íntimas, privadas ou públicas; tratava-se, antes, dos riscos para a personalidade que poderiam surgir do processamento eletrônico de dados” (MENDES, 2020b, p. 229).

Dentro dessa perspectiva se consolida o reconhecimento jurídico da autodeterminação informativa como direito fundamental. Embora o Tribunal Constitucional alemão não tenha reconhecido diretamente um direito fundamental à proteção de dados pessoais, extraiu de uma leitura conjugada do princípio da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade, um direito fundamental implícito à autodeterminação informativa, consistente na prerrogativa de cada indivíduo decidir sobre a divulgação e a utilização de seus dados pessoais (SARLET, 2021).

Assim, pode-se afirmar que o cerne da concepção do direito à autodeterminação informacional está em sua fórmula de proteção abstrata, tal como o direito geral de personalidade, oferecendo grande flexibilidade na tutela de uma multiplicidade de casos envolvendo coleta e processamento de dados pessoais

(MENDES, 2020b). O fluxo informacional como fator promocional da pessoa humana passa a ter uma proteção diferenciada dentro da autonomia da proteção dos dados pessoais, o qual transita dentre mais de uma das espécies dos direitos da personalidade (BIONI, 2019).

Em uma perspectiva material, Sarlet (2021) entende que não há muita dificuldade em demonstrar a relevância, tanto para a esfera individual de cada pessoa como para o interesse coletivo, que os valores, princípios e direitos fundamentais associados à proteção dos dados pessoais e por ela protegidos, posicionam a proteção de dados pessoais como um direito fundamental. Portanto, a criação de perfis e a realização de inferências produzidas por muitos tipos de sistemas automatizados de decisão ultrapassam a esfera individual dos destinatários, devendo ser caracterizadas como fenômeno transindividual.

Assim, o estabelecimento de limites e responsabilidades aos controladores de dados na realização de inferências e na construção de perfis deve levar em consideração a abrangência dos efeitos desse tratamento de dados que, além de afetar a esfera individual dos destinatários, coloca em risco a própria coletividade (tema que será objeto de análise do terceiro capítulo do trabalho).

Com efeito, a falta de transparência e responsabilidade dos controladores de dados na programação de sistema automatizados com o uso de modelos preditivos e perfilamento é uma questão que afeta o princípio da autodeterminação informacional tanto na sua vertente individual (como a inviabilidade dos destinatários em ter acesso ou avaliar como as inferências são feitas sobre eles) como na sua vertente coletiva, porquanto coloca em risco a precondição para uma ordem comunicacional livre e democrática (SARLET, 2021).

Analisar as inferências sob o aspecto da proteção de dados é de suma importância para definir o âmbito de aplicação da Lei Geral de Proteção de Dados (LGPD) e verificar as camadas de proteção constitucional conferidas aos destinatários dos sistemas automatizados de decisão. A ausência de transparência e de responsabilidade dos controladores de dados com o emprego de modelos preditivos e perfilamento é uma questão que afeta o princípio da autodeterminação informacional.

3.3 DIREITO A INFERÊNCIAS RAZOÁVEIS: NECESSIDADE DE AMPLIAÇÃO DO ÂMBITO DE PROTEÇÃO

A criação de perfis afeta o direito à identidade pessoal, “entendido como a representação do indivíduo perante a sociedade” (LIMA, 2020, p. 113). Partindo dessa percepção, observa-se que os sistemas automatizados de decisão trabalham com mecanismos de resultados baseados no tratamento de dados, o que inclui dados inferidos e derivados, que não necessariamente serão caracterizados como dados pessoais.

Neste ponto, torna-se necessário estabelecer alguns apontamentos a respeito da distinção de dados, informações e dados pessoais para que seja possível situar com mais precisão o enquadramento das inferências que resultam dos sistemas automatizados de decisão.

O termo “dados” significa a fonte da qual se extrai uma informação (LIMA, 2020), portanto, seriam os “rastros”, voluntários ou não, gerados e registrados em diversos bancos de dados digitais (KAUFMAN, 2019). Enquanto a “informação” é a interpretação ou representação que se extrai do dado (LIMA, 2020). Portanto, a informação está contida em um ou vários dados, dos quais ela é extraída ou inferida (LIMA, 2020). Assim, o conceito de dado como tal não tem significado, sendo atribuído significado quando entra em um processo de comunicação de informações (HOFFMANN-RIEM, 2021).

O objeto de proteção da LGPD é a “informação relacionada a pessoa natural identificada ou identificável” (art. 5º, I) que seria a qualificação legal do que se entende por um dado pessoal. Portanto, “o conceito de dados é definido de forma mais restrita na chamada lei de proteção de dados como um direito à proteção da personalidade” (HOFFMANN-RIEM, 2021, p. 14).

No mesmo sentido, o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia assim define dados pessoais em seu artigo 4º:

> Dados pessoais, informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. (UNIÃO EUROPEIA, 2016).

Desse modo, evidencia-se que a limitação legal quanto ao conceito de dados pessoais pode ser um primeiro problema a ser enfrentado no que diz respeito à efetiva tutela da autodeterminação informacional dos destinatários dos sistemas automatizados, porquanto esta interpretação mais limitada poderia criar certas barreiras quanto ao direito de inferências razoáveis extraídas do tratamento de dados. Nesse ponto, Hoffamann-Riem (2021) pondera a importância da ampliação do conceito de dados pessoais, porquanto a atual concepção tradicional de proteção de dados não oferece proteção contra a coleta e a utilização de dados que não sejam pessoais.

Dentro desse contexto, os sistemas automatizados de decisão apresentam riscos para a autodeterminação informacional dos indivíduos quando empregam métodos de análise inferencial. Por essa razão, Wacther e Mittelstadt (2019) defendem que as inferências merecem a tutela de proteção similar à concedida para os dados pessoais no intuito de viabilizar a efetiva proteção dos titulares dos dados sujeitos aos resultados do tratamento de dados combinados com análises inferenciais e correlações. Para os referidos autores (2019, p. 22) as inferências seriam “informações relacionadas a uma pessoa física identificada ou identificável, criada por dedução ou raciocínio, em vez da mera observação ou coleta do titular dos dados”.

Nesse sentido, é de relevante contribuição ao tema os trabalhos apresentados pelo Grupo de Trabalho do Artigo 29 (*Working Party article* 29) o qual distingue dados fornecidos e dados derivados e inferidos. Para o WP29 os dados inferidos e dados derivados são os dados criados pelo controlador de dados ou terceiros a partir dos dados fornecidos pelo titular dos dados, tal como por exemplo o perfil criado no contexto da gestão de risco financeiro, seja para atribuir uma pontuação de crédito ou cumprir regras de combate à lavagem de dinheiro (*EUROPEAN COMMISSION*, 2016). Portanto, as inferências podem ser consideradas dados pessoais dentro do enquadramento de dados derivados ou inferidos (WACTHER; MITTELSTADT, 2019).

Ademais, para determinar o conceito de dados pessoais, o WP 29 estabeleceu quatro requisitos: ‘1º) “qualquer informação”; 2º) “relacionada a”; 3º) “pessoa natural”; e 4º) “identificada ou identificável”’ (LIMA, 2020, p. 102). No que diz respeito ao requisito “relacionada a”, que teria uma “conotação de que um determinado dado deve dizer respeito a um indivíduo” (LIMA, 2020, p. 102), o WP29

propôs um modelo de três etapas divididas em conteúdo, propósito e resultado, nas quais o processamento de dados deve estar relacionado a uma pessoa identificável, direta ou indiretamente (*EUROPEAN COMMISSION*, 2017).

Para Wachter e Mittelstadt (2019) a terceira etapa (resultado) é a chave para o *status* legal das inferências, permitindo que dados não pessoais sejam transformados em dados pessoais por meio da vinculação a um indivíduo identificado, tal como por exemplo o valor de uma casa que pode se tornar dado pessoal se usado para avaliar o indivíduo em uma obrigação fiscal. No mesmo sentido, Lima (2020) pondera que os três elementos (conteúdo, propósito e resultado) podem indicar que um certo dado é relacionado a uma certa pessoa, apesar de não dizer respeito direta ou indiretamente a determinada pessoa, mas podendo impactar na sua esfera de interesses, motivo pelo qual merece proteção.

Portanto, fica claro que para que um dado seja adjetivado como dado pessoal exige-se uma análise contextual. Assim, deve-se adotar uma concepção expansionista, pela qual dado pessoal equivale a uma informação que, direta ou indiretamente, identifica um sujeito, abrangendo, portanto, mesmo as informações que têm o potencial de identificar alguém, ainda que de maneira remota (BIONI, 2019).

Nesse sentido, Bruno Bioni (2019) defende a alocação da proteção de dados pessoais como um novo direito da personalidade, o que garantiria um alcance normativo maior, capaz de envolver toda e qualquer atividade de processamento de dados (ainda que não pessoal), mas que impactasse na vida de um indivíduo. Nesse sentido, o parágrafo segundo do art. 12 da LGPD prescreve que são considerados dados pessoais os dados anonimizados utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Segundo Bioni (2019) as expressões “determinada pessoa” e “identificada” devem ser compreendidas com relação aos desdobramentos ou consequências que o tratamento de dados pode ter sobre um indivíduo. Portanto, “o foco não está no dado, mas no seu uso – para formação de perfis comportamentais – e sua consequente repercussão na esfera do indivíduo” (BIONI, 2019, p. 102).

Assim, a LGPD demanda uma interpretação sistemática e alinhada com os objetivos e fundamentos da própria lei, dentre eles assegurar o livre desenvolvimento da personalidade (BIONI, 2019). Desse modo, o conceito de dado pessoal deve ser desenhado e vocacionado para expandir a proteção da pessoa

natural com relação às situações nas quais a atividade de tratamento de dados afeta o livre desenvolvimento da sua personalidade (BIONI, 2019).

Essas ponderações são necessárias, porquanto a criação de perfil pode ser feita com dados anonimizados (que não estariam sujeitos às diretrizes da LGPD) e, além disso, muitas vezes o perfil pode ser direcionado a um grupo determinado de pessoas, afetando uma coletividade e não uma pessoa específica (conforme foi exposto no primeiro capítulo ao abordar *group profiling* ou *clustering*). Por esses motivos, compreende-se que as inferências produzidas pelos sistemas automatizados de decisão ultrapassam o limite do individual e a própria compreensão legal de dados pessoais, demandando uma tutela transindividual e que atenda as reais necessidades dos destinatários desses sistemas.

Segundo Ingo Sarlet (2021b, p. 188-189), o direito de proteção de dados pessoais como um direito fundamental deve ser compreendido em sentido amplo, porquanto inexistem dados pessoais irrelevantes em face do processamento eletrônico, especialmente porque “sendo os dados projeções da personalidade, o seu tratamento, seja qual for, potencialmente pode violar direitos fundamentais.”

Ainda, de acordo com o referido autor (2021b), assim como se dá com os direitos fundamentais em geral, o direito à proteção de dados possui duas dimensões: uma de ordem subjetiva e outra de ordem objetiva. Tendo em vista que essas dimensões permitem fragmentar a análise das camadas de proteção constitucional conferidas aos destinatários dos sistemas automatizados de decisão, impõe-se a sua análise em subtópicos para melhor elucidação da análise do direito às inferências razoáveis como desdobramento do direito fundamental de proteção de dados pessoais.

3.3.1 Dimensão subjetiva do direito fundamental de proteção de dados pessoais

Em uma dimensão subjetiva, o direito à proteção de dados pessoais “se codifica em um conjunto heterogêneo de posições subjetivas de natureza defensiva (negativa), mas também assume a condição de direito a prestações, cujo objeto consiste em uma atuação do Estado mediante a disponibilização de prestações de natureza fática ou normativa” (SARLET, 2007, p. 224).

Segundo Laura Mendes (2018), o controle dos seus dados pessoais pelo indivíduo compõe um aspecto essencial da dimensão subjetiva, tendo em vista que se os dados se referem ao indivíduo e influenciam a sua esfera de direitos, o titular dos dados deve ter o controle da coleta, processamento, utilização e circulação dos dados. Nesse aspecto, a dimensão subjetiva guarda relação direta com um direito à autodeterminação informativa (SARLET, 2021b).

O livre desenvolvimento da personalidade do indivíduo e de sua dignidade consubstanciam-se no núcleo duro da autodeterminação informacional e representam um fundamento jurídico constitucional que deve ser observado a cada etapa do processamento e tratamento de dados pessoais (ALBERS, 2016). Assim, para que ocorra a limitação desse direito, exige-se a autorização legal ou consentimento do titular de dados para que a coleta, o processamento, a utilização ou a circulação de dados pessoais seja considerada legítima (MENDES, 2018).

A exigência de que o controlador só possa realizar o tratamento de dados se estiver amparado em uma base legal é percebida como uma convergência de arranjo institucional presente tanto no RGPD como na LGPD, que configura o que BIONI e MENDES denominam “racionalidade *ex ante* de proteção de dados”. Esse modelo está amparado em três características centrais: “i) um conceito amplo de dado pessoal, e ii) necessidade de qualquer tratamento de dados tenha uma base legal e iii) legítimo interesse como hipótese autorizativa e a necessidade de realização de um teste de balanceamento de interesses” (BIONI; MENDES, 2020).

Ademais, no texto constitucional não há qualquer referência direta quanto a posições jurídicas-subjetivas específicas que possam ser albergadas pela dimensão subjetiva do âmbito de proteção dos dados pessoais, contudo, isso não impede que a legislação infraconstitucional especifique (SARLET, 2021b). Inclusive, nesse sentido, a LGPD prevê um rol exemplificativo de direitos do titular da proteção de dados, em seus artigos 17 e 18, a saber:

> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.
> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;

> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL, 2018)

Esse catálogo enuncia, em uma grande medida, diversas posições jurídicas subjetivas (direitos) atribuídas ao titular dos dados pessoais objeto de proteção legal, que concretiza e delimita, em parte, o próprio âmbito de proteção do direito fundamental à proteção de dados (SARLET, 2021b). Observa-se que essa lista de posições jurídicas não tem caráter taxativo, não excluindo outras possibilidades (SARLET, 2021b).

Nesse sentido, Laura Mendes (2014, p. 176) afirma que o âmbito de proteção do direito fundamental à proteção de dados pessoais consiste, ao mesmo tempo: “(i) na proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e (ii) na atribuição ao indivíduo da garantia de controlar o fluxo de seus dados na sociedade”. Nesse sentido, Doneda (2021) esclarece que ao se estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados pessoais a finalidade precípua é a tutela da própria personalidade dos titulares de dados.

Segundo o autor:

> A proteção de dados pessoais apresenta-se, portanto, como modalidade de regulação da utilização da informação pessoal durante o seu tratamento, isto é, nas várias operações às quais ela pode ser submetida. Assim, ainda que possa ser tratada de forma desvinculada do seu titular após ter sido coletada, a informação pessoal continua ligada a ele através de um vínculo jurídico, determinado pelas normas de proteção de dados pessoais e justificada pela identidade desta informação com a própria pessoa. (DONEDA, 2021, p. 678)

Assim, um direito a inferências razoáveis está ínsito na própria ideia de proteção de dados. Trata-se de um corolário lógico que busca a tutela da expressão da própria personalidade do titular afetado por sistemas automatizados de decisão.

Diante dessas ponderações, é possível extrair da LGPD uma estrutura normativa que daria embasamento legal ao direito a inferências razoáveis consistente na análise sistemática dos seguintes dispositivos: a) direito ao acesso às informações (art. 9º); b) princípios da transparência e da qualidade (art. 6º, V); c) direito de retificação (art. 18, III); d) direito de eliminação (art. 18, IV), e e) legítima expectativa (art. 10, II).

A LGPD, em seu art. 9º, ao materializar o princípio do livre acesso, garante aos indivíduos o direito ao acesso facilitado às informações sobre o "tratamento de seus dados", os quais "deverão ser disponibilizadas de forma clara, adequada e ostensiva". Ademais, essas informações poderão envolver uma série de características, dentre as quais, a título ilustrativo[27]: i) a finalidade específica do tratamento; ii) forma e duração do tratamento, observados os segredos comercial e industrial, e iii) informações acerca do uso compartilhado de dados pelo controlador e a finalidade.

A LGPD garante ao titular de dados, em seu artigo 18, inciso III, o direito de obter do agente de tratamento "a correção de dados incompletos, inexatos ou desatualizados". Esse direito de retificação é um desdobramento do princípio da qualidade dos dados que prevê como garantia a "exatidão, clareza, e relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (art. 6º, V).

Portanto, em razão do princípio da qualidade os dados precisam ser "precisos, completos e atualizados" (SILVA, 2020, p. 200) para atender a finalidade de seu tratamento. Desse modo, caso seja verificado que determinado sistema automatizado de decisão chegou a um resultado inadequado ou até mesmo ilícito (discriminatório, por exemplo) em razão de um erro na base de dados que alimentou o aprendizado de máquina, apenas seria possível o titular exigir a observância da qualidade dos dados caso soubesse dessa informação. Portanto, a própria materialização do princípio da qualidade demanda a existência de mecanismos que viabilizem uma adequada transparência, trazendo informações úteis sobre a lógica subjacente do sistema que realizou as inferências ou criou os perfis que serviram de insumos para a inteligência artificial.

---

[27] A lista apresentada pelo art. 9º é nitidamente uma lista exemplificativa, tendo em vista que é oportunizada a previsão da exigência de outras características a serem previstas em regulamento.

Ademais, o direito de retificação também é um desdobramento da garantia do livre desenvolvimento da personalidade (art. 1º, art. 2º, VII, e art. 20) na medida em que dados imprecisos ou desatualizados podem ser fonte das externalidades negativas dos sistemas automatizados de decisão, “conferindo uma situação de desvantagem ao titular, como envio equivocado de correspondência, atribuição de dívidas que não correspondem à pessoa determinada, não recebimento de valores devidos, etc” (SILVA, 2020, p. 200).

Por sua vez, a LGPD prevê em seu art. 18, inciso IV o “direito de eliminação” dos dados tratados em desconformidade com a lei. Portanto, reforçando o princípio da qualidade, se houver o tratamento de dados que gerem anomalias, o seu tratamento deve ser obstado, determinando-se a eliminação dos dados que possam encadear enviesamentos nos sistemas automatizados de decisão.

Nesse sentido, embora não exista um “direito de retificação ou eliminação” das inferências e perfis resultantes do processamento de dados realizados pelo aprendizado de máquina, a partir de uma análise sistemática da LGPD e de sua estrutura deontológica é possível afirmar a existência de um direito a inferências razoáveis. Esse direito a inferências razoáveis está em harmonia com a estrutura principiológica da LGPD, que busca garantir o desenvolvimento e a utilização de sistemas de inteligência artificial confiáveis e auditáveis (CAITLIN; GOMES, 2022).

O principal vetor para alcançar o livre desenvolvimento da personalidade é assegurar que o fluxo informacional atenda às legítimas expectativas dos indivíduos (BIONI, 2019). Nessa percepção, a legítima expectativa do titular dos dados está prevista no inciso II do art. 10 da LGPD e serve como elemento balizador da configuração do legítimo interesse do controlador de dados. Ademais, prever a necessidade de realização de um teste de balanceamento de interesses faz parte da “racionalidade *ex ante”* de proteção de dados. Assim, pode-se afirmar que a legítima expectativa do titular consagra *standards* de comportamento para o controlador do que razoavelmente é esperado pelo titular de dados (BUCAR; VIOLA, 2020).

Nessa linha de raciocínio, torna-se imperioso buscar a construção de delimitações normativas a respeito do sentido do termo “razoáveis” no direito a inferências. Para tanto, o presente trabalho adota a concepção desenvolvida por Humberto Ávila sobre o princípio da razoabilidade, em sua obra Teoria dos Princípios da definição à aplicação dos princípios jurídicos.

Segundo Cláudio Neto e Daniel Sarmento (2016), há um debate relevante sobre a existência de possíveis diferenças entre os princípios da proporcionalidade e da razoabilidade, havendo um expressivo segmento de juristas que entendem que tais princípios seriam equivalentes, enquanto outros negam esta equivalência. Além disso, há pouco consenso sobre o conteúdo do princípio da razoabilidade, pois, de modo geral, “associa-se a razoabilidade às noções, muito vagas e imprecisas, de bom senso, racionalidade e justiça estatal” (NETO; SARMENTO, 2016, p. 486).

Nesse sentido, Humberto Ávila apresenta três acepções que se destacam em relação à razoabilidade:

> Primeiro, a razoabilidade é utilizada como diretrizes que exige a relação das normas gerais com as individualidades do caso concreto, quer mostrando sob qual perspectiva a norma deve ser aplicada, quer indicando em quais hipóteses o caso individual de suas especificidades, deixa de se enquadrar na norma geral. Segundo, a razoabilidade é empregada como diretriz que exige uma vinculação das normas jurídicas com o mundo ao qual elas fazem referência, seja reclamando a existência de um suporte empírico e adequado a qualquer ato jurídico, seja demandando uma relação congruente entre a medida adotada e o fim que ela pretende atingir. Terceiro, a razoabilidade é utilizada como diretriz que exige a relação de equivalência entre duas grandezas. (ÁVILA, 2005, p. 103)

A primeira acepção Humberto Ávila (2005, p. 103) denomina de “razoabilidade como equidade”, na qual o “postulado da razoabilidade exige harmonização da norma geral com o caso individual”. Portanto, a razoabilidade como equidade “imporia a adaptação de regras gerais às peculiaridades do caso concreto, sempre que este fugisse significativamente da normalidade, tornando a incidência da regra injusta” (NETO; SARMENTO, 2016, p. 487).

Na acepção de “razoabilidade como equidade” Ávila (2005, p. 106) entende que o postulado da razoabilidade “serve de instrumento metodológico para demonstrar que a incidência da norma é condição necessária, mas não suficiente para sua aplicação”, porquanto para se adequar ao caso concreto a razoabilidade atua na interpretação das regras gerais em conformidade com o princípio da justiça.

Por sua vez, na segunda acepção, a “razoabilidade como congruência” “exige a harmonização das normas com suas condições externas de aplicação” (ÁVILA, 2006, p. 106). Em suma, a razoabilidade demandaria uma relação de congruência entre os critérios de diferenciação escolhidos e as medidas adotadas, exigindo-se uma “correlação entre o critério distintivo utilizado pela norma e a medida por ela adotada” (ÁVILA, 2006, p. 109). Portanto, a eficácia dos princípios constitucionais do

Estado de Direito soma-se à eficácia do princípio da igualdade, de modo a impedir a utilização de critérios distintivos inadequados, pois “diferenciar sem razão é violar o princípio da igualdade” (ÁVILA, 2006, p. 109).

Por fim, a terceira acepção concentra-se na “razoabilidade como equivalência” na qual o postulado “exige uma relação de equivalência entre a medida adotada e o critério que a dimensiona” (ÁVILA, 2006, p. 109). Por exemplo, não poderia haver a imposição de pena criminal pesada para um ato que não seja tão grave (NETO; SARMENTO, 2016, p. 487).

Desse modo, trazendo essas acepções da razoabilidade para a proteção do direito fundamental de proteção de dados no âmbito dos sistemas automatizados de decisão, é possível observar que o direito a inferências razoáveis conecta-se com os princípios da não discriminação e da equidade, os quais demandam uma atuação preventiva dos responsáveis pelo tratamento de dados para enfrentar os enviesamentos injustos ou discriminatórios que decorrem das informações estatísticas e correlações geradas pelos algoritmos do aprendizado de máquina.

No intuito de elucidar melhor o tema, podemos imaginar um caso usual em que é realizado um tratamento de dados em sistema automatizado de decisão, no qual o legítimo interesse do controlador de dados seja para fins de prevenção a fraude, dentro de um contexto dos programas que fazem análise de crédito (*credit scoring*).

Em um primeiro momento, poderia se imaginar que o legítimo interesse independeria da expectativa do titular. Contudo, caso o sistema automatizado responsável pela prevenção a fraude cometesse um erro ao processar um dado de forma inadequada, em razão de um perfilamento incorreto. Nesse caso, qual seria a legítima expectativa do destinatário do sistema? Sem dúvida, a legítima expectativa seria que fosse disponibilizado informações úteis de como o aprendizado de máquina chegou àquele resultado, para que, então, pudesse verificar se as inferências ou a criação do perfil do titular foi realizado atendendo as diretrizes do princípio da razoabilidade.

Dando continuidade ao exemplo, em um determinado dia, Thomaz, advogado, com excelentes condições financeiras, acaba tendo seu nome incluído no Serasa por uma operadora de telefone “z”. Em contato com a operadora de telefone é verificado que alguém, mediante fraude, utilizou dados pessoais de Thomaz e possuía uma conta em seu nome, o que teria ensejado o débito com a operadora. O

atendente da empresa retira a negativação do nome do Thomaz do Serasa, contudo, por questões de procedimentos internos da empresa de telefonia “z”, não há a correção que daquele débito que foi originado de uma fraude e não de uma eventual inadimplência contratual do exímio advogado.

Todavia, como esse dado não é corrigido, entidades financeiras ao utilizarem dados compartilhados pela empresa de telefonia “z” alimentam seus sistemas como se aquela inscrição negativa no Serasa tivesse decorrido de uma inadimplência. O resultado desse compartilhamento incorreto de dados acarreta uma queda na avaliação do direito a crédito que Thomaz eventualmente teria na instituição financeira, quando utilizado na base de dados de sistemas automatizados de decisão, que enquadram Thomaz em determinado perfil em razão das inferências e correlações realizadas com a big data. Portanto, fica evidenciada uma discriminação limitadora do exercício de direitos conforme detalhado no primeiro capítulo do trabalho.

Nesse exemplo fica fácil perceber que se Thomaz não tiver acesso a informações úteis a respeito da lógica subjacente dos sistemas automatizados empregados pela instituição financeira para avaliar seu crédito, fica difícil questionar eventual pontuação que lhe foi conferida a partir da criação de perfis oriundos de inferências no compartilhamento de dados. Nesse caso concreto, qual seria a legítima expectativa do advogado?

A legítima expectativa seria, no mínimo, uma atuação de conformidade da instituição financeira com a LGPD, de modo que fosse disponibilizado o acesso de forma prévia às justificativas utilizadas, como uma maneira de identificar se as inferências realizadas no compartilhamento de dados com a operadora de telefonia “z” foram razoáveis. Essa transparência deveria ser acompanhada da possibilidade de Thomaz questionar a utilização das correlações fornecidas pela operadora de telefonia “z”, porquanto o débito cancelado no Serasa não seria oriundo de inadimplência do advogado, mas sim, de fraude perpetrada por terceiros. Essa correção evitaria uma avaliação inadequada pelos algoritmos dos sistemas automatizados empregados pela instituição financeira.

Portanto, o direito a inferências razoáveis pode ser compreendido como um *standard* de comportamento para o controlador de dados, seja para o desenvolvimento e implementação de tecnologias de sistemas automatizados de decisão que empreguem inferências e criação de perfis, seja para a construção de

estratégias no projeto que viabilizem o fornecimento de justificativas prévias aos destinatários de modo a operacionalizar a efetivação dos direitos à explicação e revisão constantes na LGPD.

Diante do exposto, torna-se relevante analisar a proteção dos indivíduos destinatários dos sistemas automatizados de decisão sob o aspecto da dimensão objetiva do direito fundamental à proteção de dados pessoais.

3.3.2 Dimensão objetiva do direito fundamental de proteção de dados pessoais

Segundo Ingo Sarlet (2021b, p. 227), os direitos fundamentais, além de constituírem direitos subjetivos de defesa do indivíduo, “constituem decisões valorativas de natureza jurídico-objetiva da Constituição, com eficácia em todo o ordenamento jurídico e que fornecem diretrizes para os órgãos legislativos, judiciários e executivos”. Nesse contexto, entre as funções e conteúdos normativos, três são particularmente relevantes: i) eficácia irradiante; ii) deveres de proteção, e iii) parâmetros para a criação e constituição de organizações (ou instituições) estatais e para o procedimento (SARLET, 2021b).

No que diz respeito à eficácia irradiante, decorrente da força jurídica objetiva autônoma dos direitos fundamentais, esta fornece impulsos e diretrizes para a aplicação e interpretação do direito infraconstitucional, apontando para a necessidade de uma interpretação conforme aos direitos fundamentais (SARLET, 2007). Nesse sentido, Sarmento (2008, p. 127) pondera que “a eficácia irradiante dos direitos fundamentais se manifesta, sobretudo, em relação à interpretação e aplicação das cláusulas gerais e conceitos jurídicos indeterminados, presentes na legislação infraconstitucional”.

Desse modo, o principal vetor para alcançar o livre desenvolvimento da personalidade é franquear ao cidadão controle sobre seus dados pessoais e essa estratégia vai além do consentimento do titular dos dados, pelo qual ele autorizaria o seu uso (BIONI, 2019). Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade (BIONI, 2019).

A legítima expectativa tem conotação subjetiva pela lei, sendo vinculada ao que o próprio titular deseja e espera que seja feito com seus dados (BIONI, 2021).

Contudo, ainda que apresente um conceito jurídico indeterminado, o conceito jurídico da legítima expectativa deve ser interpretado levando em conta a dimensão axiológica da função objetiva do direito fundamental de proteção dos dados, isso como decorrência dos efeitos irradiantes consagrados no núcleo da dignidade da pessoa humana.

Nesse sentido, ao ponderar sobre as implicações associadas à dimensão objetiva dos direitos fundamentais, Ingo Sarlet esclarece que:

> Como primeiro desdobramento de uma força jurídica objetiva autônoma dos direitos fundamentais, costuma apontar-se para o que a doutrina alemã denominou de uma eficácia irradiante (*Ausstrahlunggswirkung*) dos direitos fundamentais, no sentido de que estes, na sua condição de direito objetivo, fornecem impulsos e diretrizes para a aplicação e interpretação do direito infraconstitucional, o que, além disso, apontaria para a necessidade de uma interpretação conforme aos direitos fundamentais [...]. (SARLET, 2021b, p. 173)

Assim, como forma de assegurar o livre desenvolvimento da personalidade dos indivíduos sujeitos a sistemas automatizados de decisão, a LGPD deve ser interpretada como peça-chave para concretizar o desenvolvimento de mecanismos que condicionem a atuação os controladores de dados na utilização de tecnologias que sejam confiáveis e auditáveis, bem como mitigam, através da gestão de risco, as externalidades negativas oriundas dos vieses discriminatórios e opacidade.

Ademais, a eficácia irradiante faz com que o aspecto valorativo que passou a revestir os direitos fundamentais (dimensão objetiva) penetre em todo o ordenamento jurídico, condicionando a interpretação das normas legais, o que inclui “a consequência lógica e natural da constitucionalização do Direito Civil” e a consequente e “induvidosa aplicação dos direitos fundamentais mesmo nas relações estritamente privadas” (CHAVES; ROSENVALDO, 2017, p. 74).

Com efeito, através da eficácia irradiante os direitos fundamentais deixam de ser meros limites ao direito positivo e se transformam no eixo gravitacional de todo o ordenamento jurídico, estendendo-se às relações privadas (SARLET, 2007). Essa é outra importante função atribuída aos direitos fundamentais e desenvolvida a partir da dimensão objetiva.

Desse modo, o Estado não apenas deve se abster de violar os direitos fundamentais como também deve proteger seus titulares diante de lesões e ameaças advindas de terceiros, sendo que em toda e qualquer relação jurídica entre

particulares “devem estar salvaguardados os direitos fundamentais dos sujeitos” (CHAVES; ROSENVALDO, 2017, p. 75), o que inclui o tratamento de dados pessoais realizados por empresas no desenvolvimento e implementação de sistemas automatizados de decisão.

Nesse panorama, o estabelecimento de mecanismos de proteção aos direitos da autodeterminação informacional e o livre desenvolvimento da personalidade no âmbito dos sistemas automatizados de decisão é um fator impositivo. Esse comando constitucional pode ser materializado pela construção de ferramentas de governança que forneçam justificativas prévias e informações úteis a respeito da lógica subjacente ao processamento de dados resultante da realização de inferências e criação de perfis em sistemas automatizados de decisão.

No que diz respeito ao dever de proteção, o Ministro Gilmar Mendes, em seu voto proferido na medida cautelar da ADI 6387, ponderou que a dimensão objetiva do direito à proteção de dados pessoais impõe ao legislador um verdadeiro dever de proteção do direito à autodeterminação informacional, através da previsão de mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento e normas de proteção.

Esse dever de proteção estatal que decorre das implicações diretamente associadas à dimensão axiológica da função objetiva dos direitos fundamentais, não se trata de uma obrigação relacionada apenas ao legislativo, mas a todos os órgãos estatais incumbidos na efetivação da dignidade da pessoa humana. Os direitos fundamentais ao exprimirem os valores nucleares de uma ordem jurídica democrática “devem se irradiar para todos os campos do ordenamento jurídico, impulsionando e orientando a atuação do Legislativo, Executivo e Judiciário (SARMENTO, 2008, p. 106).

Com efeito, o reconhecimento da autodeterminação informacional como um direito fundamental conectado com a dimensão subjetiva do direito fundamental da proteção dos dados pessoais (SARLET, 2021b), viabiliza a tutela dos dados pessoais em uma multiplicidade de casos (MENDES, 2020), o que também deve abranger o direito a inferências razoáveis. Assim, a efetiva tutela contra inferências ou perfilamentos discriminatórios ou injustos é reforçado pela própria dimensão objetiva do direito à proteção de dados pessoais.

Dentro dessa perspectiva constitucional, a dimensão objetiva da proteção dos dados pessoais demanda a construção de mecanismos de governança como

ferramentas de salvaguardas da autodeterminação informacional e do livre desenvolvimento da personalidade frente aos riscos oriundos da utilização de perfis que não consideram os indivíduos em sua singularidade e o emprego de sistemas automatizados de decisão que partem de generalizações e metodologias estatísticas.

A partir do estabelecimento de um direito a inferências razoáveis é possível formular mecanismos de governança focados no fornecimento de uma justificativa *ex ante* que mitigue as externalidades negativas de aplicações de inteligência artificial de alto risco. Essa estrutura normativa pode ser extraída da LGPD por meio de quatro pilares, relacionados à tutela da autodeterminação informacional envolvendo decisões automatizadas, a saber: i) estruturação principiológica (art. 6º); ii) regras de boa governança (art. 50); iii) legítimo interesse (art. 7º, IX) e iv) direito à explicação e à revisão (art. 20).

Nessa linha de raciocínio, o Ministro Gilmar Mendes asseverou que o devido processo informacional pode ser extraído da dimensão subjetiva do direito à proteção dos dados pessoais. Por sua vez, a dimensão objetiva do direito de proteção de dados pessoais demandaria o estabelecimento de mecanismos de salvaguarda do direito à autodeterminação informacional (BRASIL, 2020).

No mesmo sentido, Bioni e Martins (2020) apontam que a capacidade de se defender de ações arbitrárias e intrusivas oriundas de sistemas automatizados de decisão vem sendo ameaçada, seja por razões técnicas (opacidade), seja por razões jurídicas (segredo comercial ou industrial). Em razão disso, os autores (2020) defendem uma releitura do devido processo legal sob uma perspectiva de salvaguarda em sistemas automatizados de decisão, de modo a garantir maior densidade jurídica no exercício de contraponto às ações opacas dos algoritmos decisórios.

Transpondo-se esse princípio para a seara da proteção de dados, observa-se a importância da criação de mecanismos capazes de garantir justiça e transparência aos destinatários das decisões automatizadas. Desse modo, o direito a inferências razoáveis como substrato normativo no desenvolvimento de mecanismos de governança baseadas na gestão de risco representa a consolidação de ferramentas voltadas ao fornecimento de informações úteis relativas à lógica subjacente dos sistemas automatizados de decisão.

Ademais, a partir de uma interpretação sistemática da LGPD, condicionando o direito a inferências razoáveis como seu substrato normativo, é possível condicionar a explicabilidade como pressuposto básico para o desenvolvimento de sistemas automatizados de decisão de alto risco (especialmente aqueles que possam afetar garantias e direitos fundamentais), impondo a demanda por mecanismos que assegurem transparência e legibilidade, bem como promovam a *accountability* dos controladores de dados.

Essa construção dogmática, esmiuçada no terceiro capítulo, tem como objetivo sugerir linhas normativas baseadas em uma governança de gestão de riscos que permitam a concretização de um devido processo legal na sua acepção substancial, ou seja, de adaptar a essência da exigência de justificativas prévias aos controladores de dados quando desenvolverem sistemas automatizados de decisão que possam afetar garantias e direitos fundamentais dos destinatários desses sistemas.

Por fim, a constituição de instituições estatais e para o procedimento está relacionada ao dever de proteção do Estado, tendo em vista que esses “podem, por vezes, concretizar-se por meio de normas dispondo sobre o procedimento administrativo ou judicial, bem como da criação de órgãos, constata-se que, desde já, a conexão pode existir entre estas duas facetas da perspectiva jurídico-objetiva dos direitos fundamentais” (SARLET, 2021b, p. 229).

Nesse ponto, embora o Estado possa dispor de várias alternativas para dar conta dos deveres de proteção, quando se refere ao direito fundamental de proteção de dados, o *enforcement* da LGPD, seguindo o fluxo internacional, demanda a criação e estruturação de uma autoridade independente para fiscalização e controle dos agentes de tratamento de dados. Esse ponto será aprofundado dentro do próximo tópico.

Nesse viés, a autodeterminação informacional e o livre desenvolvimento da personalidade dos indivíduos somente podem ser assegurados nos sistemas automatizados de decisão se forem previstas medidas de proteção suficientes para contornar os riscos oriundos das externalidades negativas presentes nas referidas tecnologias.

Essa ponderação justifica-se pelo fato que o valor das informações obtidas não reside apenas na capacidade de armazenamento de grande volume de dados, mas, principalmente, na possibilidade de se obterem novos elementos informativos a

respeito dos cidadãos a partir do tratamento desses dados (MENDES, 2014). E justamente quando se fala em obtenção de novos elementos informativos a respeito dos indivíduos torna-se possível se cogitar em um direito a inferências razoáveis como desdobramento da proteção constitucional conferida aos dados pessoais pela Suprema Corte.

A partir disso, passe-se para o terceiro capítulo, no qual, tendo como ponto de partida a análise da racionalidade *ex ante* de proteção de dados trabalhada por Bruno Bioni e Laura Mendes, serão desenvolvidos os mecanismos de governança que podem ser extraídos do direito a inferências razoáveis como um substrato normativo da LGPD voltado a implementação de transparência e *accountability* nos sistemas automatizados de decisão.

4 DIREITO A INFERÊNCIAS RAZOÁVEIS COMO SUBSTRATO NORMATIVO NA CONSOLIDAÇÃO DE MECANISMOS DE GOVERNANÇA

Geralmente os indivíduos, como público, não têm a clareza sobre como os algoritmos exercem seu poder sobre eles. Apenas com essa clareza é que seria possível que as pessoas tivessem maior capacidade de debater e dialogar publicamente sobre os méritos de qualquer poder algorítmico específico (DIAKOPOULOS, 2017). Portanto, deve-se reconhecer que a capacidade para entender o porquê um sistema automatizado alcançou uma decisão específica é uma questão a ser analisada como uma das ferramentas para contornar a opacidade encoberta por camadas de complexidade técnica, além das barreiras referentes à integridade dos sistemas e à rivalidade econômica (segredo comercial e industrial).

Segundo Bioni e Mendes (2020), existem diversos pontos convergentes entre a LGPD e o RGPD, tendo em vista a importância da equivalência da regulação nacional com o regulamento europeu para garantir a efetiva proteção de dados pessoais. Nesse sentido, os autores (2020) reforçam que um sistema de corregulação, por meio do princípio da *accountability*, parece ser uma tendência que aproxima o modelo brasileiro do europeu, havendo uma convergência de arranjo institucional na racionalidade *ex ante* de proteção e da guinada da accountability.

A racionalidade ex ante de proteção de dados está na premissa de que o controlador de dados só pode tratar dados se estiver amparado em uma base legal (BIONI; MENDES, 2020). Esse modelo está amparado em três características centrais: “i) um conceito amplo de dado pessoal, e ii) necessidade de qualquer tratamento de dados tenha uma base legal e iii) legítimo interesse como hipótese autorizativa e a necessidade de realização de um teste de balanceamento de interesses” (BIONI; MENDES, 2020).

No que diz respeito ao conceito amplo de dado pessoal, este tema foi explorado no capítulo anterior, no qual se buscou construir elementos que permitam o reconhecimento de um “direito a inferências razoáveis” como desdobramento do direito fundamental de proteção de dados e em harmonia com os princípios constitucionais implícitos da autodeterminação informacional e livre desenvolvimento da personalidade.

Por sua vez, a necessidade de base legal para a realização de tratamento de dados e o legítimo interesse serão objeto de análise em tópicos específicos relacionados aos mecanismos de salvaguardas oriundos da estruturação normativa decorrente do desdobramento da dimensão objetiva do direito fundamental de proteção de dados.

Diante da necessidade de garantir transparência e *accountability* em sistemas automatizados de decisão o reconhecimento de um "direito a inferências razoáveis" demonstra-se ser uma proposição interessante para consolidar a exigência de justificativas prévias e uma atuação de conformidade (*compliance*) por parte dos responsáveis pela realização de tratamento de dados em sistemas automatizados de decisão. Ademais, justamente essa atuação em conformidade com as diretrizes da LGPD demandaria que as empresas fossem compelidas a desenvolver mecanismos de governança focados no estabelecimento de critérios objetivos e informações úteis sobre a lógica subjacente no tratamento de dados, adicionando camadas importantes de transparência nos projetos tecnológicos e criando caminhos para o fortalecimento de uma *accountability* algorítmica, o que será objeto de análise no quarto capítulo da presente pesquisa.

Assim, o direito a inferências razoáveis deve ser compreendido como um substrato normativo que garante a intersecção entre os mecanismos de governança no intuito de buscar a implementação de transparência e *accountability* nos sistemas automatizados de decisão. A finalidade é conferir aos destinatários desses sistemas um leque de ferramentas que possam servir de salvaguardas na tutela da autodeterminação informacional e do livre desenvolvimento da personalidade.

Nesse contexto, observa-se que o reconhecimento de um direito a inferências razoáveis atrelado ao direito fundamental de proteção de dados tem como consequência, na sua perspectiva jurídico-objetiva do dever de proteção, o estabelecimento de mecanismos ou salvaguardas de governança que permitam o desenvolvimento de uma justificativa *ex ante*. Desse modo, orientando-se pela necessidade de uma interpretação sistemática da LGPD torna-se necessário abordar quais seriam esses mecanismos de *compliance* e *accountability* algorítmica que estariam relacionados ao direito a inferências razoáveis.

Como desdobramento da perspectiva objetiva do direito fundamental de proteção de dados pessoais é possível extrair uma estrutura normativa na LGPD que inaugura o Direito a inferências razoáveis como substrato normativo de um

devido processo legal na sua vertente substancial. Essa cadeia de mecanismos é consolidada em quatro pilares divididos da seguinte maneira: i) guias deontológicos (art. 6º); ii) regras de boa governança (art. 50); iii) legítimo interesse (art. 7º, IX) e iv) direitos à explicação e à revisão (art. 20).

A análise conjunta desses pilares levará ao estabelecimento de um panorama amplo sobre o *enforcement* da LGPD voltado à efetiva tutela da autonomia informacional dos indivíduos sujeitos aos sistemas automatizados de decisão.

A próxima seção iniciará com a análise dos direitos à revisão e à explicação, porquanto esses mecanismos seriam os quais a LGPD e o RGPD teriam atribuído maior relevância para a tutela de direitos e garantias dos titulares dos dados, no intuito de possuírem, em tese, um escopo necessário para enfrentar os problemas relacionados às externalidades negativas do uso de sistemas automatizados de decisão. Contudo, como será exposto, a procedimentalização dos referidos institutos encontra diversas barreiras relacionadas à eficácia, especialmente quando analisados de forma isolada.

Diante disso, torna-se relevante uma análise holística da LGPD que contemple os direitos à revisão e à explicação como vetores instrumentais de um devido processo legal substancial. Tal raciocínio decorre da importância na consolidação de um conjunto de ferramentas de governança que permitam a construção de mecanismos de *compliance* voltados ao estabelecimento de uma *accountability* algorítmica na tutela da autodeterminação informacional e do livre desenvolvimento da personalidade dos destinatários dos sistemas automatizados de decisão.

4.1 DIREITO A EXPLICAÇÃO COMO VETOR INSTRUMENTAL NA PROMOÇÃO DA TRANSPARÊNCIA

No âmbito europeu o ponto de partida para tratar sobre o uso de sistemas automatizados de decisão é o artigo 22 do RGPD, o qual prevê o direito de não se submeter a decisões totalmente automatizadas. Com base no referido dispositivo o titular dos dados tem direito de não ficar sujeito a uma decisão baseada exclusivamente no tratamento automatizado, incluindo o *profiling*, quando esse tratamento produza efeitos jurídicos ou o afete de forma significativa. Contudo, o mesmo artigo prescreve algumas exceções que acabam por mitigar esse “direito”,

abrindo brechas para que seja possível a submissão dos indivíduos a decisões automatizadas.

Conforme consta no item 2 do art. 22 do RGPD seria possível que um indivíduo se sujeitasse a decisão de sistema automatizado quando: a) fosse necessário para celebrar ou executar um contrato entre o titular dos dados e um controlador de dados; b) houvesse autorização pela legislação da União Europeia ou do Estado-membro a que o responsável pelo tratamento esteja sujeito, e c) estivesse baseado no consentimento explícito do titular dos dados.

Em relação à última exceção, ela acaba sendo demasiadamente ampla diante das fragilidades inerentes a proteção de dados através do consentimento informado. O consentimento “informado” estaria relacionado à ideia de uma obrigação do controlador de dados consistente em propiciar “ao cidadão os elementos necessários para o início de um processo de tomada de decisão no que tange ao fluxo de seus dados” (BIONI; LUCIANO, 2021, p. 153). Contudo, “tem-se questionado sobre a capacidade e racionalidade do sujeito em manter o controle sobre seus dados pessoais diante do modo com o qual este consentimento vem sendo obtido” (FRAJHOF; MANGETH, 2020, p. 67).

Nesse sentido, BIONI (2019, p. 189) esclarece sobre a existência de uma vulnerabilidade específica dos titulares dos dados diante da relação assimétrica a respeito do complexo ecossistema formada pela mineração de dados:

> A própria lógica do *trade-off* da economia dos dados pessoais é traiçoeira, portanto, frente a tal arquitetura de escolha de decisões, notadamente por essa idiossincrasia entre gratificações imediatas e prejuízos mediatos/distantes. A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais é posta em xeque por toda essa complexidade envolta ao fluxo das informações pessoais. Ele está em uma situação de vulnerabilidade específica em meio a uma relação assimétrica que salta aos olhos, havendo uma série de evidências empíricas a esse respeito.

Essa vulnerabilidade existente enfraquece o consentimento como mecanismo de salvaguarda dos titulares de dados, na medida em que é pouco provável que os indivíduos tenham habilidades suficientes para absorver, memorizar e processar todas as informações relevantes para um processo de tomada de decisão quanto à disponibilização de seus dados (BIONI, 2019). Ademais, quando se relaciona o consentimento do usuário ao processamento de dados pessoais e o uso de perfis

automatizados, “provavelmente não ficará claro para o envolvido qual será a extensão e impacto da criação de perfis em sua pessoa”, o que coloca em questão “até que ponto o titular dos dados pode dar livremente seu consentimento livre e informado” (SCHERMER, 2011, p. 52).

Diante disso, ainda não é possível saber se essas restrições efetivamente representam uma exceção do uso de sistemas automatizados de decisão no contexto europeu. Contudo, ainda que eventualmente a restrição geral do art. 22 não iniba o emprego dessas tecnologias, o referido dispositivo, em seu item 3, apresenta um rol exemplificativo de salvaguardas dos direitos e liberdades e dos interesses legítimos do titular dos dados, quais sejam: i) obter intervenção humana; ii) manifestar o seu ponto de vista e, iii) contestar a decisão.

Nesse sentido, Selbst e Powles (2017) ponderam que o artigo 22 do RGPD prescreve o dever de inclusão de medidas adequadas para salvaguardar os direitos e liberdades e interesses legítimos do titular de dados. Ademais, para os autores o art. 22(3) fornece uma lista não exaustiva de possíveis salvaguardas, isso porque o Considerando 71 do RGPD, que completa a leitura do art. 22, propõe salvaguardas adicionais, tais como “informações específicas para o titular dos dados” e “direito de obter uma explicação da decisão tomada”.

O raciocínio delineado por Selbst e Powles (2017) fica ainda mais robusto quando eles propõem uma inversão na abordagem do direito à explicação, asseverando que o art. 22 e o Considerando 71 do RGPD servem como base para a interpretação dos artigos 13 ao 15 do mesmo diploma legal europeu. O Regulamento Geral de Proteção de Dados possui nítida preocupação com o acesso à informação quando trata dos direitos dos titulares dos dados pessoais.

Esse cuidado especial é externalizado no artigo 13, nº 2, alínea “f”, artigo 14, nº 2, alínea “g” e artigo 15, nº 1, alínea “h”, todos do RGPD, que consagram em conjunto o direito de acesso à informação, a saber:

> Art. 13. Informações a serem fornecidas quando os dados pessoais são coletados do titular dos dados [...] 2. Além das informações referidas no n.º 1, o responsável pelo tratamento deve, no momento da obtenção dos dados pessoais, fornecer ao titular dos dados as seguintes informações adicionais necessárias para garantir um tratamento justo e transparente: [...] (f) a existência de tomada de decisão automatizada, incluindo criação de perfis, referida no artigo 22.º, n.ºs 1 e 4 e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas de tal tratamento para o titular dos dados. [...]

> Art. 14. Informações a serem fornecidas quando os dados pessoais não foram obtidos do titular dos dados [...] 2. Além das informações a que se refere o n.º 1, o responsável pelo tratamento deve fornecer ao titular dos dados as seguintes informações, necessárias para garantir um tratamento justo e transparente em relação ao titular dos dados: [...] (g) a existência de tomada de decisão automatizada, incluindo criação de perfis, referida no artigo 22.º, n.ºs 1 e 4 e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas de tal tratamento para o titular dos dados. [...]
> Art. 15 [...] 1. O titular dos dados terá o direito de obter do responsável pelo tratamento a confirmação do tratamento ou não dos dados pessoais que lhe digam respeito e, se for o caso, o acesso aos dados pessoais e às seguintes informações: [...] (h) a existência de tomadas de decisão automatizadas, incluindo a definição de perfis, referidas nos n.ºs 1 e 4 do artigo 22.º e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas desse tratamento para o titular dos dados. (UNIÃO EUROPEIA, 2016).

Os referidos artigos consagram a obrigação do agente de tratamento de dados de fornecer informações úteis relacionadas à lógica subjacente dos sistemas automatizados de decisão. De igual modo, os responsáveis devem explicar a importância e as consequências previstas no referido tratamento de dados.

Ademais, em reforço ao direito de acesso à informação, o art. 12 do RGPD prevê que o responsável pelo tratamento de dados deve tomar as medidas adequadas para fornecer qualquer informação (referida nos artigos 13, 14 e 15) relativa ao tratamento de forma “concisa, transparente, inteligível e facilmente acessível”, utilizando uma linguagem simples. Portanto, o art. 12 do RGPD, ao espelhar o princípio da transparência, revela que ao titular dos dados deve ser conferido o direito de ter conhecimento antecipado sobre o alcance e as consequências que podem resultar do processamento de dados.

Nesse sentido, o extinto WP29 entende que, para fins de tratamento de dados em sistemas técnicos complexos, os controladores de dados, além de garantir o acesso à informação consagrado nos artigos do RGPD, devem também explicar em linguagem clara e inequívoca quais as consequências e efeitos mais importantes de um processamento de dados específico (*EUROPEAN COMMISSION*, 2017c). Para Bayamlıoğlu (2021), o art. 22 do RGPD obrigada o controlador de dados a tornar contestáveis as decisões automatizadas, portanto, muito mais do que uma mera explicação da decisão, é essencial assegurar os direitos de acesso à informação relacionadas às decisões, os quais somente podem ser efetivamente aplicados se contribuírem para a efetividade das salvaguardas previstas no art. 22.

No mesmo raciocínio, Selbst e Powles (2017) entendem que o direito à explicação pode ser extraído do direito de acesso a informações úteis previsto nos artigos 13 ao 15 do RGPD. Nesse ponto, os autores fazem algumas observações de como o direito à explicação deve ser tratado para que tenha o impacto sugerido pelo RGPD no intuito de fortalecer a proteção de dados como um direito fundamental. Dentre as observações realizadas, os referidos autores (2017) propõem que a explicação seja abordada como um valor instrumental, o que ofereceria uma maneira mais concreta para medir se a explicação é significativa o suficiente.

Por sua vez, no âmbito da Lei Geral de Proteção de Dados brasileira os sistemas de tomada de decisão automatizada são objeto de disciplina no artigo 20. No “caput” do referido dispositivo há a previsão de um “direito de revisão”, que estaria limitado a decisões totalmente automatizadas e que afetassem interesses dos titulares dos dados, apresentando-se um rol exemplificativo que abrangeria decisões destinadas a definir perfil pessoal, profissional, de consumo, de crédito ou outros aspectos de sua personalidade.

Por sua vez, no parágrafo primeiro do art. 20 assegura-se o “direito à explicação” constituído no dever do controlador de dados de fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. Ao final do referido dispositivo, o legislador consagrou a ressalva para os casos de segredo comercial e industrial.

Em uma primeira leitura do art. 20, poderia se defender que os direitos de revisão e explicação estariam aptos na resolução de problemas envolvendo as externalidades negativas dos sistemas automatizados de decisão, em especial o viés discriminatório e a opacidade. Contudo, uma análise mais aprofundada dos referidos mecanismos previstos na LGPD demonstra que os direitos de revisão e explicação, considerados de forma isolada, são incapazes de apresentar soluções compatíveis com as complexidades decorrentes das análises inferenciais e correlações que servem de insumo para os sistemas automatizados de decisão.

Primeiro, existem alguns pressupostos básicos que não foram definidos pela legislação e seriam imprescindíveis para a melhor compreensão do direito à explicação e à revisão, tais como: i) o que vem a ser uma decisão totalmente automatizada; ii) que tipos de decisão automatizada afetam a esfera jurídica dos titulares de dados, e iii) qual é o grau de transparência e explicação que será

exigível em situações desse gênero (MONTEIRO, CRUZ, 2021; BECKER; FERRARI, 2020; FRAZÃO, 2018).

No primeiro ponto, esse questionamento se torna relevante, porque consoante o art. 20 da LGPD[28], para que seja exercido o direito de revisão, é imprescindível que a decisão seja tomada unicamente com base em tratamento automatizado de dados pessoais. Assim, tendo em vista que o nível de intervenção humana para tomar a decisão não é claro, em uma interpretação literal do dispositivo, ainda que a participação humana seja limitada a determinadas etapas do processo decisório, isso por si só, já afastaria a aplicação do direito à revisão. Essa ausência de clareza também existe no art. 22 do RGPD da União Europeia, e tem sido amplamente empregada pelos controladores de dados para contornar as proteções legais conferidas aos destinatários dos sistemas automatizados de decisão (BAYAMLIOĞLU; 2021).

A princípio essa não parece ser a melhor interpretação do dispositivo tendo em vista que não estaria em consonância com as diretrizes da estrutura principiológica constante no art. 6º da LGPD. Ademais, haveria uma certa contradição, na medida que o parágrafo primeiro do art. 20 da LGPD[29] não prevê essa limitação quanto ao exercício do direito de explicação.

No mesmo sentido, o WP29 entende que mesmo a intervenção humana não afastaria o que se entende por decisão totalmente automatizada, salvo se a participação humana no processo de tomada de decisão fosse significativa de modo a ter autoridade para influir no resultado da decisão (*EUROPEAN COMMISSION*, 2017). Portanto, dando preferência a uma interpretação que favoreça a efetiva proteção da autodeterminação informacional dos destinatários dos sistemas automatizados de decisão, deve ser permitido o exercício do direito de revisão ainda que a decisão não seja totalmente automatizada, desde que reste demonstrado que o sistema automatizado tenha concorrido de forma significativa para o resultado da decisão objeto de questionamento.

---

[28] “Lei 13.709/2018. Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.” (BRASIL, 2018).

[29] “Lei 13.709/2018. Art. 20 [...] § 1° O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.” (BRASIL, 2018)

No segundo ponto, no que diz respeito aos tipos de decisão automatizada que afetam a esfera jurídica dos titulares de dados, as ponderações de Marcela Mattiuzzo (2021) parecem trazer algumas diretrizes interessantes sobre o tema. Na percepção da autora (2021) existem casos em que o uso automatizado de decisão, ao representar um problema para o sistema jurídico, deve ter seu uso evitado. Dentre os casos em que o uso de generalizações não seria adequado ao regime jurídico, destaca-se: a) sempre que a Constituição Federal proibir inferências e exigir decisões baseadas em evidências diretas de comportamentos individuais específicos, tal como ocorre no âmbito do Direito Penal, e b) quando envolver exercício de julgamento ou prudência que demande valoração, ou seja, avaliações éticas ou morais (MATTIUZZO, 2021).

No primeiro caso, pode-se citar o exemplo do COMPAS, *Correctional Offender Management Profiling for Alternative Sanctions* (Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativas), elaborado pela empresa Northpointe, utilizado pelo sistema judiciários de vários Estados norte-americanos. O referido sistema está inserido nos programas denominados *risk assessments*, que possuem a finalidade de calcular o risco de reincidência de pessoas acusadas de cometer crimes e são usados para orientar os juízes a respeito de quem pode ser posto em liberdade durante o trâmite processual (BENANTI, 2020). Portanto, o COMPAS é utilizado para determinar a probabilidade de reincidência de prisioneiros.

Em maio de 2016 a ProPublica, agência de imprensa independente e sem fins lucrativos, avaliou o COMPAS e descobriu que réus negros eram muito mais prováveis do que réus brancos de serem incorretamente enquadrados pelo sistema com maior risco de reincidência (LARSON *et al*, 2016). Portanto, a referida instituição identificou que os dados alimentados no sistema eram viciados com informações anteriores, o que sem dúvida colocava em risco o resultado supostamente neutro dos algoritmos.

Ainda que o COMPAS tenha apresentado vários problemas no que diz respeito ao seu viés discriminatório, o que, por si só, já levantaria sérias dúvidas quanto a sua eficiência, a grande questão é que o uso deste sistema, dentro das diretrizes levantadas por Mattiuzzo (2021), deveria ser evitado ou proibido por lei. Tal afirmação decorre do raciocínio que o COMPAS ajuda os juízes a formarem conclusões sobre o risco de reincidência dos réus, contexto de uso que não se recomenda o uso de inferências.

Deve-se observar que a análise preditiva dos sistemas é completamente contrária aos princípios basilares da Constituição Federal, tal como da presunção de inocência e do devido processo legal, inviabilizando, portanto, que o condenado pudesse contrapor os fundamentos opacos resultados das decisões automatizadas. Ademais, o próprio sistema automatizado coloca em risco a parcialidade do juiz, porquanto as ferramentas tecnológicas oferecem recomendações que tornam extremamente difícil para um tomador de decisão humano refutar tal recomendação (CUMMINGS, 2004).

No segundo caso, quando envolver exercício de julgamento ou prudência que demande valoração ética ou moral, também haverá um fator de risco significativo ou até mesmo uma impossibilidade técnica de sua implementação pela máquina, porquanto os algoritmos atuais de IA não são capazes de raciocinar conforme já exposto no primeiro capítulo do presente trabalho. A tecnologia atual não é capaz de desenvolver algoritmos que possam criticar padrões de acordo com uma ordem de valores, o que inviabilizaria, pelo menos por enquanto, o desenvolvimento de sistemas que pudessem chegar de forma automatizada em uma decisão justa (MATTIUZZO, 2021). Contudo, esse aspecto ainda é muito amplo e demandará uma análise circunstancial pela Autoridade Nacional de Proteção de Dados do contexto em que empregado os sistemas automatizados de decisão.

Por fim, em relação ao terceiro ponto (referente aos pressupostos básicos que não foram definidos pela legislação) em relação ao grau de transparência e explicação exigível, observa-se que é um problema muito mais complexo, porquanto está intrinsecamente relacionado ao nível de aprendizado de máquina empregado no desenvolvimento dos sistemas automatizados de decisão e a opacidade resultante dessa implementação. A depender do nível de tecnologia utilizada no desenvolvimento dos sistemas, maior poderá ser a sua opacidade em razão do *tradeoff* entre precisão e transparência (KAUFMAN, 2021).

Além dessas incertezas, Edwards e Veale (2017) revelam que a eficácia do exercício do direito de explicação teria que lidar com alguns problemas adicionais, tais como: i) os danos algorítmicos possuem uma perspectiva transindividual, pois normalmente surgem da forma como os sistemas classificam ou estigmatizam os grupos, e; ii) as barreiras técnicas dificultam a efetivação de explicações significativas, pois os indivíduos, em sua maioria, são muito carentes em termos de

tempo, recursos e conhecimentos necessários para fazer uso do direito de explicação de forma adequada.

No que diz respeito a natureza transindividual dos danos, os riscos dos vieses discriminatórios dos sistemas automatizados, por exemplo, na maioria das vezes demandam tutela da coletividade, especialmente quando envolve a criação de perfis que levam em conta generalizações sobre correlações de informações de diversos indivíduos, direcionando-se a um determinado grupo e não a uma pessoa específica conforme exposto nos primeiros capítulos do trabalho. Ademais, ainda que envolvam direitos individuais, estes podem ser individuais homogêneos ou direitos individuais indisponíveis que também serão abarcados por obstáculos multifacetados que inviabilizariam o exercício do direito de explicação de forma individual, seja pela opacidade do sistema ou por ausência de determinações legais quanto às obrigações que deveriam ser assumidas pelos controladores de dados no estabelecimento de justificativas no desenvolvimento do projeto.

Em agosto de 2020, algoritmos desenvolvidos pelo Governo britânico causaram polêmica na avaliação de estudantes do ensino médio que buscavam uma colocação nas universidades do Reino Unido. Transcorridos alguns meses de testes, houve o desenvolvimento do algoritmo denominado Approach-1, o qual seria alimentado por diversos dados, desde informações extraídas dos registros históricos dos alunos, como dados gerados de forma mais especulativa, como por exemplo, informações dos professores a respeito das notas que seus alunos poderiam ter obtido se os exames finais tivessem ocorridos (LAMONT, 2021).

Após novos testes, a própria Ofqual estava preocupada com alguns resultados anômalos que representavam menos de um quarto de 1%, mas que acabavam derrubando notas de alunos brilhantes em escolas com desempenho historicamente baixo, assunto registrado em um memorando encaminhado ao escritório de Boris Johnson denominado “os riscos de desvantagem para alunos discrepantes” (LAMONT, 2021). Portanto, um aluno com bom desempenho acabava sendo prejudicado em razão de estudar em uma escola de baixo desempenho, diminuindo significativamente sua chance de obter uma boa colocação na universidade.

Esses resultados anômalos não preocuparam os responsáveis pela continuidade do projeto, deixando-se de lado qualquer debate prévio com as comunidades locais a respeito dos riscos encontrados. Contudo, as injustiças que

advieram da implementação do sistema foram sentidas de forma imediata pela comunidade, incluindo especialmente os alunos e professores. O desastre do algoritmo gerou protestos em cidades inglesas, com jovens carregando cartazes: “o algoritmo roubou meu futuro” (AMOORE, 2020).

Em razão disso, o governo recuou e permitiu que os alunos voltassem para o sistema anterior de avaliação de notas. Logo após, em uma reunião, Roger Taylor, responsável pela Ofqual, após se desculpar com todos os que foram prejudicados pelo Approach-1, registrou que os algoritmos revelaram e amplificaram os preconceitos humanos cruéis já existentes no sistema de ensino inglês e que serviram de base de dados para os sistemas desenvolvidos (LAMONT, 2021).

Portanto, no caso do Approach-1 foi nítida a iniquidade de tratamento ocasionada aos alunos oriundos de escolas mais deficitárias, reforçando a desigualdade já existente no sistema tradicional e representando danos de natureza transindividual. Claro que nesse ponto, houve a aplicação de sistemas automatizados de decisão pelo setor público, o que sem dúvida reforça a necessidade de mecanismos de governança destinados a controladores de dados de sistemas automatizados em um sentido amplo, independentemente em razão de se tratar de uma empresa privada ou um órgão público.

No que diz respeito à tutela coletiva, o art. 22 da LGPD prevê que “a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva”. Embora o referido dispositivo faça referência a aspectos processuais referente ao exercício em juízo, entende-se que também seria possível uma tutela preventiva extrajudicial dos danos de natureza transindividual através dos mecanismos de governança e *compliance*, baseados na análise de riscos, que serão abordados nos próximos tópicos.

Nessa linha de raciocínio, importa consignar que existe uma proposta de Resolução do Conselho Nacional do Ministério Público (CNMP) que visa instituir a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais do Ministério Público brasileiro e dá outras providências (Proposição nº 1.00415/2021-60)[30].

[30] O inteiro teor da proposta de resolução pode ser obtida no sítio eletrônico do CNMP: https://www.cnmp.mp.br/portal/atos-e-

Da leitura da proposta observa-se que as unidades do MP deverão promover a estruturação de suas promotorias e procuradoria para “atuação na defesa da ordem jurídica e da dimensão coletiva do direito à proteção aos dados pessoais, diante de violações à legislação por pessoas físicas ou jurídicas, de direito público ou privado” (art. 56). De igual modo, “incumbe ao Ministério Público a proteção dos dados pessoais no âmbito das relações de consumo, das relações de trabalho, nos serviços públicos e de relevância pública ou em relações jurídicas de outra natureza, quando se revelar afetação à coletividade” (art. 57).

Além dessas previsões, o artigo 59 da Resolução estabelece que o Ministério Público deverá atuar para prevenir e coibir a violação das normas de proteção de dados pessoais e da autodeterminação informativa, especialmente quando constatada lesão ou ameaça de lesão a direitos individuais indisponíveis, difusos e coletivos, em razão de práticas, dentre as quais, destacam-se: i) tratamentos automatizados de dados pessoais, inclusive sensíveis; ii) uso de instrumentos de inteligência artificial; iii) análises de perfis de titulares, inclusive por meio de agregações de dados históricos; iv) prejuízos à igualdade de oportunidades; v) abuso de poder econômico; vi) abuso do poder de direção em relações de trabalho em geral, inclusive no âmbito de grupos econômicos e em contratos de prestação de serviços; vii) ausência de interesses legítimos do controlador; viii) ausência de transparência algorítmica; ix) prejuízos ao exercício da cidadania em meios digitais; x) obtenção indevida de dados pessoais; xi) coleta de dados pessoais sem necessidade ou finalidade delimitadas; xii) vinculação ou associação indevidas, direta ou indireta, de dados pessoais; xiii) falha ou erro de processamento durante a execução de operações de tratamento; xiv) técnicas de engenharia social que acarretem o ilícito tratamento de dados pessoais, inclusive a indevida inclusão de dados pessoais inexatos, e xv) quaisquer outras violações aos princípios e às normas protetivas de dados pessoais.

Dentre as ferramentas que o MP terá à disposição nessa atuação preventiva destaca-se a possibilidade de requisitar o Relatório de Impacto à Proteção de Dados Pessoais (RIDP), com a descrição dos processos de tratamento que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais, de forma a promover medidas, salvaguardas e mecanismos de eliminação

---

normas/norma/7935/#:~:text=Institui%20a%20Pol%C3%ADtica%20Nacional%20de,1.00415%2F2021%2D60).

e mitigação de danos e riscos (art. 60). Diante disso, o procurador da república Vladimir Aras (2022) entende que o Ministério Público (MP) poderá atuar no exame da conformidade (*compliance*) das práticas adotadas pelas empresas que realizem o tratamento de dados, destacando que dentre as atribuições conferidas ao órgão ministerial estaria a possibilidade de requisição do RIDP (ARAS, 2022).

Além disso, o Ministério Público, em defesa dos direitos fundamentais individuais indisponíveis, coletivos e difusos, terá acesso incondicional a bancos de dados pessoais de caráter público ou relativos a serviços de relevância pública, bem como a bancos de dados privados, podendo, para tanto, exercitar seu poder de requisição. Esse acesso aos dados, com exceção das hipóteses de reserva de jurisdição estabelecidas pela CF, também facilitaria a atuação do órgão ministerial na sua atuação extrajudicial e preventiva, no intuito de coibir a violação das normas de proteção de dados pessoais e da autodeterminação informativa.

Apresentados alguns apontamentos a respeito da possibilidade de uma atuação extrajudicial do Ministério Público, cumpre voltar a leitura do art. 22 da LGPD na análise da tutela judicial de dados através de ações individuais ou coletivas. O referido dispositivo está em consonância com o princípio da inafastabilidade da jurisdição consagrado no inciso XXXV do art. 5º da CF.

Embora não seja o objeto do presente trabalho abordar questões ligadas à tutela judicial da proteção de dados pessoais, impõe-se registrar que a proteção dos direitos transindividuais dos titulares de dados afetados no âmbito do emprego de sistemas automatizados de decisão é amplamente viabilizada pela LGPD mediante a adoção “dos instrumentos de tutela individual e coletiva” – art. 22, da LGPD – e sujeição dos controladores de dados “às regras de responsabilidade previstas” no Código de Defesa do Consumidor (CDC) – art. 45, da LGPD[31], quando o titular do direito estiver enquadrado nas relações de consumo.

Assim, o art. 22 da LGPD ao prever de forma genérica a aplicação de “instrumento de tutela coletiva” permite uma conexão segura e sólida com a proteção conferida pelo microssistema do processo coletivo, em especial com o núcleo[32] “duro” valorativo do microssistema protetivo consistente na Lei da Ação

[31] “Lei 13.709/2018. Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.” (BRASIL, 2018)

[32] ‘O CDC, ao alterar a Lei n. 7.347/1985 (LACP), atuou como verdadeiro agente unificador e harmonizador, empregando e adequando à sistemática processual vigente do Código de Processo

Civil Pública (Lei nº 7.347/85) e o Código de Defesa do Consumidor (Lei nº 8.078/90), o qual viabiliza a tutela preventiva (ameaça de lesão) ou reparatória. Tal raciocínio é possível a partir do postulado hermenêutico do microssistema no qual deve ocorrer a aplicação integrada das leis para a tutela coletiva, em nítida aderência à teoria do diálogo das fontes trabalhada no Brasil por Cláudia Lima Marques (DIDIER JR.; ZANETI JR., 2019).

Ao tratar da atuação do Ministério Público na tutela coletiva quanto à proteção de dados pessoais, Vladimir Aras afirma que:

> O Ministério Público é uma instituição de promoção e de defesa de direitos da pessoa humana e da coletividade. Em linha com o art. 127e art. 129, incisos I, II e II, cumpre-se promover, na competência cível e criminal, os direitos de todos, sejam vítimas de crimes ou pessoas atingidas em seus direitos individuais indisponíveis, coletivos e difusos.
> A proteção de dados pessoais é um novo campo de atuação do Ministério Público na tutela coletiva, tarefa que deverá ser desempenhada por seus membros no âmbito dos Estados, do Distrito Federal e na jurisdição federal, por meio de inquéritos civis e ações civis públicas e de improbidade administrativa. Quando atinente à tutela coletiva em sentido amplo, essa atividade do Parquet poderá fundar-se na violação da própria LGPD, do CDC ou do MCI ou de outras leis aplicáveis, sendo pertinente considerar também a disciplina processual prevista no próprio CDC e na Lei de Ação Civil Pública (Lei nº 7.347/1985), sobretudo para a tutela de direitos dos consumidores (art. 1º, inciso II), relativos à honra e à dignidade de grupos raciais, étnicos ou religiosos (inciso VII) e de qualquer outro interesse difuso ou coletivo (inciso IV). (ARAS, 2022, p. 112).

Ademais, além da atuação do órgão ministerial, é possível extrair da leitura conjunta do art. 5º da LACP e do art. 82 do CDC a presença de outros legitimados para a tutela de direitos transindividuais envolvendo a proteção de dados pessoais. Portanto, em nítida aplicação do princípio da integratividade do microssistema processual coletivo, pode-se afirmar a existência de outros legitimados na tutela da autodeterminação informacional, tais como a Defensoria Pública, os entes federativos (União, estados, Distrito Federal e municípios), as entidades da administração indireta (autarquias, empresas públicas, fundações e sociedades de economia mista), os órgãos da Administração Pública, direta ou indireta, ainda que

---

Civil e da LACP para defesa de direitos “difuso, coletivos, e individuais, no que for cabível, os dispositivos do Título III da Lei 8.078, de 11.09.1990, que instituiu o Código de Defesa do Consumidor. Com isso criou-se a novidade de um microssistema processual para as ações coletivas [...] A disciplina comum das ações coletivas no Brasil encontra-se, portanto, no Título III do CDC, que representa, por ora, o “Código Brasileiro de Processos Coletivos”. Chega-se a essa conclusão, como foi visto, pela interpretação sistemática entre as regras do art. 21 da LACP e a do art. 90 do CDC.’ (DIDER JR, Fredie; ZANETI JR, Hermes. Curso de Direito Processual Civil: processo coletivo. Salvador: JusPodvim, 2019, pp. 68-70)

sem personalidade jurídica, mas destinados à defesa de interesses protegidos pelo CDC (por exemplo o PROCON) e as associações em sentido amplo, abrangendo além das associações em sentido estrito, as entidades de classe, os sindicatos e os partidos políticos.

Além dessa questão transindividual que os sistemas automatizados de decisão apresentam, as barreiras técnicas e o sigilo corporativo, travestidos na condição de opacidade dos sistemas de aprendizado de máquina conforme exposto no primeiro capítulo do trabalho, representam problemas significativos para a eficácia do exercício do direito de explicação. A obtenção de explicações significativas sobre o funcionamento dos sistemas automatizados de decisão está intrinsecamente associada à efetiva acessibilidade e compreensibilidade das informações que servem de insumos ao desenvolvimento dessas tecnologias.

Nesse viés, a acessibilidade das informações sobre a funcionalidade dos algoritmos costuma ser intencionalmente pouco acessível, em razão de envolver sigilo comercial, segurança dos sistemas ou a própria privacidade dos usuários (MITTELSTADT *et al*, 2016). No que diz respeito à compreensibilidade, a opacidade dos algoritmos, em especial dos sistemas que empregam aprendizado de máquina, criam barreiras relacionados a interpretabilidade dos resultados dos sistemas diante de processos complexos de tomada de decisão que muitas vezes não são acessíveis e compreensíveis (MITTELSTADT *et al*, 2016).

Em que pese o nível de desenvolvimento da tecnologia estar associado à opacidade e às dificuldades de se garantir transparência a respeito da funcionalidade dos sistemas automatizados de decisão, atualmente uma das questões que representa verdadeira barreira para ampliar a acessibilidade das informações é a forma intencional de autoproteção das empresas em manter seus segredos comerciais e vantagens competitivas no desenvolvimento dos algoritmos.

Nesse ponto, a Lei Geral de Proteção de Dados (LGPD) [33] é expressa, em seu §1º do art. 20, ao restringir o exercício do direito à explicação quando envolver os segredos comercial e industrial. A legislação brasileira, tal como a europeia, acaba sendo muito genérica quanto a essa limitação, o que sem dúvida coloca em risco a própria aplicabilidade do exercício do direito à explicação.

[33] “Lei 13.709/2018. Art. 20 [...] § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial”. (BRASIL, 2018)

Ademais, conforme exposto no primeiro capítulo, as barreiras relacionadas aos negócios acabam se confundindo entre integridade do sistema e rivalidade econômica, no contexto em que a ocultação das informações, são muito empregadas como estratégias pelos controladores de dados (BAYAMLIOGLU, 2021). Ademais, o emprego de uma ressalva genérica, tal como ocorre na LGPD (art. 20, §1º), no intuito de tutelar segredos empresariais dá uma carta em branco aos controladores de dados, além de constituir uma limitação que potencializa a capacidade dos responsáveis pelo tratamento de coletar dados, fazer inferências e construir perfis, sem qualquer diálogo com a sociedade para discutir se as práticas de processamento são normativamente aceitáveis (WACHTER; MITTELSTADT, 2019).

Desse modo, todas as questões levantadas colocam em dúvida se o direito à explicação realmente seria um remédio eficaz para dirimir os problemas de discriminação e injustiça ocasionados pelo uso de sistemas automatizados de decisão. Realmente se não existem justificativas *ex ante* que viabilizem informações sobre a lógica subjacente da funcionalidade dos sistemas automatizados de decisão, torna-se muito difícil e custoso que os destinatários desses sistemas consigam obter esclarecimentos necessários e suficientes para verificar individualmente a caracterização de eventuais injustiças ou discriminações.

Por esses motivos, confiar no direito à explicação como meio para que os usuários assumam o controle dos sistemas permite a criação de uma “falácia da transparência”, pois os indivíduos não têm poder de fazer uso do tipo de explicações algorítmicas que provavelmente lhes serão oferecidas (EDWARDS; VEALE, 2017). Com efeito, Selbst e Barocas (2018) reforçam que as explicações dos sistemas técnicos são necessárias, mas não suficientes para alcançar metas de leis e políticas que se preocupam com garantias voltadas à existência de uma maneira de avaliar a tomada de decisões realizadas por algoritmos.

Por essa razão, Wachter e Mittelsatadt (2019) apontam que a abordagem processual na legislação europeia de proteção de dados para proteger a privacidade dos indivíduos concentra-se em mecanismos para gerenciar a entrada do processamento dos dados (supervisão e controle sobre como os dados pessoais são coletados e processados), deixando de prever mecanismos mais contundentes quanto a dados inferidos e derivados, perfis e decisões. Esse mesmo raciocínio pode ser aplicado à LGPD.

Nesse contexto, diante da existência de lacunas legislativas envolvendo os sistemas automatizados de decisão, abre-se um amplo leque de opções ao exercício de autonomia privada das empresas. Os controladores de dados praticamente definem o propósito e a relevância dos dados e metadados coletados e submetidos ao tratamento, bem como a partir de qual ponto haverá sigilo das regras que regem o processo de tomada de decisão sob o manto do “segredo comercial e industrial”.

A falta de transparência a respeito da identificação explícita dos critérios utilizados no tratamento dos dados pelos controladores inexoravelmente afeta o exercício do contraditório e da ampla defesa, mitigando a possibilidade de resistência quanto às externalidades negativas advindas dos sistemas automatizados que possam afetar ou colocar em risco a autodeterminação informacional. Com efeito, as informações prestadas aos indivíduos sobre a tomada de decisão algorítmica devem ser fornecidas de forma suficiente para que um indivíduo possa efetivamente agir, caso contrário restaria inviabilizado o direito de revisão ou contestação das imprecisões apresentadas nos dados de saída.

O RGPD europeu, ao prever um direito de contestação como salvaguarda, demanda que seja viabilizado aos indivíduos, em um determinado grau, esclarecimentos necessários a respeito dos fatores relevantes para a tomada de cisão automatizada. Nesse sentido, Kaminski (2018, p. 213) pondera que “se alguém tem o direito de correção, precisa ver os erros”, caso contrário, “as assimetrias de informação tornam os direitos subjacentes efetivamente nulos”.

Por essa razão, ao combinar transparência e compreensibilidade, Malgieri e Comandé (2017, p. 03) propõem o conceito de legibilidade que deve garantir a “capacidade autônoma dos indivíduos para entender o funcionamento e o impacto de algoritmos que lhes digam respeito”. Por essa razão, a falta de transparência a respeito dos critérios e métodos usados para a criação de perfis e realização de inferências demanda o desenvolvimento de mecanismos de governança que promovam os direitos fundamentais e assegurem a autodeterminação informacional dos destinatários dos sistemas automatizados de decisão.

Em face disso, propõe-se uma análise holística da LGPD que contemple os direitos à revisão e explicação como vetores instrumentais de um devido processo legal substancial, que juntamente com outras ferramentas, têm como função fortalecer a defesa da autodeterminação informacional no contexto do uso de sistemas automatizados de decisão. Ainda que o direito à revisão e à explicação

previstos no art. 20 da LGPD revelem-se, de forma isolada, como ferramentas incompletas, é possível extrair do referido dispositivo uma espécie de devido processo legal constituído por um bloco de direitos em relação aos sistemas automatizados de decisão (FRAZÃO, 2018c).

Esses direitos basicamente seriam constituídos por: i) direito de acesso a informação; ii) direito de oposição; iii) direito de revisão, e iv) direito de petição à autoridade nacional para a realização de auditoria (FRAZÃO, 2018c). Além disso, o art. 20 da LGPD representa um verdadeiro “dever de governança” (LÓPEZ, 2021) que está conectado com a estrutura deontológica constante no art. 6º da LGPD, em especial com os princípios da transparência e da *accountability*.

Com efeito, embora a LGPD seja omissa quanto aos desdobramentos dos sistema automatizados de decisão, é possível afirmar que “o tratamento de dados automatizados submete-se às regras gerais de utilização e tratamento de dados” (LIMA; FREIRE DE SÁ, 2020), o que sem dúvida envolve a necessidade da observância dos princípios (art. 6º), da existência de base legal para a realização do tratamento de dados (art. 7º), da observância dos direitos e garantias dos titulares de dados (art. 18), da responsabilização civil por danos gerados em razão do tratamento de dados (art. 42), da realização de programas de conformidade ou integridade com a LGPD (arts. 50 e 51), dentre outros dispositivos que podem ser relacionados ao contexto do uso de tratamento de dados.

O §1º do art. 20 da LGPD ao prever o direito de revisão, demanda que seja viabilizado aos indivíduos, em um determinado grau, esclarecimentos necessários a respeito dos fatores relevantes para a tomada de decisão automatizada, porquanto o direito à explicação é corolário lógico do direito de revisão dos sistemas automatizados de decisão (FRAZÃO, 2021). Portanto, o direito a explicação possui um valor instrumental na materialização da transparência, seja através da obrigação de informações significativas sobre a lógica envolvida, seja através da legibilidade, conferindo aos indivíduos direito a justificativas prévias sobre a funcionalidade dos sistemas automatizados de decisão (KAMINSKI, 2019; SELBST; POWLES, 2017).

Nesse sentido, Frajhof (2022) aponta que para atender ao comando do art. 20 da LGPD é imprescindível a adoção de uma série de medidas prévias e posteriores, ou seja, condutas preventivas e reativas, que viabilizem uma verdadeira *accountability* algorítmica. Portanto, o direito à explicação desloca-se de um eixo central para servir como um dos mecanismos de implementação da *accountability*,

de modo a reforçar a transparência e a responsabilização dos controladores de dados.

Diante do que acima exposto, é possível afirmar que todos os estágios de tratamento de dados que envolvam a construção de perfis e a realização de inferências por sistemas automatizados de decisão estarão sujeitos a diversas exigências jurídicas da LGPD que constituem verdadeiros mecanismos de governança para os agentes responsáveis pelo tratamento de dados. Assim, os controladores do tratamento de dados devem viabilizar transparência e *accountability* a respeito dos seus sistemas automatizados de decisão, sob pena de responder pelos danos advindos de violações ou tratamentos inadequados (MULHOLLAND, 2020).

Para tanto, passa-se à análise dos demais mecanismos de governança que podem ser extraídos da LGPD e que estão relacionados à estruturação normativa do direito a inferências razoáveis. Nesse raciocínio, impõe-se retomar a racionalidade *ex ante* de proteção de dados (BIONI; MENDES, 2020) que demanda como premissa que qualquer tratamento de dados tenha uma base legal, bem como a presença do legítimo interesse do controlador de dados, o qual deve estar em harmonia com a legítima expectativa do titular de dados e os direitos e garantias fundamentais.

4.2 LEGÍTIMO INTERESSE COMO INSTRUMENTO DE *ACCOUNTABILITY* ALGORÍTMICA

A Lei Geral de Proteção de Dados Pessoais (LGPD), inspirada no regulamento europeu, dispõe em seu artigo 7º as hipóteses legais que autorizariam o tratamento de dados pessoais. O referido dispositivo representa de forma concomitante uma garantia ao titular de dados, quanto ao dever de respeito dos direitos e garantias fundamentais na realização do tratamento de dados, e ao mesmo tempo um direito aos controladores legitimando a sua atuação em conformidade com o desenvolvimento econômico, financeiro e incentivo à inovação.

As hipóteses que autorizam o tratamento de dados pessoais estão previstas da seguinte forma:

> 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;
> 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; (Redação dada pela Lei nº 13.853, de 2019)
> 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. (BRASIL, 2018)

Da leitura do dispositivo é possível constatar que as bases legais são enquadradas conforme as circunstâncias concretas e a finalidade do tratamento de dados. Desse modo, em uma primeira leitura da lei é possível observar a existência de uma aplicação abrangente que englobaria várias atividades de tratamento, as quais podem ser executadas por motivos diferentes (BLUM; FURTADO, 2021).

Dentre as bases legais que autorizam o tratamento de dados, o legítimo interesse (art. 7º, IX) revela-se como elemento essencial para a mitigação dos riscos oriundos da implementação de sistemas automatizados de decisão. Isso porque o legítimo interesse tem uma abordagem essencialmente preventiva, que ao mesmo tempo que serve como um fundamento para os controladores de dados projetarem seus sistemas, representa a assunção de obrigações e deveres jungidos às diretrizes principiológicas da LGPD.

Nesse ponto, embora o conceito de legítimo interesse possa denotar uma natureza jurídica indeterminada, Bruno Bioni (2021) apresenta os critérios norteadores para a sua aplicação, destacando que o art. 7º, inciso IX, deve ser lido em conjunto com a integralidade do art. 10 da LGPD, a saber:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. (BRASIL, 2018)

Segundo Bioni (2019), o teste multifatorial de legítimo interesse (*Legitimate Interests Assessment* – LIA) está estruturado em quatro passos. No primeiro, realiza-se a aferição da existência do legítimo interesse com base na finalidade legítima e na situação concreta (art. 10, caput e inciso I, da LGPD). Em um segundo momento, verifica-se a necessidade (art. 10, §1º, da LGPD), ou seja, se os dados coletados são realmente aqueles necessários (princípio da minimização) para se atingir a finalidade pretendida (BIONI, 2019). Em um terceiro passo, materializa-se a principal fase consistente no teste de proporcionalidade na qual sopesam-se os interesses do controlador diante dos interesses do titular dos dados (art. 10, II, da LGPD).

Segundo Bruno Bioni:

> Deve-se perquirir: c.1) se o novo uso atribuído ao dado está dentro das legítimas expectativas do titular dos dados. Isso é parametrizado pela noção de compatibilidade entre o uso adicional e aquele que originou a coleta dos dados pessoais. Eles devem ser próximos um do outro, demandando-se uma análise contextual para verificar se esse uso secundário seria esperado pelo titular dos dados. Aliás, não foi por outra razão a escolha do termo "legítimo", o qual qualifica não só a base legal em questão, mas também o princípio da finalidade; e c.2) de que forma os titulares dos dados serão impactados, especialmente repercussões negativas em termos de discriminação e sobre a sua autonomia (liberdades e direitos fundamentais). Caso, mas não necessariamente, o tratamento de dados também os "beneficie", a balança tende a estar equilibrada. (BIONI, 2021, pp. 165-166)

Com efeito, o inciso II do art. 10 da LGPD apresenta os elementos centrais para a operacionalização do processo do legítimo interesse, consignando que o tratamento de dados realizado pelo controlador deve respeitar as legítimas expectativas do titular dos dados, assim como os seus direitos e liberdades

fundamentais. Nesse sentido, o *Working Party article 29* (WP29) aponta que um interesse somente pode ser considerado legítimo se o controlador perseguir um interesse que esteja em conformidade com a lei de proteção de dados (*EUROPEAN COMMISSION*, 2014).

Portanto, dentre os principais fatores de avaliação do legítimo interesse pode-se afirmar que a parametrização é baseada na legítima expectativa do titular dos dados e os impactos que o tratamento dos dados pode gerar nas liberdades de direitos fundamentais. Desse modo, quando os sistemas automatizados realizam inferências e criam perfis que serão objeto de insumo de decisões de aprendizado de máquina o balanceamento dos interesses em jogo pode acarretar desequilíbrio diante das externalidades negativas que impactam na autodeterminação informacional e no livre desenvolvimento da personalidade dos destinatários dessas tecnologias.

Segundo Bucar e Viola (2020), a cláusula geral do interesse legítimo permite certa flexibilidade ao controlador de dados, contudo, ao mesmo tempo lhe traz um ônus argumentativo para demonstrar que atua em conformidade com a lei. Portanto, a operacionalização do legítimo interesse por parte dos controladores de dados é um ônus argumentativo, de modo a viabilizar que o tratamento de dados atenda as finalidades e adequações do sistema em consonância com as liberdades e direitos dos indivíduos, viabilizando uma transparência no tratamento de dados e a prestação de contas através do registro das operações realizadas (BIONI; 2019).

Por fim, como último passo do teste multifatorial de legítimo interesse (LIA), Bioni (2019) elenca os mecanismos de salvaguardas (art. 10, §§2º e 3º, da LGPD) que basicamente são: i) a observância do princípio da transparência; ii) a existência de mecanismos de oposição (*opt-out*) e iii) a mitigação dos riscos.

A relação entre as três salvaguardas é assim apresentada por Bruno Bioni:

> Não é porque o legítimo interesse prescinde do consentimento do titular que a atividade de tratamento de dados deve ser opaca. Pelo contrário, reforça-se d.1) o dever de transparência. Objetiva-se, com isso, franquear ao cidadão d.2) poder de tomada de decisão para se opor a tal atividade de tratamento de dados (opt-out), podendo optar por estar fora do que considera ser incompatível com as suas legítimas expectativas. E, por fim, d.3) o controlador dever adotar ações que mitiguem os riscos do titular dos dados (v.g., anonimização dos dados), sendo este o sentido da previsão da eventual necessidade elaboração de relatório de impacto à privacidade na LGPD. (BIONI, 2021, p. 166)

Portanto, verifica-se que a transparência, como mecanismo de salvaguarda no teste multifatorial, está relacionada com o princípio da explicabilidade (*answerability*), a qual viabilizaria ao titular de dados informações úteis sobre o tratamento de dados que permitissem uma avaliação quanto à compatibilidade ou não do procedimento em relação às suas legítimas expectativas. Até porque "se uma pessoa não sabe o que acontece com seus dados, não poderá se proteger" (ROSENVALD; FALEIROS JÚNIOR, 2022, p. 776).

Segundo Rosenvald e Faleiros Júnior (2022, pp. 776-777), a *answerabilty*, "materializada no dever recíproco de construção da fidúcia a partir do imperativo da transparência", "é um procedimento recíproco de justificação de escolhas que extrapola o direito à informação, facultando-se a compreensão de todo o cenário da operação de tratamento de dados para agente e titular". Por essa razão, os referidos autores apontam que a explicabilidade representa uma verdadeira camada adicional na função preventiva da responsabilidade dos controladores de dados.

Portanto, como desdobramento do legítimo interesse, o direito de oposição (*opt-out*) pode ser extraído do parágrafo segundo do art. 18 da LGPD e revela-se como um verdadeiro mecanismo de salvaguarda (BIONI, 2019) que franqueia aos indivíduos a possibilidade de se opor às atividades de tratamento de dados, o que incluiria a exigência de justificativas *ex post* a respeito das inferências realizadas pelos sistemas automatizados de decisão. Nesse viés, o direito de oposição da LGPD guarda muita semelhança ao direito de contestação previsto no art. 22 do RGPD.

Nesse ponto, dentre os fatores de avaliação necessários para a materialização do legítimo interesse, o balanceamento do tratamento de dados com a legítima expectativa e os direitos e liberdades fundamentais (art. 7º, IX c/c art. 10, II, da LGPD) representam um eixo central no estabelecimento de diretrizes para o desenvolvimento de mecanismos que mitiguem os riscos e fortaleçam a transparência dos sistemas automatizados de decisão.

Por essa razão, as salvaguardas referente às ações do controlador voltadas à mitigação dos riscos devem ser analisadas em harmonia com os programas de conformidade e *compliance*, traduzidos na observância dos princípios estruturais, das boas práticas e governança que devem ser adotadas pelos controladores de tratamento de dados como forma de mitigar os riscos nas suas atividades. Somente assim os controladores de dados podem cogitar em afastar eventual

responsabilização por danos causados aos destinatários dos sistemas automatizados de decisão (CAITLIN; GOMES).

Por fim, além do princípio da transparência, objeto de verificação sob uma perspectiva de salvaguarda, deve-se ter em conta que a avaliação das condições de legitimidade de tratamento de dados, em uma perspectiva da racionalidade *ex ante* de proteção de dados (MENDES; 2019, p. 47), demanda uma análise conjunta da estrutura principiológica prevista no art. 6º da LGPD.

Desse modo, considerando que os princípios da LGPD constituem pressupostos argumentativos para qualquer das possibilidades de tratamento dos dados pessoais (BUCAR; VIOLA, 2020), passa-se à análise da estrutura deontológica que serve de diretriz ao *enforcement* da legislação protetiva de dados na consolidação de mecanismos de governança que viabilizem uma *accountability* algorítmica.

4.3 GUIAS DEONTOLÓGICOS

Inicialmente torna-se relevante registrar que a regulação baseada em princípios pode ser vista como um compromisso com a governança, como autorregulação e corregulação (LATZER; JUST, 2020). Tal raciocínio, reforça a ideia da corregulação como um mecanismo de harmonização de várias formas de atuação no intuito de se garantir uma adequada ferramenta para responder aos problemas complexos que emergem da utilização das tecnologias atuais (SILVA, 2012).

O debate, quando envolve a utilização de princípios e o desenvolvimento de tecnologias, centra-se em tornar transparente o funcionamento dos sistemas. Tal finalidade permite a utilização de soluções técnicas e ferramentas disponíveis para aprimorar o processamento dos dados que são coletados, de modo a mitigar os efeitos de injustiça e discriminação, bem como definir quem seria o responsável pelos efeitos da tomada de decisão algorítmica (LATZER; JUST, 2020).

Seguindo o fluxo internacional na regulamentação de proteção de dados, a Lei Geral de Proteção de Dados (LGPD) consagrou uma estrutura principiológica significativa ao abordar diversas obrigações a serem observadas pelos controladores de dados. Dentre os princípios mais relevantes quando se trata de sistemas automatizados de decisão, destacam-se os da transparência (artigo 6º, VI);

da adequação (artigo 6º, II); da prevenção (artigo 6º, VIII); da não discriminação (artigo 6º, IX) e da responsabilização e prestação de contas (artigo 6º, X).

Conforme dispõe a LGPD o princípio da transparência garante aos destinatários dos tratamentos de dados informações claras, precisas e facilmente acessíveis sobre a realização desses tratamentos, ressalvando os segredos comercial e industrial (art. 6º, VI). Nesse sentido, o princípio da transparência demanda que a realização de qualquer tratamento de dados pessoais não pode ser perfectibilizada sem o conhecimento do titular dos dados, “que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento (DONEDA; 2021, p. 682).

Por sua vez, o princípio da adequação orienta a realização de um tratamento de dados compatível com as finalidades informadas ao titular e especialmente de acordo com o contexto do tratamento (art. 6º, II). Ou seja, “os dados armazenados devem ser fiéis à realidade, atualizados, completos e relevantes”, bem como a coleta e o tratamento de dados deve ser feita com cuidado e correção (DONEDA; 2021, p. 682).

O princípio da prevenção espelha a adoção de mecanismos baseados na gestão de risco que evitem a ocorrência de danos em virtude do tratamento de dados (art. 6º, VIII), enquanto o princípio da não discriminação serve como diretriz para evitar tratamento de dados com finalidade discriminatória ilícita ou abusiva (art. 6º, IX).

Por fim, os princípios da responsabilização e da prestação de contas visam garantir a efetiva tutela de garantias e direitos dos destinatários de tratamento de dados (art. 6º, X), de modo que constituem o denominado princípio da *accountability*, demandando a criação de instrumentos vocacionados a identificação e mitigação de riscos, conforme foi devidamente detalhado no tópico anterior.

Conforme Mulholland e Gomes ponderam (2022), a estrutura principiológica da LGPD constitui um instrumento para regulação da inteligência artificial tendo como pressuposto o desenvolvimento de uma IA confiável e auditável. Para tanto, os princípios éticos que orientam o desenvolvimento e a utilização dos sistemas de IA buscam fomentar ao agente de tratamento a função de mitigar os riscos nas atividades de tratamento de dados pessoais. Essa mitigação dos riscos está relacionada à garantia da transparência.

A busca de alternativas que viabilizem maior transparência no desenvolvimento de tecnologias que empregam inteligência artificial tem sido objeto de vários estudos a nível internacional e tem sido objeto de pesquisas focadas no estabelecimento de princípios destinados a fornecer uma orientação normativa para o desenvolvimento dessas tecnologias.

Um estudo coordenado por Luciano Floridi (2018), com a finalidade de propor recomendações para o desenvolvimento de uma “Boa Sociedade de IA”, apontou quatro princípios, não exaustivos, extraídos da bioética e que se adaptam bem aos novos desafios éticos colocados pela inteligência artificial: beneficência, não maleficência, autonomia e justiça. Além desses, Floridi *et al* (2018) defendem o princípio da explicabilidade, o qual incorporaria tanto a intelegibilidade quanto a responsabilidade.

Nesse viés, os princípios da beneficência e não maleficência desempenham um papel relevante quando se propõe à análise de mecanismos para a implementação de transparência nos algoritmos decisórios. Isso ocorre, porque ambos os princípios se revestem de caráter preventivo.

Segundo o princípio da beneficência, as tecnologias devem ser desenvolvidas a favor do ser humano, promovendo o bem-estar, dignidade e o bem comum das pessoas, da sociedade e do planeta (MAGRANI; GUEDES, 2022). Por sua vez, segundo o princípio da não maleficência o desenvolvimento da IA deve estar focado na precaução, buscando o estabelecimento de mecanismos que compreendam as limitações das tecnologias de IA e gerencie os riscos associados, de modo a evitar danos previsíveis e não intencionais (GUSZCZA *et al*., 2020).

Portanto, para que os sistemas automatizados de decisão funcionem de forma confiável os controladores de dados devem tomar medidas preventivas para identificar e mitigar os riscos oriundos das limitações relacionadas ao emprego de algoritmos de aprendizado de máquina. Nesse sentido, James Guszcza *et al*. (2020) propõem algumas táticas a serem observadas pelos controladores de dados, que poderiam estar em harmonia com o princípio da não maleficência, tais como: i) avaliar a proveniência dos dados de treinamento (por exemplo, quais inferências foram extraídas dos dados e quão relevante essas inferências são para a situação concreta); ii) restringir o uso de algoritmos para ambientes em que provavelmente não serão confiáveis, tratando a autonomia total da máquina como casos excepcionais, e iii) assumir um padrão de colaboração entre o computador e o

humano, porquanto este último teria maior capacidade para desenvolver raciocínios baseados no bom senso e tomar decisões flexíveis.

De igual modo, o Grupo de Especialistas de Alto Nível em Inteligência Artificial da Comissão Europeia (*High-Level Expert Groupon Artificial Intelligence* – AI HLEG), publicou documento denominado “Orientações Éticas para uma IA de Confiança” *(Ethic Guidelines For Trustworthy AI*). Da leitura do referido estudo é possível extrair quatro princípios éticos que devem ser observados para assegurar que os sistemas de inteligência artificial sejam desenvolvidos, implementados e utilizados de forma confiável, quais sejam: i) respeito à autonomia humana; ii) prevenção de danos; iii) equidade, e iv) explicabilidade (*EUROPEAN COMMISSION*, 2019). Com efeito, nota-se que essas orientações buscam servir como parâmetro para que sejam adotadas medidas adequadas no intuito de atenuar ou prever a dimensão dos riscos oriundos da implementação de Inteligência Artificial, o que inexoravelmente envolve o processamento e tratamento de dados por sistemas automatizados de decisão.

Ademais, no referido documento, o AI HLEG elencou entre a formas de combate a opacidade dos algoritmos o princípio da explicabilidade, que tem como objetivo viabilizar que os indivíduos possam compreender a engrenagem articulada pelos sistemas que empregam alguma modalidade de inteligência artificial (*EUROPEAN COMMISSION*, 2019). Portanto, evidencia-se que o princípio da explicabilidade está nitidamente ligado à ideia de transparência e é fundamental para manter a confiança dos destinatários dos sistemas automatizados de decisão.

No mesmo sentido, o princípio da equidade na sua dimensão processual implicaria a possibilidade de contestar ou de se contrapor de forma eficaz contra as decisões tomadas por sistemas de inteligência artificial (*EUROPEAN COMMISSION*, 2019). Tal como a transparência, o princípio da equidade conecta-se ao princípio da explicabilidade, pois se as decisões não são explicáveis aos destinatários dos sistemas automatizados de decisão, dificilmente será possível contestar ou se insurgir contra eventuais decisões oriundas do aprendizado de máquina.

Em recente publicação, o projeto denominado “*Principled Artificial Intelligenc: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*”, conduzido por Jessica Fjeld e seus colegas, propõe um mapa principiológico para orientação dos formuladores de políticas públicas, acadêmicos e pesquisadores, entre outros que trabalhem na linha de frente com temas envolvendo danos das

tecnologias de IA. No referido estudo foram identificados oito temas principais: i) privacidade; ii) prestação de contas (responsabilidade); iii) segurança e proteção; iv) transparência e explicação; v) justiça e não discriminação; vi) controle humano da tecnologia; vii) responsabilidade profissional e viii) promoção dos valores humanos.

Novamente, no referido estudo, ficou evidenciado um nexo de interdependência entre a responsabilidade (prestação de contas), transparência e explicação. “Os princípios de responsabilização são frequentemente mencionados juntamente com o princípio da IA transparente e explicável, muitas vezes destacando a necessidade de responsabilização como meio de ganhar a confiança do público na IA e dissipar os medos” (FJELD *et al*., 2020, p. 29). Ademais, a capacidade de contestar as decisões automatizadas também está relacionada a uma camada do princípio da responsabilidade (FJELD *et al*., 2020).

Seguindo essa linha de raciocínio, Luciano Floridi *et al*. (2018) ponderam a importância da necessidade de compreender os processos de tomada de decisão da IA, cujo funcionamento frequentemente é invisível ou ininteligível para a maioria das pessoas. Portanto, o princípio da explicabilidade desponta como um elemento crucial na delimitação da responsabilização dos controladores de dados, pois para que seja possível analisar se a IA é benéfica ou não, se promove ou não a autonomia humana, se é justa ou injusta, torna-se imprescindível viabilizar a capacidade de compreensão a respeito do seu funcionamento (FLORIDI *et al.*, 2018).

Apresentada a estrutura principiológica que deve ser norte de atuação dos responsáveis pelo tratamento de dados, propõe-se a análise das regras de boas práticas e governança de dados” que se revelam como importantes instrumentos para a materialização do *compliance* na busca de *accountability* (FRAZÃO, 2022).

4.4 REGRAS DE BOAS PRÁTICAS E GOVERNANÇA DE DADOS

Os artigos 50 e 51 da LGPD consagram a adoção de políticas de boas práticas e governança de dados, impondo aos controladores de dados a obrigação do fornecimento de informações claras sobre o uso de IA no tratamento dos dados pessoais dos titulares e destinatários dos sistemas, bem como quais a finalidades e resultados esperados em tais aplicações (CAITLIN; GOMES, 2022). Nesse contexto, em conformidade com o princípio da responsabilidade, os controladores de dados

responsáveis pela implementação de sistemas avançados de IA, tal como decisões automatizadas, devem ser considerados partes interessadas nas implicações morais de seu uso (MAGRANI, 2019).

Portanto, a LGPD, ao prever mecanismos de boas práticas e governança, procura “estimular uma postura proativa por parte de agentes de tratamento de dados pessoais” (CARVALHO; MATTIUZZO; PONCE, 2021, p. 361). Ademais, a implementação de uma política de boas práticas está longe de ser uma lista de *checkboxes (*CARVALHO; MATTIUZZO; PONCE, 2021). Nesse sentido, o parágrafo segundo do art. 50 destaca que a implementação do programa de governança levará em conta “a estrutura”, “a escala” e “o volume de operações”, além da probabilidade e gravidade dos danos para os titulares dos dados em razão do tratamento de dados realizado pela empresa.

Embora a implementação da política de boas práticas não seja uma *chekboxes*, o inciso I do parágrafo segundo do art. 50 da LGPD apresenta um rol mínimo de requisitos que um programa de governança em privacidade deve conter, a saber: “a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Da análise dos requisitos mínimos para a implementação de um programa de governança de dados, chama à atenção o conteúdo do parágrafo segundo do art. 50 e da alínea “d” constante no inciso I do mesmo parágrafo da LGPD. No parágrafo segundo há expressa menção quanto à necessidade que o controlador de dados se atente para a “probabilidade e a gravidade dos danos para os titulares dos dados”,

enquanto na alínea “d” do inciso I do mesmo parágrafo consta que na implementação do programa de governança o controlador deverá estabelecer “políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade”.

Nesse sentido, as boas práticas e governança de dados recomendam a análise de impacto e avaliação de risco pelas empresas que pretendem colocar em serviço ou no mercado uma IA de alto risco, realizando uma avaliação de conformidade prévia (MAGRANI; CAMPELLO; OLIVEIRA; 2021). De igual modo, a elaboração e manutenção de relatórios é um ponto benéfico para eventuais auditorias que funcionam como mecanismos de *compliance* e de governança.

Segundo Carvalho, Mattiusso e Ponce (2021), a identificação de riscos pelas empresas na realização de tratamento de dados é uma questão fundamental no desenvolvimento de quaisquer medidas de boas práticas. Embora a LGPD não apresente nenhum rol de atividades de tratamento que possam ser consideradas de alto risco, a legislação indica a probabilidade e gravidade dos riscos como um critério a ser considerado no desenvolvimento de medidas de governança (art. 50, §1º).

Além disso, dentre os princípios e boas práticas éticas difundidas e aceitos pela comunidade internacional e que devem servir de base para a elaboração de políticas de empresas e da discussão legislativa destaca-se a explicabilidade que se divide em duas ideias principais: intelegibilidade e *accountability* (FLORIDI; COWLS, 2019). Desse modo, programas de governança de dados devem primar pelo desenvolvimento de requisitos técnicos que incorporem conceitos de proteção da autodeterminação informacional desde a concepção dos sistemas e projetos que envolvam a utilização de aprendizado de máquina.

A implementação de transparências em camadas mais complexas de tecnologias demandam a proteção de dados por projeto (*by design*) ou por padrão (*by default*). Nesse sentido, ‘tanto a Lei 13.709/2018 (a Lei Geral de Proteção de Dados, ou “LGPD”) quanto o Regulamento Geral de Proteção de Dados (*General Data Ptocection Regulation*, ou “GDPR”) europeu têm como aspecto fundamental o princípio de que a privacidade deve ser protegida desde a concepção de um produto ou serviço, e que esta preferência deve ser mantida da mesma forma por todos os ciclos de desenvolvimento e inovação’ (ARBIX, 2020, pp. 56-57).

A política *privacy by design* desenvolvida originalmente na década de 1990 pela Comissária de Informação e Privacidade de Ontário, Canadá, Dra. Ann Cavoukian (MORASSUTTI, 2019). A *privacy by design* seria uma metodologia na qual a proteção de dados pessoais é pensada desde a concepção dos sistemas e projetos que envolvam a utilização de tecnologias, os quais se alimentem de dados e informações constantes na internet (MORASSUTTI, 2019, p. 76).

No plano europeu, o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia aborda expressamente sobre privacidade por projeto em seu artigo 25 (UNIÃO EUROPEIA, 2016), denominado proteção de dados por *design* e por padrão *(data protection by design and by default)*. O referido diploma sublinha a necessidade de implementação de medidas técnicas na tutela da privacidade quando do desenvolvimento das tecnologias, bem como a observância dos princípios de proteção de dados de forma a proteger os direitos dos titulares dos dados (UNIÃO EUROPEIA, 2016).

Por sua vez, “a LGPD eleva *Privacy by Design and Default* ao *status* de princípio norteador das atividades que serão realizadas pelos agentes de tratamento” (ARBIX, 2020, p. 57). Tal perspectiva, viabiliza a construção de um verdadeiro *tecnhological enforcement* na qual a proteção de dados seria autoexecutável pelo próprio sistema tecnológico (MODENESI, 2021).

Na LGPD, o princípio da *privacy by design and default* pode ser extraído da leitura conjunta do parágrafo quinto do art. 35 e do art. 46, ambos da LGPD, a saber:

> Art. 35 [...] § 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei [...]
> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. (BRASIL, 2018)

Consoante a legislação, as medidas técnicas e organizacionais adotadas pelos operados são essenciais para garantir a observância da estrutura deontológica constante na LGPD. Ademais, essas medidas técnicas devem ser observadas desde a fase da concepção do produto ou do serviço até a sua execução (art. 46, §2º, da LGPD).

Por sua vez, da leitura do parágrafo primeiro do art. 46 observa-se a importância do papel da Agência Nacional de Proteção de Dados na implementação de políticas voltadas à implementação do princípio da *privacy by design and default*. Diante disso, é possível afirmar que "a cooperação com a futura Autoridade Nacional de Proteção de Dados será o caminho para alcançar soluções melhores para as pessoas, as organizações que processam dados, a economia e a sociedade", sem aqui desprezar a o multissetorialismo que está no DNA da LGPD (BIONI; RIELLI, 2021) e materializado na composição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP).

Portanto, a colaboração e diálogo multissetorial entre organizações, representantes da academia, empresas, consumidores e outros agentes públicos é de extrema valia para a construção de políticas públicas voltadas ao desenvolvimento de tecnologias socialmente adequadas. 'Essa abordagem de "design sensível à valores", como privacidade, segurança, ética e direitos humanos, é adequada à ideia de que os benefícios e os efeitos positivos da inteligência artificial não podem ser garantidos apenas pelo cumprimento do quadro regulamentar, mas também assegurados por padrão, desde o início do desenvolvimento dos sistemas e reforçados durante a sua utilização, de acordo com estratégias *by design e by default*.' (MAGRANI; GUEDES, 2022, p. 84).

A utilização da política de *privacy by design and default* demonstra ser uma boa metodologia a ser empregada, embora o desafio, muitas vezes, consista em dar efetividade ao conceito. Neste sentido, cumpre transcrever a lúcida reflexão de Marion Albers sobre o tema:

> Assim como a proteção de dados através do design de sistemas, a proteção de dados através do desenvolvimento, da moldagem e do uso de tecnologia é uma tarefa ambiciosa. E ela depende, da mesma maneira, de clareza e respeito dos objetivos da proteção e dos interesses protegidos, e, incluindo formas de *soft law* e instrumentos diversos, leva o direito referente à proteção de dados para além dos padrões tradicionais do direito regulatório. (ALBERS, 2016, p. 42)

Essas iniciativas de implementação de transparência por projeto visam melhorar a responsabilidade dos controladores de dados e a interpretabilidade dos sistemas de IA de alto risco, tornando os dados de saída (*output*) mais inteligíveis à razão humana, de modo que garanta a confiabilidade e auditabilidade dos sistemas automatizados de decisão, elementos da estrutura principiológica da LGPD.

Nesse contexto, a adoção do direito a inferências razoáveis permitiria viabilizar condutas do próprio desenvolvedor no intuito de traçar caminhos que permitissem eventuais justificativas prévias a questões envolvendo a proteção dos dados e da autodeterminação informacional dos indivíduos afetados pelos sistemas. Nesse viés, Emre Bayamlioglu aponta a importância da regulamentação baseada em *design* com o objetivo de viabilizar que modelos de aprendizado de máquina sejam mais receptivos à explicabilidade e à contestabilidade. Portanto, os controladores de dados devem preferir modelos que podem ser mais facilmente analisados.

A partir disso, revela-se a importância do instituto da *accountability* materializada na legislação mediante a inclusão de mecanismos regulatórios preventivos, em especial numa abordagem voltada à governança baseada na gestão de risco. Para tanto, no próximo capítulo será realizada a análise de uma abordagem de governança baseada em risco dentro do contexto da LGPD.

5 O PAPEL DA GOVERNANÇA DE ALGORITMOS NO CONTEXTO DA LGPD

Diante do que exposto no primeiro capítulo, foi possível constatar que os sistemas automatizados de decisão possuem desafios técnicos significativos na sua mecânica de funcionamento. Ao contrário do que indica o senso comum, decisões algorítmicas não são inquestionáveis, sendo necessário a criação de estratégias para auditagem e desenvolvimento de mecanismos de governança de algoritmos (FERRARI; BECKER; WOLKART, 2018).

Dentre os principais desafios a serem enfrentados destaca-se a falta de transparência, que inviabiliza a identificação explícita dos critérios utilizados no tratamento dos dados pelos controladores. Essa ausência de transparência inexoravelmente afeta o exercício do contraditório e da ampla defesa, dificultando eventual contestação das decisões que colocam em risco a autodeterminação informacional dos destinatários dos sistemas.

Por sua vez, em razão da falta de transparência, resta inviabilizada a estruturação de um procedimento de prestação de contas e a responsabilização dos controladores de dados. A ausência de métodos prévios capazes de avaliar como os algoritmos chegaram à determinada conclusão coloca em risco a própria confiabilidade dos sistemas, porquanto inexistem justificativas que viabilizem uma análise normativa das correlações realizadas pelos algoritmos, de modo que não se tem acesso de forma explícita as regras que regem como as inferências são extraídas no processo do tratamento dos dados realizados pelos sistemas.

Nesse sentido, um estudo publicado pelo Parlamento Europeu, denominado "*A governance framework for algorithmic accountability and transparency"* (Uma estrutura de governança para responsabilidade algorítmica e transparência), destacou que como a injustiça em sistemas algorítmicos tem o potencial de surgir de uma série de fontes, existiriam múltiplas soluções potenciais para enfrentá-la (KOENE, 2019). Nesse viés, ao observar as injustiças resultantes da aplicação de sistemas algorítmicos, o relatório propõe diversos mecanismos de governança que poderiam ser empregados como ferramentas para garantir o desenvolvimento responsável em benefício da sociedade e tendo como foco os direitos humanos (KOENE, 2019).

No presente trabalho o termo “governança”[34] deve ser compreendido como quaisquer processos de coordenação social, não se confundindo e nem se restringindo ao governo, bem como não se limitando à forma hierárquica e verticalizada, baseada no controle direto e formal típico do governo do Estado (VIEIRA; BARRETO, 2019). Nesse panorama, a governança de algoritmos[35] tem por finalidade o estudo de novas formas de vencer as barreiras tecnológicas que influenciam e guiam o comportamento humano e das sociedades, reconhecendo a necessidade de se estabelecer um controle social, seja por meio da lei ou outros mecanismos (LATZER; JUST, 2020) que viabilizem a conformidade do uso da tecnologia com os direitos fundamentais, em especial a proteção dos dados pessoais e da autodeterminação informacional dos indivíduos.

Como opções de estrutura de governança de algoritmos podemos citar a constatação da existência de alguns importantes mecanismos, tais como: i) soluções de mercado; ii) autorregulação; iii) corregulação, e iv) intervenção estatal (Frazão, 2019; Pagallo; Casanovas; Madelin, 2019; Koene *et al*, 2019; Ferrari, 2018; Doneda; Almeida 2016; Saurwein; Latzer, Just, 2015). Como se evidencia as ferramentas de governança se aproximam muito aos fundamentos políticos da regulação dividida em autorregulação, corregulação e heterorregulação (regulação estatal direta), sendo que essas diversidades de modelo de regulação visam a formalizar o equilíbrio entre as formas de legislação de cima para baixo e as abordagens puramente de baixo para cima (PAGALLO; CASANOVAS; MADELIN, 2019).

Tais apontamentos reforçam os motivos pelos quais tem se utilizado o termo “governança” para tratar de diversos temas envolvendo a aplicação de tecnologias com o emprego da inteligência artificial, servindo como um verdadeiro termo guarda-chuva que permite a idealização multissetorial e interdisciplinar de vários *frameworks* para enfrentar os desafios apresentados pelas inovações tecnológicas.

---

[34] Esse tema será melhor desenvolvido na seção 5.1.

[35] O estudo da “governança de algoritmos” parte da constatação da existência de uma “governamentalidade algorítmica” conforme exposto no primeiro capítulo. Nesse contexto, deve-se registrar que a “governança de algoritmos” não se confunde com “governança algorítmica” (ou governança por algoritmos ou algocracia). A governança algorítmica decorre da disseminação das tecnologias de vigilância e o crescimento da Internet das coisas, que permite a manutenção de uma rede interconectada de dispositivos de coleta de dados, atualizados em tempo real, na qual os algoritmos são usados para influenciar, guiar, provocar, controlar, manipular e restringir o comportamento humano (DANAHER *et al*, 2017). Portanto, dentro da concepção denominada “governança por algoritmos”, a tecnologia seria utilizada para exercer um controle social em prol de determinadores *players* que possuem o domínio sobre essas máquinas. Tal percepção é muito similar a “governamentabilidade algorítmica” desenvolvida por Antoinette Rouvroy e Thomas Berns (2015) conforme exposto no primeiro capítulo deste trabalho.

Dentro dessa perspectiva da análise dos mecanismos de governança, Latzer e Just (2020), Koene (2019), Magrani (2018; 2019) e Doneda e Almeida (2016), esclarecem que existem diferentes abordagens voltadas com a mesma preocupação, sendo que a governança pode variar entre aspectos jurídicos e regulatórios até uma postura mais orientada pela intervenção técnica. Nesse contexto, os referidos autores são uníssonos[36] em relacionar algumas abordagens que tentam enfrentar os problemas relacionados aos sistemas de decisão automatizadas, tendo como objeto: i) uma abordagem principiológica com valores éticos; ii) uma abordagem com transparência e *accountability*, e iii) uma abordagem com análise de fatores de risco (*risk-basead approach*); iv) abordagem baseada em direitos humanos.

Deve-se registrar que todas as abordagens merecem a devida atenção e permitem um entrelaçamento significativo de modo a reforçar a proteção da autodeterminação informacional, o livre desenvolvimento da personalidade e a responsabilização pelo uso inadequado dos sistemas de decisões automatizadas numa perspectiva de corregulação.

Contudo, tendo em vista que os mecanismos de *enforcement* da LGPD estão estruturados dentro de uma ideia de corregulação e *accountability,* serão delineadas as opções de estrutura de governança nessa perspectiva, com a abordagem baseada na análise de fatores de risco.

Assim, o próximo tópico busca enfrentar o problema dos desafios regulatórios e investigar os mecanismos de governança algorítmica dentro do contexto da LGPD. De igual modo, serão abordados temas relacionados a uma estrutura de corregulação permeada por uma análise de fatores de risco que garantam maior transparência e responsabilidade por parte dos controladores de dados.

5.1 OPÇÕES DE ESTRUTURA DE GOVERNANÇA: CORREGULAÇÃO E O *ENFORCEMENT* DA LGPD COMO EIXO VALORATIVO

A evolução tecnológica impõe novas proposições de mecanismos de redistribuição de poder, devendo haver maior abertura aos atores sociais e a

[36] Doneda e Almeida (2016) destacam uma abordagem com emprego de garantias técnicas, que ao final também se revelam ferramentas que podem ser encontradas na abordagem com análise de fatores de risco.

reconfiguração de uma Administração Pública que promova a boa relação entre os atores públicos e privados (ALENCAR, 2018). A regulação estatal manifesta-se no exercício do Poder de Polícia do Estado tendo como finalidade limitar a autonomia da vontade do particular adequando-a aos valores constitucionais.

Nesse panorama, a análise de arranjos institucionais regulatórios é essencial para construção de mecanismos de *accountability* e responsabilidade dos controladores de dados em sistemas automatizados de decisão.

Dentre as políticas regulatórias destaca-se a regulação econômica que busca analisar os elementos que fundamentam a intervenção do Estado na economia no intuito de mitigar os riscos de instabilidade do sistema capitalista que podem provocar desperdícios sociais (RAGAZZO, 2011). Contudo, “além do papel de corrigir falhas de mercado, a regulação pode ser entendida como um conjunto de técnicas visando a promoção de valores sociais e culturais, que servem de instrumento à realização de preceitos garantidos em norma” (KELLER, 2019, pp. 141-142).

As modificações recentemente introduzidas pela big data mostram como o poder econômico, hoje associado ao poder da informação, apresenta riscos e custos ainda maiores para a preservação da competição nos mercados, dentro de uma perspectiva que assegure a liberdade econômica de todos os agentes envolvidos (FRAZÃO, 2019, p. 115). Tal fato ocorre, “porque o que está em jogo não é apenas o poder de mercado dos gigantes digitais contemporâneos, mas a formação de um sistema econômico apoiado inteiramente na coleta, na armazenagem e na análise de dados pessoais” (ZANATTA; ABRAMOVAY, 2019, p. 431).

Ademais, os problemas apresentados pelos sistemas de decisão automatizados que empregam inteligência artificial possuem as mesmas características quando do surgimento da internet, a qual exigiu a criação de alternativas governamentais para fins de sua regulamentação. Com efeito, ao longo do tempo notou-se que a procura por soluções exclusivamente no direito positivo, aguardando-se uma atuação legislativa, era um estágio fadado ao fracasso e que o alcance de resultados concretos para tutelar adequadamente direitos no âmbito da Rede dependeriam de uma abordagem multidisciplinar (LEONARDI, 2012, p. 147).

Nesse sentido, Gary Marchant (2011) aponta que com a progressão cada vez mais rápida da ciência e da tecnologia, um grande desafio que surge é a capacidade da legislação de acompanhar o rápido desenvolvimento das inovações tecnológicas.

Tal questionamento é tratado pelo referido autor (2011) como “problema de ritmo”, que deve ser enfrentado pelo menos em duas dimensões: a primeira refere-se ao reconhecimento que as estruturas legais são baseadas em uma visão estática e não dinâmica da sociedade, e; a segunda refere-se a constatação que as instituições legais possuem diminuída capacidade de adaptação às mudanças tecnológicas, especialmente considerando a lentidão do processo legislativo e o descuido da relevância de muitos temas colocados em pauta para votação, cuja importância do debate acaba corroída por uma percepção de urgência e conveniência política.

Portanto, o desafio imposto ao processo de governança de algoritmos é a integração dos aspectos técnicos e normativos, uma vez que é difícil fazer uma distinção clara entre os dois quando se desenvolve o tema tecnologia e Direito. Ademais, a forma tradicional em disciplinar temas voltados à inovação tecnológica, em particular o emprego de instrumentos de intervenção direta nos primeiros estágios de desenvolvimento de sistemas tecnológicos, pode revelar-se uma prática indesejável, porquanto inibiria a própria evolução da técnica ao amordaçar o conhecimento e a criatividade humana (MOLINARO; SARLET, 2015).

As adversidades do acentuado progresso científico e tecnológico revelam a manifesta insuficiência ou incapacidade das estruturas tradicionais do Poder Público para responderem aos problemas complexos e impõe uma busca permanente na reestruturação da governança[37]. Assim, mecanismos alternativos de técnicas regulatórias apresentam-se como caminhos para regular de maneira mais eficiente tecnologias, especialmente aquelas que empregam inteligência artificial. Dentre as quais, o Direito deve disponibilizar alternativas aos atores privados, deixando de focar na regulação como um instrumento para ativar o “comando e controle” (ALENCAR, 2018).

No direito administrativo, ainda que a regulação seja centrada no Estado, ela pode ser desempenhada a partir de arranjos institucionais diversos, existindo uma gama de opções de estratégias institucionais possíveis entre uma regulação estatal

[37] “A inadequação dos instrumentos do agir administrativo tradicional é especialmente notória em determinados setores em que a evolução tecnológica redefine e altera diariamente os mercados, transfere capital e destrói artificialmente as fronteiras territoriais, como acontece com o setor financeiro.
É certo inferir que, dada a tecnicidade que se apresenta diante da sociedade, impõe-se, para além das diretrizes constantes na ordem econômica constitucional, a busca pela permanente reestruturação da governança brasileira. A organização administrativa deve ser compatível e ter metodologia própria para atuar na garantia e efetividade dos direitos fundamentais, especialmente diante dos avanços tecnológicos.” (GUERRA, 2021, p. 154)

direta e a autorregulação (KELLER, 2019). Para Gustavo Binenbojm (2020) a realidade da Administração Pública contemporânea revela uma tendência de combinação do método tradicional de comando e controle com o uso de métodos e técnicas mais flexíveis de indução, além de meios alternativos de realização de objetivos regulatórios, por diferentes estratégias institucionais integradas.

Segundo Mayntz (2003), o termo “governança” atualmente é empregado para indicar um novo modo de governar, diferente do antigo modelo hierárquico no qual as autoridades locais exercem controle soberano sobre as pessoas e grupos. Nesse sentido, a autora (2003) assinala que governança se refere a um todo basicamente não hierárquico de governar, onde atores corporativos privados não-estatais (organizações formais) participam da formulação e implementação de políticas públicas.

Por esse motivo, Albers (2016) defende a necessidade de novas abordagens que superem o pano de fundo das ideias tradicionais de implementação hierárquica (de cima para baixo), de modo que sejam realizadas abordagens teóricas por meio de conceitos mais flexíveis do direito. Essa superação do modelo hierárquico impõe o reconhecimento de que uma “abordagem de baixo para cima pode ser fortalecida por meio de mecanismos participativos que visam garantir o alinhamento com os valores sociais e a compreensão da opinião pública por meio de um diálogo entre todas as partes interessadas” (FLORIDI et al., 2018, p. 06).

Segundo os Bioni e Rielli a LGPD programa-se em um sistema de governança em rede:

> Em poucas palavras, o arranjo institucional da LGPD não aposta em um sistema de supervisão em que haja uma autoridade única e que centralize todas as ações. Pelo contrário, programa-se um sistema de governança em rede, em que se distribuem competências entre uma série de atores, privados e públicos. Essa é justamente uma das definições de multissetorialismo, modelo no qual essa teia de atores se contrapõe a uma estratégia de regulação monopolizada pelo Estado. (BIONI; RIELLI, 2021, p. 250).

Nesse panorama, a LGPD está inserida dentro da compreensão de uma governança pública, na qual os atores públicos e privados participam com vistas à resolução de problemas e à criação de oportunidades dentro de uma colaboração multissetorial (ALENCAR, 2018). Segundo Alencar (2018) a governança em rede, ao procurar o envolvimento e a adesão de diversos atores no procedimento de decisão,

permite a obtenção de uma visão abrangente do assunto, com planejamento e constante correção de equívocos.

Segundo o autor (2018, p. 145), essa metodologia apresenta várias funções significativas dentro de um contexto dinâmico e sujeito a adaptações, tais como: “(i) diálogo; (ii) criação e desenvolvimento institucional; (iii) definição e edição de normas; (iv) implementação das normas; e (v) monitoramento e controle mediante *feedback* e correção de problemas”.

A governança em rede impele o Estado[38] na construção de mecanismos que facilitem o relacionamento entre o Estado e a sociedade, com a finalidade de satisfazer os interesses da coletividade. Os interessados são chamados a assumir papel ativo na construção de resultados, com colaborações multissetoriais que devem ser acopladas ao Estado, enquadrando-se na corregulação entre agentes públicos e privados (ALENCAR, 2018).

Essa abordagem multidisciplinar, caracterizada pela complexidade que engloba vários aspectos, entre os quais tecnológicos, socioeconômicos, de desenvolvimento, jurídico e político foi consolidada pela governança da internet (KURBALIJA, 2016), na qual são equacionadas as divergências e idealizados os consensos quanto à regulação e ao controle da infraestrutura da internet, representando um cenário propício ao estímulo de um melhor entendimento e engajamento (CANABARRO; WAGNER, 2014).

Ademais, a governança da internet abrange uma ampla variedade de partes interessadas e possui uma atuação multissetorial[39], envolvendo um amplo rol de atores que abrange governos nacionais, organizações internacionais, o setor empresarial, a sociedade civil e a comunidade técnica (KURBALIJA, 2016). Por essa

---

[38] A concepção de governança pública representa uma mudança no papel do Estado, um verdadeiro novo modelo de gestão, na qual se aceita uma maior participação da sociedade na formulação das políticas públicas. Com efeito, a governança deve conduzir a reformulação da Administração Pública com a instauração de um conjunto de instrumentos técnicos de gestão que assegurem a eficiência da ação pública. O Decreto nº 9.203, de 22 de novembro de 2017, instituiu a política de governança pública na Administração Pública federal, trazendo o seguinte conceito de governança: “conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade” (art. 2º, I).

[39] O Brasil foi pioneiro na abordagem multissetorial de governança da internet através da consolidação de um modelo aberto e participativo, bem representado pelo Comitê Gestor da Internet (CGI.br) e considerado uma fonte de inspiração internacional – por exemplo, a França construiu o seu *Conseil National du Numérique* tomando ampla inspiração do CGI.br (BELLI; DONEDA, 2021).

razão, Polido (2020) pondera que a prospecção científica e acadêmica em torno dos sistemas autônomos e inteligências e suas aplicações para a vida humana tem sido uma preocupação transversal de análise, de tomada de decisões por atores estatais e não estatais, o que envolve discussões sobre a viabilidade ou necessidade de regulação de sistemas autônomos e suas interfaces com o direito amplamente considerado.

Portanto, a abordagem multissetorial representa um passo importante na regulação da inteligência artificial e pode representar um caminho significativo na proteção de dados pessoais. Segundo Polido (2020) as iniciativas e diálogos estabelecidos por organizações internacionais, academia e organizações da sociedade civil são realçados em torno de instrumentos alternativos e esquemas de autorregulação, como recomendações, princípios gerais, diretrizes éticas que representam um verdadeiro conjunto de *soft law*.

A lei não é o único sistema regulatório que existe, além dela, deve-se levar em consideração outros sistemas regulatórios, como o mercado e um conjunto compartilhado de valores e princípios sociais (PAGALLO; CASANOVAS; MADELIN, 2019). Isso revela-se diante da insuficiência do modelo baseado na sanção, criando-se possibilidades de modo a propiciar e estimular a cooperação entre o Estado e os cidadãos, bem como incentivar uma atuação convergente com os propósitos da regulação estatal (FRAZÃO, 2022, p. 42).

Doneda e Almeida (2016) reforçam que é preciso considerar um processo de governança para os algoritmos, diante dos riscos que o seu uso pode trazer para à sociedade. Quando se opta por uma abordagem de governança busca-se reduzir os resultados indesejáveis tentando preservar a eficácia do uso dessas inovações tecnológicas (DONEDA; ALMEIDA, 2016).

Nesse contexto, Frazão e Medeiros (2019, p. 74) ponderam como “a importância dos programas de *compliance* ganha força em razão das limitações do *enforcement* tradicional, baseado na regulação jurídica estatal e na imposição de sanções”. A complexidade oriunda da evolução tecnológica e a insuficiência do regime de comando-sanção do Estado para assegurar a eficácia dos comandos legais, demandam a necessidade da busca de novos horizontes para a regulação estatal, conectando-a com o estímulo à autorregulação (FRAZÃO; MEDEIROS, 2019).

Entre os principais defensores da autorregulação estão as corporações e, de maneira mais geral, as forças do mercado (PAGALLO; CASANOVAS; MADELIN, 2019). O mercado de dados se consolidou a partir da difusão da ideia de que seria eficiente e justo, de modo a justificar a dispensa de qualquer tipo de regulação estatal (FRAZÃO, 2019).

Com efeito, ainda que sejam boas as intenções da autorregulação, deve-se observar que o desenvolvimento das tecnologias pelas empresas é uma atuação tipicamente empresarial lastreada na racionalidade econômica dos dados[40] e nos interesses específicos da empresa, ainda que eventualmente possam levar em conta interesses de usuários ou interesse geral (HOFFMANN-RIEM, 2020). Ademais, a autorregulação dentro de uma perspectiva da racionalidade econômica dos dados é fortemente utilitarista, sustentando a ideia que para a inovação seria possível o sacrifício de direitos fundamentais elementares (FRAZÃO, 2019). Tal visão é mantida tendo por concepção a ideia de um verdadeiro *trade-off* entre inovação e privacidade, de forma que os usuários receberiam contrapartidas adequadas pelos seus dados (FRAZÃO, 2019).

Com efeito, o próprio papel do Estado de Direito é questionado diante do agravamento da prática de tecnorregulação dos cidadãos em dispositivos e plataformas digitais, especialmente quando restringem o usuário àquilo que já foi programado (MAGRANI, 2019). Assim, a governamentalidade algorítmica acaba cerceando de forma cristalina a autodeterminação informacional e o livre desenvolvimento da personalidade dos destinatários das tecnologias dentro de um viés econômico dos dados.

Desse modo, na busca de mecanismos que permitam a utilização da lei como premissa para o desenvolvimento tecnológico, Magrani (2019) propõe reflexões

[40] ‘Algumas das empresas mais ricas do mundo, como Facebook e Google, são construídas com capital de dados. Estima-se que a indústria de corretagem de dados gere US$ 200 bilhões em receita anual (Crain, 2016). Os três maiores corretores de dados - Experian, Equifax e Transunion - cada um traz bilhões de dólares anualmente. Mesmo para corretores de dados relativamente pequenos, a diferença entre o valor dos dados e a compensação fornecida por eles é impressionante (Roderick, 2014) Além disso, outros setores importantes, como finanças, seguros e manufatura, dependem cada vez mais do capital de dados para gerar valor. Para muitas dessas empresas, os dados que usam são principalmente sobre pessoas e criados por essas pessoas fazendo coisas. Essas empresas estão acumulando bilhões de dólares em mais-valia do “trabalho digital” feito pelas pessoas (Scholz, 2012), enquanto pagam pouco ou nada em troca. Thatcher *et al.* (2016: 994) argumentam que essas práticas extrativas vão tão longe a ponto de “espelhar processos de acumulação primitiva ou acumulação por espoliação que ocorrem quando o capitalismo coloniza tempos e lugares privados anteriormente não-mercantilizados.” Quando uma pessoa não recebe uma oferta justa pelo trabalho que fez ou pelas coisas que vendeu, chamamos isso de “exploração” - e esse nível de exploração e desigualdade é indicativo de extração.’ (SADOWSKI, 2019, p. 08).

sobre a necessidade de transcender o tradicional “dever ser” dos sistemas legais, empregando o direito como técnica de regulação, capaz de influenciar o *design*, códigos e arquiteturas das tecnologias desenvolvidas. Por essa razão, a regulação jurídica dos dados se apresenta como importante contraponto na questão da proteção dos dados, justificando-se sob o prisma da garantia da liberdade e da autodeterminação, que são pressupostos econômicos da própria existência dos mercados (FRAZÃO, 2019).

Assim, alcançar o livre desenvolvimento da personalidade dos indivíduos sujeitos aos sistemas automatizados de decisão é viabilizar a existência de estruturas que permitam a efetiva tutela dos direitos fundamentais. O desafio em torno da agenda de regulação de algoritmos e de inteligência artificial está em arquitetar processos de governança que impeçam a ocorrência de efeitos indesejados ao se introjetar tecnologias nas decisões sociais cotidianas (BIONI; LUCIANO, 2018).

Desse modo, desponta-se a importância da heterorregulação no estabelecimento de abordagens de governança e da corregulação baseada na estruturação principiológica das leis gerais de proteção de dados. Para Pagallo, Casanovas e Madelin (2019), a regulamentação legal desempenha um papel crucial no conjunto de ferramentas de governança global.

Por esse motivo, os referidos autores (2019), ao apontarem a existência de diferentes significados da noção de “governança”, assinalam que a maioria dos significados e definições incluem a regulamentação legal (heterorregulação) como componente-chave do modelo. Tal entendimento se faz presente tendo em vista que a funcionalidade de uma governança moderna depende intrinsecamente de um Estado suficientemente poderoso que leve em conta o interesse público e não beneficie apenas os próprios atores participantes, porquanto a autorregulação no contexto da governança é sempre uma autorregulação regulada (MAYNTZ, 2003).

Nesse panorama, Ana Frazão pondera a respeito da importância da corregulação como mecanismo essencial para dar concretude à lei:

> Daí a discussão atual sobre um terceiro gênero – o da corregulação – que combinaria diferentes categorias de práticas regulatórias e exigiria o envolvimento central dos agentes privados e dos governos, a fim de propiciar muitas vantagens da autorregulação se as mesmas desvantagens. Apesar das controvérsias a respeito das eventuais distinções entre a autorregulação e corregulação, o que importa é que, na seara da

> *compliance* de dados, a atuação complementar entre a iniciativa privada e o Estado seja intensa, consistente e frutífera. Daí por que a autorregulação e a corregulação têm papel central para concretude à lei e, se for o caso, até ir além dela. (FRAZÃO, 2022, p. 46)

"A partir dessa caracterização de estruturas descentralizadas e mistas que contam com a presença estatal, é possível verificar a associação da corregulação com os conceitos de governança, que também presumem uma diversidade de agentes envolvidos no processo de regulação" (KELLER, p. 177). Dentro dessa perspectiva, Silva (2012) assevera que o enfrentamento de temas complexos exige ações integradas, sendo a corregulação um mecanismo viável para contornar esses desafios e comprometer cooperativamente todos os atores envolvidos.

Ainda, a autora (2012) reforça que a corregulação valoriza a participação social e política dos usuários, vinculando os particulares à defesa de direitos fundamentais e impondo ao Estado novos papéis e funções à medida que salvaguarda os espaços de liberdade em face do Estado. Segundo Hoffmann-Riem (2020), é um desafio garantir a boa governança durante o desenvolvimento de sistemas algorítmicos e durante sua aplicação, porquanto ela não se estabelece automaticamente, dependendo de requisitos legais normativos e suplementares não normativos, tal como preceitos éticos e morais. Por isso "uma das tarefas do Estado é criar leis ou modificá-las de forma a possibilitar e estimular a boa governança digital" (HOFFMANN-RIEM, 2020, p. 128).

Segundo Pagallo, Casanovas e Madelin (2019), o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia adotou a opção regulatória que combina formas de autorregulação com ferramentas de heterorregulação, porquanto a referida legislação estabelece tanto os princípios que devem ser seguidos pelos controladores de dados quanto os resultados aos quais eles devem obedecer. Essa percepção também pode ser extraída da Lei Geral de Proteção de Dados (LGPD) a qual é uma lei fundamentalmente principiológica, baseada em cláusulas gerais e *standards* de comportamento, que oferecem um eixo valorativo endereçado a facilitar a interpretação e a aplicação das demais legislações nos casos envolvendo o tratamento e a proteção de dados (FRAZÃO, 2020).

Segundo Bioni e Rielli (2021), o multissetorialismo está no DNA da LGPD, porquanto o seu desenvolvimento teve forma a partir de um processo

multiparticipativo, com a presença de representantes do setor privado, do terceiro setor, do Governo e da academia.

Nesse panorama, Bioni e Rielli elencam uma série de elementos que evidenciariam essa estratégia corregulatória da LGPD:

> "[...] o desenho final da LGPD programa que: a) ANPD deve cooperar com outros órgãos reguladores (artigo 55-J, incisos IX, XXI, XXII e XXIII e §§ 3º e 4º); b) o tradicional sistema de tutela de direitos difusos e coletivos brasileiro também poderá ser acionado, tanto em âmbito administrativo como judicial (respectivamente, Procons e Secretaria Nacional de Defesa do Consumidor e ações civis públicas e coletivas) (artigo 22); c) os agentes de tratamento de dados, no âmbito do setor privado e do setor público, são incentivados a se auto-organizar por meio de códigos de boas condutas (artigos 32, 46 e 49); d) selos, certificações e outros instrumentos contratuais privados são mecanismos de transferência internacional (artigo 33, II, d, e artigo 35), de modo que essa auto-organização dos agentes privados pode ser premiada pela própria ANPD para destravar o fluxo transfronteiriço (artigo 55-J, XIV); e) é um dever da ANPD realizar consultas públicas, bem como avaliações de impacto regulatório para que haja uma oitiva – uma espécie de contraditório e ampla defesa – das partes afetadas pelo exercício do seu poder de regulamentação (artigo 55-J, § 2º)" (BIONI; RIELLI, 2021, p. 249).

Portanto, é possível observar que o texto da LGPD aposta numa ideia de corregulação, intercambiada por uma atuação conjunta do Estado e das empresas privadas, para a interpretação e a fiscalização da LGPD, especialmente diante da complexidade do tema que exige a participação multissetorial. No Brasil, a LGPD, em razão de forte influência europeia, "adotou sistemática regulatória bastante moderna, incorporando, para além das formas tradicionais de produção e implementação de normas jurídicas relativas à proteção de dados pessoais", "outros mecanismos regulatórios calcados em regras livremente pactuadas pelos interessados" (WIMMER, 2021, p. 378).

Além disso, dentro de uma perspectiva multissetorial, existem diversos atores do ecossistema de proteção de dados, responsáveis por estabelecer regras calibradas que visam harmonizar interesses econômicos e sociais em jogo (MONTEIRO, 2018a). Por esse motivo, embora a LGPD tenha um papel fundamental na heterorregulação, a sua efetividade está intrinsecamente associada a mecanismos de autorregulação e programas de *compliance* (FRAZÃO, 2019).

Nesse ponto, a LGPD consagra uma seção específica para "boas práticas e governança" em seu artigo 50, a saber:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018)

De igual modo, o parágrafo primeiro do referido dispositivo apresenta diretrizes de atuação pelo controlador e operador, os quais ao estabelecerem regras de boas práticas, devem levar em consideração "a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular", revelando-se nítida coerência com o princípio da prevenção (art. 6º, VIII) e estando em conformidade com o princípio da não maleficência.

Nessa perspectiva de corregulação numa relação multissetorial é evidenciada a importância da Autoridade Nacional de Proteção de Dados (ANPD), a qual assume um papel estratégico para suprir as lacunas legislativas, regulamentando e fiscalizando o cumprimento das obrigações legais estabelecidas pela LGPD. A criação da autoridade nacional revela-se como "elemento-chave" para a sistemática do *enforcement* da LGPD, encontrando-se alinhada ao cenário atual de combinar os mecanismos regulatórios tradicionais e elementos de corregulação (WIMMER, 2021).

No âmbito europeu, a Carta de Direitos Fundamentais da União Europeia ao prever em seu artigo 8º sobre o direito à proteção dos dados pessoais, dispõe sobre a necessidade de criação de uma autoridade independente (art. 8º, item 3) [41] que possa fiscalizar o cumprimento da garantia fundamental consagrada no referido documento. No mesmo sentido, a Convenção de Estrasburgo sobre a Proteção de Dados Pessoais (Convenção 108, de 28 de janeiro de 1981), estabelece "a necessidade de criação de uma autoridade independente para a efetiva proteção dos dados pessoais, destacando que a lei por si só será pouco eficaz" (LIMA, 2020, p. 252).

[41] Artigo 8º - Proteção de dados pessoais. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto 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 respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. (UNIÃO EUROPEIA, 2000)

De igual modo, a OCDE, através do documento "*Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*" recomenda que os países-membros criem e mantenham autoridades para o *enforcement* da privacidade, as quais devem ter estrutura técnica e expertise para exercer suas atribuições de forma objetiva (CRESPO, 2021).

Nesse sentido, a GDPR, em seus artigos 51 a 59 enfatiza a necessária independência desta autoridade, com função de fiscalização e controle do cumprimento da lei pelos agentes responsáveis pelo tratamento de dados (LIMA, 2021). Ademais a GDPR[42] prevê de forma expressa que as autoridades de supervisão devem agir "com total independência no desempenho das suas funções o no exercício dos seus poderes" (art. 52, item 1), bem como que cada Estado-Membro deve assegurar que cada autoridade de supervisão disponha de recursos humanos, técnicos e financeiros necessários ao desempenho efetivo das suas funções e ao exercício das suas competências (art. 52, item 4), devendo ser assegurado orçamento específico para tanto (art. 52, item 6).

Assim, é possível observar que "a independência é um traço bem marcante destes órgãos, pois tem a missão, dentre outras, de fiscalizar os agentes de tratamento sejam eles entes públicos, sejam entes privados" (LIMA, 2020, p. 255). No Brasil, tais características estariam muito próximas as das agências reguladoras (LIMA, 2021).

No âmbito nacional, a LGPD "criou uma estrutura de princípios e outras normas para a proteção de dados pessoais que depende em grande parte da

[42] Art. 52 [...] 1. Cada autoridade de supervisão deve agir com total independência no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento.
2. O membro ou os membros de cada autoridade de supervisão devem, no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, manter-se isentos de influências externas, diretas ou indiretas, e não solicitar nem aceitar instruções de ninguém.
3. O membro ou os membros de cada autoridade de supervisão devem abster-se de qualquer ato incompatível com as suas funções e não podem, durante o seu mandato, exercer qualquer atividade incompatível, remunerada ou não.
4. Cada Estado-Membro deve assegurar que cada autoridade de supervisão dispõe dos recursos humanos, técnicos e financeiros, das instalações e das infraestruturas necessárias ao desempenho efetivo das suas funções e ao exercício das suas competências, incluindo as que devem ser desempenhadas no âmbito da assistência mútua, cooperação e participação no Conselho.
5. Cada Estado-Membro deve assegurar que cada autoridade de controlo escolha e disponha do seu próprio pessoal, que estará sujeito à orientação exclusiva do membro ou membros da autoridade de controlo em causa.
6. Cada Estado-Membro deve assegurar que cada autoridade de supervisão esteja sujeita a um controlo financeiro que não afete a sua independência e que tenha orçamentos públicos anuais separados, que podem fazer parte do orçamento geral do Estado ou do orçamento nacional. (UNIÃO EUROPEIA, 2016)

interpretação e a da complementação de um órgão público federal, a Autoridade Nacional de Proteção de Dados" (CRESPO, 2021, p. 930). Nesse sentido, Cíntia Rosa Pereira de Lima (2020, p. 295) pondera que a existência de uma ANPD independente é um dos pilares da proteção de dados, especialmente diante das suas funções essenciais de "fiscalizar o cumprimento das regras sobre o tema, especificar padrões técnicos e administrativos para garantir a segurança das atividades de coleta e tratamento de dados, elaborar regulamentos, analisar os Códigos de Boas Práticas (as normas deontológicas), etc".

Não é por outro motivo que a versão original do texto da LGPD aprovada pelo Senado Federal previa a ANPD como uma autarquia especial integrante da administração pública federal indireta, portanto, sem subordinação hierárquica com a administração direta e com independência administrativa e autonomia financeira. Ademais, seus dirigentes possuiriam mandato fixo e estabilidade (art. 55*, caput* e §3º do texto original). Essas disposições legais foram vetadas pelo Presidente Michel Temer. O principal argumento do veto foi que a criação da ANPD pelo legislativo constituiria vício de constitucionalidade formal (ou nomodinâmica), propriamente dita, tendo em vista a presença de vício subjetivo quanto ao sujeito competente para tomar a iniciativa, pois a criação da ANPD seria de competência do Chefe do Poder Executivo.

Diante do veto da criação da ANPD pelo legislativo, Michel Temer propôs a criação da autoridade nacional através da Medida Provisória 869/2018, contudo, como um órgão subordinado à Presidência da República. Durante a tramitação da referida MP 869, os parlamentares conseguiram fazer algumas alterações, e quando da sua conversão para a Lei 13.853/2019 foi possível dotar a ANPD de uma natureza transitória, com a possibilidade de tornar-se uma autarquia dois anos após a sua criação (BIONI; RIEELI; VICENTE, 2019).

Portanto, atualmente, nos termos prescritos no artigo 55-A da LGPD a Autoridade Nacional de Proteção de Dados (ANPD) possui natureza de um órgão integrante da administração pública federal direta, vinculada à Presidência da República. Contudo, conforme anteriormente registrado, essa natureza jurídica é transitória e a ANPD poderá ser transformada em uma entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República (art. 55-A, §1º). A avaliação dessa transformação deverá

ocorrer em até 2 (dois) anos da entrada em vigor da estrutura regimental da ANPD (art. 55-A, §2º).

O Decreto nº 10.474, de 26 de agosto de 2020, aprovou a estrutura regimental da ANPD, passando a prever diversas atribuições preventivas (poder-dever regulatório) e fiscalizatórias (poder-dever sancionatório) consoantes `as diretrizes já constantes no art. 55-J da LGPD. Ademais, o art. 55-B da LGPD garante a autonomia técnica e decisória da ANPD.

A composição da ANPD é formada pelo Conselho Diretor (órgão máximo de direção), composto por 5 diretores, escolhidos pelo Presidente da República e por ele nomeados através um ato complexo que demanda a aprovação do Senado Federal nos termos da alínea “f” do inciso III do art. 52 da Constituição Federal (art. 55-D, §1º, LGPD). Além do Conselho Diretor, há a previsão do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP), que possui uma composição multissetorial (LIMA, 2021).

Essa composição multissetorial é detalhada no art. 58-A da LGPD (incluído pela Lei nº 13.853/2019), que prevê a composição do CNPDP por 23 representantes, titulares e suplentes, oriundos de diversos órgãos, a saber:

> Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos:
> I - 5 (cinco) do Poder Executivo federal;
> II - 1 (um) do Senado Federal;
> III - 1 (um) da Câmara dos Deputados;
> IV - 1 (um) do Conselho Nacional de Justiça;
> V - 1 (um) do Conselho Nacional do Ministério Público;
> VI - 1 (um) do Comitê Gestor da Internet no Brasil;
> VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais;
> VIII - 3 (três) de instituições científicas, tecnológicas e de inovação;
> IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo;
> X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e
> XI - 2 (dois) de entidades representativas do setor laboral. (BRASIL, 2018)

Ademais, os representantes dos órgãos do Estado serão indicados pelos respectivos órgãos e entidades da administração pública (art. 58-A, §2º), enquanto os representantes da sociedade civil, das instituições científicas, das confederações sindicais, do setor empresarial e do setor laboral serão indicados na forma de regulamento (art. 58-A, §3º).

Atualmente, conforme supramencionado, a Autoridade Nacional de Proteção de Dados (ANPD) é apenas um órgão da administração pública direta federal que faz parte da Presidência da República. Tal situação coloca em dúvida se a ANPD teria autonomia e independência suficientes, tal como das agências reguladoras, para desempenhar atribuições técnicas e essenciais tão importantes dentro de um contexto complexo e multidimensional oriundo dos desafios impostos pela implementação de novas tecnologias.

Nesse sentido, Chiara Teffé e Mario Viola ponderam sobre a importância de verdadeiramente assegurar a independência e autonomia a ANPD, sob pena, inclusive, de muitas questões sobrecarregarem o próprio Poder Judiciário:

> Uma autoridade verdadeiramente independente, autônoma e com corpo técnico qualificado é fundamental para que a regulação do tema não seja fracionada nas mais diversas instâncias que passarão a aplicar a lei nos níveis federal, estadual e municipal. Como a Autoridade deve ter entre suas funções a possibilidade de monitorar o próprio Estado, ela deve se encontrar em posição que lhe permita atuar sem intervenções indevidas. A entidade exerceria uma função uniformizadora, orientando a fiscalização do cumprimento da nova lei. Além disso, a Autoridade Nacional poderia também oferecer orientações sobre como interpretar os dispositivos legais. Sem ela, são elevadas as chances de que os indivíduos comecem a levar ao Judiciário os direitos que a lei nova traz e que isso comece a gerar os mais variados entendimentos nos tribunais brasileiros, tribunais esses que não têm o conhecimento técnico especializado que a matéria exige, havendo então a possibilidade de interpretações diametralmente opostas sobre um mesmo tema, o que poderá gerar uma enorme insegurança jurídica. Pela experiência prática, sabe-se que serão necessários pelo menos três anos de vigência da lei para que as discussões comecem a chegar aos tribunais superiores, quando, só então, os entendimentos começarão a ser uniformizados. (TEFFÉ; VIOLA, 2018, pp. 07-08)

Portanto, fica evidente a importância de uma autoridade nacional independente e autônoma, inclusive com orçamento próprio, para lidar com os complexos problemas relacionados à proteção de dados que, em muitas ocasiões, exigirão conhecimentos técnicos especializados. Além disso, a própria necessidade de fiscalizar atividades de tratamento de dados realizados pelo poder público (art. 55-J, XI e XVI, da LGPD) demanda a ausência de subordinação com a administração direta, sob pena de eventuais conflitos de interesses internos que possam representar prejuízo à imparcialidade do órgão, atualmente subordinado à Presidência da República.

Nesse panorama, se houver, posteriormente, a transformação da ANPD em uma agência reguladora, sem dúvida, seriam estabelecidos mecanismos mais

propícios para o estímulo da corregulação presente no texto legal da LGPD, atendendo, assim, a perspectiva jurídico-objetiva do direito fundamental de proteção de dados. Nesse viés, Marcelo Crespo (2021, p. 931) afirma que "a legislação brasileira segue a linha de uma tendência internacional de proteção de dados, isto é, focada em algo como uma corregulação e no princípio de *accountability*".

5.2 *ACCOUNTABILITY* E *COMPLIANCE*: ARRANJOS INSTITUCIONAIS NO CONTEXTO DA LGPD

A LGPD não apenas sistematizou como ampliou diversos direitos previstos em normativas setoriais esparsas[43], "como também inaugurou novos direitos e mecanismos de *enforcement*, ampliando e consolidando o rol de direitos dos titulares" (MONTEIRO; CRUZ, 2021, p. 260). Segundo Ana Frazão (2022, p. 35) "a compreensão e a efetivação da LGPD certamente exigirão de intérpretes e aplicadores o enfrentamento de diversos desafios e a solução de complexos *tradeoffs*", tais como o "conflito existente entre transparência e *accountability* e a proteção do segredo de negócios".

O arranjo institucional da LGPD programa-se em um sistema de governança em rede, com nítidas características de multissetorialismo, no qual há uma teia de atores em cooperação com o Estado (BIONI; RIELLI, 2021). Ademais, destaca-se a importância de uma interoperabilidade entre a proteção de dados em âmbito nacional ou transnacional, bem como a garantia de um fluxo de dados entre países (BIONI; MENDES, 2020).

Com o advento da LGPD passam a integrar o ordenamento uma nova série de institutos próprios da disciplina da proteção de dados, com um novo enfoque de tutela dos titulares que é proporcionado por regras de demonstração e prestação de contas (*accountabilty*), nas quais são considerados elementos que levam em conta o risco das atividades de tratamento de dados (DONEDA, 2020, p. 255).

Segundo Mariana de Moraes Palmeira:

> Tanto a LGPD quanto o GDPR trazem indicações assertivas a respeito das práticas de segurança e de governança, em maior ou menor grau de

[43] Marco Civil da Internet (Lei nº 12.965/2014), o Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei do Cadastro Positivo (Lei nº 12.414/2011).

> detalhamento. Um pano de fundo comum nos dois diplomas, a despeito das técnicas legislativas serem diferentes – lei e regulamento, respectivamente –, é a ideia de construção coletiva de uma cultura preventiva de proteção de dados pessoais, onde todos os atores precisam entender e assumir suas responsabilidades. (PALMEIRA, 2020, p. 340)

Essa cultura preventiva de proteção de dados está associada à lógica da responsabilização e prestação de contas. A *accountability* tem um papel importante quando se fala em responsabilização pelos efeitos dos sistemas automatizados de decisão, porquanto é responsável pela "inclusão de parâmetros regulatórios preventivos que promovem uma interação entre a *liability*[44] (responsabilidade) do Código Civil e a regulamentação voltada à governança de dados, seja em caráter *ex ante* ou *ex post*" (ROSENVALD; FALEIROS JÚNIOR, 2022, p. 777).

Para fins desse trabalho, torna-se relevante a *accountability* no plano *ex ante* que "é compreendida como um guia para controladores e operadores, protagonistas do tratamento de dados pessoais, mediante a inserção de regras de governança e boas práticas que estabeleçam procedimentos, normas de segurança e padrões técnicos, tal como se extrai do artigo 50 da LGPD" (ROSENVALD; FALEIROS JÚNIOR, 2022, p. 778).

Segundo Marcelo Crespo (2021), há uma certa dificuldade de precisão conceitual do que efetivamente representaria a ideia de *accountability*, embora o termo seja comum no âmbito anglo saxão trazendo uma compreensão ampla do seu significado relacionado à ideia de responsabilidade e prestação de contas. Essa lógica mais responsiva nas normas de proteção de dados pessoais tem como origem as diretrizes da OCDE sobre privacidade e fluxos transnacionais de dados (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*) que estabelece, dentre outras coisas, que os países membros devem implementar a adoção de princípios de proteção de dados, apoiar a autorregulação, além de consagrar o princípio da *accountability* (WIMMER; PIERANTI, 2022).

Nesse contexto, a LGPD ao exigir transparência por parte dos responsáveis de tratamento de dados, exige uma abordagem proativa na qual se deve demonstrar conformidade com a legislação. Dentro desse raciocínio, a *accountability*

---

[44] "Na *common law,* há um termo que se ajusta perfeitamente ao clássico sentido civilístico da responsabilidade. Trata-se da *liability*, cuja acepção remete à indenização haurida pelo nexo causal que conecta conduta e dano, acrescida por outros elementos aferidos em conformidade com o nexo de imputação concreto, tendo em conta as peculiaridades de cada jurisdição." (ROSENVALD; FALEIROS JÚNIOR, 2022, p. 774).

representaria a demonstração de conformidade com a LGPD, de forma sistemática e contínua, por meio da implementação de medidas técnicas e organizacionais, apropriada aos riscos envolvidos nessas atividades (SILVA, *et al*., 2019).

Desse modo, pode-se afirmar que essa adequação à LGPD é um elemento desse sistema amplo de gestão de *compliance* que surge na legislação como expressão do princípio da *accountability* (SAAVEDRA, 2021).

No RGPR europeu o princípio da *accountability* está previsto no art. 5, item 2. Contudo, a descrição da "responsabilidade do controlador" é mais clara no item 1 do art. 24, que contém o seguinte teor:

> 1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para assegurar e poder demonstrar que o tratamento seja efetuado em conformidade com o presente regulamento. Essas medidas devem ser revistas e atualizadas sempre que necessário. (UNIÃO EUROPEIA, 2016).

Portanto, evidencia-se essa característica de programas de conformidade (integridade ou *compliance*), nos quais ao responsável de tratamento de dados é atribuída a função de implementar medidas técnicas e organizacionais adequadas para assegurar e demonstrar que o tratamento de dados está sendo realizado conforme o *enforcement* da legislação de proteção de dados. "O sistema de gestão de *compliance* de dados aparece nessa legislação como expressão do princípio da *accountability* e como meio de proteção dos direitos subjetivos/fundamentais de dados" (SAAVEDRA, p. 731).

Nesse sentido, o princípio da *accountability* previsto na LGPD (responsabilização e prestação de contas, art. 6º, X), também busca o estabelecimento de diretrizes baseadas na *compliance* ao estabelecer que o agente deve demonstrar a adoção "de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". Portanto, essa necessidade de adequação do controlador de dados às orientações constantes na LGPD revelam a conexão da abordagem baseada em gestão do risco como um elemento do sistema de gestão de *compliance*.

Em uma definição simples o *compliance* pode ser apresentado como “a adesão dos agentes de tratamento de dados pessoais a padrões e normas, oriundas de leis, do mercado e das normas, aos princípios de boa governança e aos padrões éticos e sociais comumente aceitos*”* (MULHOLLAND; GOMES, 2022, p. 163).

Por sua vez, Giovani Saavedra afirma que *compliance*:

> [...] consiste em um estado dinâmico de conformidade a uma orientação normativa de comportamento com relevância jurídica por força de contrato ou lei, caracterizado pelo compromisso com a criação de um sistema complexo de políticas, de controles internos e de procedimentos, que demonstrem que a empresa está buscando “garantir”, que se mantenha um estado de *compliance*”. (SAAVEDRA, 2021, p. 729)

Contudo, no âmbito europeu, a legislação vai um pouco além, ao estabelecer uma obrigação por parte do responsável de dados a implementar medidas adequadas e eficazes que demonstrem a conformidade das atividades de tratamento de dados com o Regulamento Geral de Proteção de Dados (RGPD), levando em consideração “a natureza, o âmbito, o contexto e as finalidades do tratamento”, bem como o “risco para os direitos e liberdades das pessoas singulares” (Considerando 74 do RGPD). Nesse último ponto, o RGPD reforça que as medidas de *accountability* devem ser adotadas através de uma abordagem baseada no risco (*risk-basead aprroach*).

Portanto, a *accountability* traz consigo uma preocupação importante relacionada à necessidade da realização de um tratamento de dados com um certo grau de adequação, confiabilidade e segurança para que os sistemas automatizados de decisão possam ser implementados no âmbito social de forma a minimizar os riscos e danos. Segundo Helen Nissebaum (1996), a responsabilização pode ser uma ferramenta poderosa para motivar melhores práticas no desenvolvimento de sistemas mais confiáveis, porquanto a responsabilização das pessoas pelos danos ou riscos que eles trazem fornece uma motivação para tentar preveni-los ou minimizá-los.

Nesse sentido, Ana Frazão (2022, p. 46) pondera que “um bom programa de *compliance* precisa se basear na análise de risco da atividade e na criação de uma organização compatível com o risco assumido, a fim de se evitar ilícitos ou, caso esses aconteçam, restaurar a legalidade da forma mais rápida e eficiente possível”. Afinal, a prestação de contas serve para “garantir o desenvolvimento responsável e

o uso de sistemas algorítmicos de forma que protejam os direitos humanos e beneficiem a sociedade" (KOENE, *et al*., 2019).

Ademais, impõe-se registrar que a gestão de riscos tem sido aprimorada nos últimos anos pelos sistemas de controle externo e interno da Administração Pública, em face da adoção de metodologias voltadas à implementação de uma governança pública no âmbito administrativo dos entes federados. "As atividades administrativas submetem-se a difusos mecanismos de *accountability*, com maior garantia de controle sobre os resultados, ainda que em certos momentos possa haver sobreposição. Inclusive, as atividades de auditoria permitem a adequada correção de rumo e auxiliam na prevenção de desvios" (ALENCAR, 2018, p. 115).

A exemplo disso, cita-se o Decreto nº 9.203/2017 (que dispõe sobre a política de governança da administração pública federal) que em seu art. 3º, inciso V, apresenta a *accountability* (responsabilidade e prestação de contas) como um dos princípios da governança pública, além de outros associados a um sistema de avaliação, direcionamento e monitoração de ações públicas, tais como: capacidade de resposta, integridade, confiabilidade, melhoria regulatória e transparência (BRASIL, 2017). Ademais, o referido decreto inclui o "controle" como um mecanismo para o exercício da governança pública, que compreende "processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos" (BRASIL, 2017).

No mesmo sentido, a Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016 (que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal), apresenta o conceito de *accountability*: "conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações" (BRASIL, 2016). Ademais, o mesmo instrumento normativo apresenta o conceito de "gerenciamento de riscos" que consiste em um "processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização" (BRASIL, 2016).

Desse modo, observa-se que a governança pressupõe a *accountability*, inclusive na seara pública, na qual o sistema de gestão de riscos e controles internos são imprescindíveis para uma gestão administrativa eficiente que supere desafios de performance diante das novas relações entre sociedade e Estado dentro de um contexto plural, fragmentado e complexo (ALENCAR, ano, p. 115).

Transposta essa análise a respeito da íntima conexão entre *accountability*, *compliance* e gerenciamento de riscos, no próximo tópico serão abordados alguns temas referentes à construção e implementação de um sistema de gestão de *compliance* através da avaliação de riscos.

5.3 ABORDAGEM BASEADA EM RISCO E METODOLOGIAS DE COGNIÇÃO

Ao se analisar o modelo tipológico da regulação do risco, tendo como uma das vertentes os avanços dos instrumentos regulatórios na Europa, podem ser extraídos os seguintes elementos do instituto: i) existência de instrumentos para tutela coletiva no diálogo preventivo; ii) regulação *ex ante* atribuídas aos controladores para identificação de riscos; iii) disseminação de metodologias de "gestão de risco", dentro de um panorama de tratamento de uso de dados pessoais e discussão ética sobre os limites do progresso técnico (ZANATTA; 2017)

Nesse viés, uma análise baseada em risco permite a utilização de métodos para maximizar os benefícios e minimizar os riscos decorrentes do uso da tecnologia, alocando recursos proporcionalmente aos riscos para a sociedade, considerando tanto os impactos quanto a probabilidade de eles acontecerem (KOENE, *et al*, 2019). Nesse ponto, a LGPD apresenta-se como um feixe de entrada para aplicação do princípio da precaução, reforçando uma interpretação que leve em consideração a regulação de risco e o princípio da *accountability* como vetores do processo de regulação das tecnologias (BIONI; LUCIANO, 2018).

A regulação de risco provoca uma mudança de rota, abrindo uma agenda de pesquisa para a proteção de dados pessoais dentro de uma visão preventiva baseada em uma "abordagem de riscos" (ZANATTA, 2017). Uma das formas efetivas de mensurar os riscos relacionados à criação de perfis, discriminação e limitação de direitos e liberdades, seria a realização de uma avaliação do impacto à proteção de dados (ZANATTA, 2017). Não é por outro motivo que os Relatórios de

Impacto à Proteção de Dados (RIPDP) têm ganhado protagonismo (BIONI; LUCIANO, 2018).

Segundo Juliana Ruiz e Sofia Franco, o conceito de regulação de risco aparece expressamente na LGPD em dispositivos relacionados:

> (i) à qualificação e regulamentação sobre a elaboração de relatórios de impacto à proteção de dados pessoais, (ii) ao enfrentamento de incidentes de segurança da informação, (iii) ao estabelecimento de programas de governança[45] por parte dos agentes de tratamento de dados pessoais para adequar suas atividades às exigências da LGPD, e (iv) ao ressarcimento de danos provocados aos titulares de dados[46]. (RUIZ; FRANCO, 2022, p. 526)

No que diz respeito aos incidentes de segurança da informação, a LGPD se refere expressamente à avaliação de risco ao exigir dos "controladores que notifiquem a ANPD e os titulares de dados nos casos em que o incidente acarretar risco ou dano relevante a esses titulares." (RUIZ; FRANCO, 2022, p. 527). Quanto aos critérios que deverão orientar a procedimentalização dessa notificação existe uma Nota Técnica da ANPD[47]. Transposto isso, passa-se a análise do Relatório de Impacto de Proteção de Dados (RIDPD).

Por sua vez, o Relatório de Impacto à Proteção de Dados Pessoais (RIDPD) está definido no inciso XVII do art. 5º da LGPD como "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco". Da leitura do inciso XVI do art. 5º da LGPD, tal como ocorre no RGPD europeu, o RIDPD "não será necessário para

---

[45] No que se refere ao estabelecimento de programas de governança, esse tema foi objeto de análise no terceiro capítulo do trabalho. Além disso, em razão de possuir pontos de contato importantes com a regulação de risco, está sendo desenvolvido no presente capítulo junto com a noção de *accountability* e *compliance*.

[46] Esse tema não será objeto do presente trabalho, porquanto ultrapassaria a pretensão estipulada no objeto de pesquisa. Contudo, deve-se registrar que existe um artigo relevante sobre a questão de autoria de Nelson Rosenvald e José Faleiros Júnior, denominado "*Accountability* e mitigação da responsabilidade civil na lei geral de proteção de dados pessoais", na qual a gestão de risco é inserida no contexto de uma *accountability* no plano *ex ante* e *ex post.* Na vertente *ex post*, a *accountability* atuaria como um verdadeiro guia para o magistrado e outras autoridades, na identificação e quantificação de responsabilidades e lastreando o estabelecimento os remédios mais adequados na seara administrativa e para a responsabilidade civil (ROSENVALD; FALEIROS JÚNIOR, 2022). Para tanto, recomenda-se a leitura do artigo disponível na obra "*Compliance* e políticas de proteção de dados" da editora Revista dos Tribunais.

[47] "Em fevereiro de 2021, a Nota Técnica nº 3/2021/CGN/ANPD, por meio da qual iniciou a tomada de subsídios sobre a notificação de incidentes de segurança, bem como disponibilizou formulário de comunicação de incidente de segurança com dados pessoais à ANPD e documento que contém orientações sobre o que fazer em caso de um incidente, enquanto não emite regulamentação sobre o tema". (RUIZ; FRANCO, 2022, p. 527).

todas as atividades de tratamento previamente identificadas e registradas pelo controlador, restringindo-se àquelas que apresentem maior risco aos direitos e às liberdades dos titulares" (RUIZ; FRANCO, 2022, p. 532).

Ademais, da leitura do parágrafo único do art. 38 da LGPD é possível extrair uma lista não exaustiva dos elementos que devem conter o Relatório de Impacto, a saber: "a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" (BRASIL, 2018). Portanto, assim como o DPIA europeu, a elaboração do RIDPD deve levar em consideração a necessidade do estabelecimento de medidas, salvaguardas e mecanismos necessários a contornar os riscos de forma proporcional.

Nesse contexto, o fato de o RIDPD não ser necessário em todas as atividades, tal como naquelas que apresentem menor risco, por exemplo, não inibe que os controladores sejam responsáveis pelo cumprimento das obrigações de proteção de dados, "incluindo a demonstração de conformidade em relação a qualquer processamento de dados, independentemente da natureza, escopo, contexto, finalidade do processamento e riscos para os titulares dos dados" (*EUROPEAN COMMISSION*, 2014). Conforme aponta o WP29, os direitos conferidos ao titular dos dados pela legislação "devem ser respeitados independentemente do nível dos riscos em que este incorre pelo tratamento de dados envolvido" (*EUROPEAN COMMISSION*, 2014, p. 03).

Embora o RIDPD possua muita similaridade com o teste de legítimo interesse, os referidos institutos não se confundem. O teste de legítimo interesse é uma fonte mais simples de mensuração de riscos, empregado sempre que a base de tratamento for o legítimo interesse, enquanto o RIDPD é um instrumento mais detalhado a ser usado em casos de "alto risco" ou que representem significativas ameaças aos direitos e liberdades dos titulares de dados.

Nesse sentido, a Autoridade Independente de proteção de dados do Reino Unido esclarece que o teste de legítimo interesse, por ser mais simples, não será a base mais apropriada para o processamento de dados que possa ser enquadrado de "alto risco". Desse modo, havendo a identificação de riscos significativos, seria

necessária a realização de um *Data Protection Impact Assesment* (DPIA)[48] para avaliar o risco e aplicar medidas de mitigação adequadas ao caso concreto (*INFORMATION COMMISSIONER'S OFFICE*, 2021).

Por sua vez, impõe-se observar que na LGPD não existem definições detalhando em que circunstâncias o relatório de impacto seria obrigatório, delegando-se tal atribuição à Autoridade Nacional de Proteção de Dados conforme se evidencia do inciso XIII do art. 55-J, a saber:

> Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)
> [...]
> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018)

Segundo Isabella Frajhof (2022), a LGPD delega a ANPD a discricionariedade em exigir a elaboração do Relatório de Impacto à Proteção de Dados (RIPDP) e não deixa claro qual é o grau de comprometimento dos controladores com a referida obrigação. Desse modo, tendo em vista que a LGPD não procedimentalizou minimamente o RIPDP, a sua eficácia fica condicionada à regulamentação posterior, o que torna a lei de proteção de dados uma legislação fraca quanto à eficácia da aplicação do princípio da precaução (BIONI; LUCIANO, 2018).

Ainda que a LGPD seja omissa quanto a algumas definições relevantes sobre o RIDPD, é possível constatar alguns casos em que a lei autoriza a ANPD a solicitar a elaboração do Relatório de Impacto ao controlador: i) quando a atividade de tratamento estiver lastreada no legítimo interesse (art. 10, §3º); ii) quando o tratamento for realizado pelo poder público (art. 32), e iii) quando o tratamento envolver operações em geral, incluindo a utilização de dados pessoais sensíveis (art. 38).

Nesse ponto, o parágrafo terceiro do art. 10 da LGPD autoriza a ANPD a "solicitar" do controlador de dados o RIDPD quando o tratamento de dados se efetivar com base no legítimo interesse. No mesmo sentido, o art. 32 da LGPD aponta que a autoridade nacional "poderá solicitar" a agentes do Poder Público a publicação do RIDPD. Nesse ponto em específico, o texto acaba sendo um pouco

[48] No âmbito do RGPD europeu o Relatórios de Impacto à Proteção de Dados (RIPDP) é denominado Data Protection Impact Assesment (DPIA).

confuso, porquanto refere-se à solicitação da “publicação” do Relatório de Impacto, o que poderia conduzir a interpretação que o RIDPD seria obrigatório na seara pública, independentemente do grau do risco da atividade de tratamento. Contudo, não é essa a orientação constante no Guia de Boas Práticas elaborado pelo Comitê Central de Governança de Dados.

Por sua vez, o artigo 38 da LGPD sugere que se o tratamento de dados de modo geral, incluindo o emprego de dados sensíveis, a ANPD “poderá” exigir o RIPDP conforme previsão em regulamento. Portanto, esse dispositivo não tem aplicabilidade imediata, porquanto o art. 38 da LGPD delega a ANPD a atribuição de determinar a elaboração do referido relatório: “a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial” (BRASIL, 2018).

Assim, da interpretação literal dos dispositivos supramencionados (art. 10, §3º, art. 32 e art. 38, todos da LGPD), pode-se concluir que essa exigência é uma faculdade da autoridade nacional, tratando-se, portanto, de um ato administrativo discricionário, no qual a ANPD teria uma margem de liberdade em verificar a conveniência e oportunidade da referida exigência ao controlador de dados. Contudo, essa margem de liberdade (mérito administrativo) da ANPD deve estar atrelada às diretrizes do interesse público na prevenção dos riscos decorrentes das atividades sob a análise (BIONI *et al*., 2021), bem como aos limites normativos extraídos da estrutura deontológica da LGPD, que determinam, por exemplo, a efetiva transparência, responsabilidade e prestação de contas por parte dos agentes responsáveis pelo tratamento de dados que possam impactar nos direitos e liberdades dos titulares de dados.

Seguindo essa ordem de ideias, em junho de 2021 a Autoridade Nacional de Proteção de Dados (ANPD) realizou três reuniões[49] técnicas voltadas à discussão do

[49] “Os três encontros técnicos da ANPD contaram com a participação de especialistas selecionados pela Autoridade dentre mais de 500 inscritos, sendo a grande maioria dos expositores profissionais atuantes no setor privado. Essa seleção, inclusive, provocou a manifestação da sociedade civil organizada, que pontuou à ANPD que tal ausência de diversidade setorial na composição das reuniões técnicas se deu em descompasso à tônica de construção multissetorial da LGPD e de suas previsões sobre a composição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD)”. (BIONI et al., 2021, p. 02). Para maiores esclarecimentos recomenta-se a leitura da Carta a respeito da composição da lista elaborada pelo instituto Colisão Diretos na Rede,

RIPDP. “As reuniões se inserem na fase 1 da agenda regulatória do órgão, a qual prevê a regulamentação do instrumento no formato de Resolução para os casos em que o tratamento de dados representar alto risco à garantia dos princípios gerais de proteção de dados pessoais” (BIONI *et al*., 2021, pp. 01-02).

Nas sessões de discussão nas reuniões técnicas promovidas pela ANPD um dos principais debates foi a respeito de qual metodologia para fins de cognição seria o mais adequado, diante da necessidade do estabelecimento de parâmetros pela Autoridade Nacional de Proteção de Dados e a limitação da subjetividade dos procedimentos a serem adotados pelos controladores de dados (BIONI *et al*., 2021). Diante disso houve controvérsias a respeito da abordagem baseada em análise de risco e a abordagem baseada em direitos, porquanto essa última representaria uma certa resistência à primeira, cujas críticas endereçadas consistiriam na ineficiência na efetiva proteção aos direitos dos titulares de dados (BIONI *et al*., 2021).

Nesse ponto específico, cumpre relembrar que na seção 5.1 do presente capítulo houve o registro da existência de diferentes abordagens de governança de algoritmos: i) abordagem principiológica com valores éticos; ii) uma abordagem com transparência e *accountability*, e iii) abordagem com análise de fatores de risco (*risk-basead approach*), e iv) abordagem baseada em direitos humanos.

Especificamente quanto à abordagem baseada em fatores de risco (*risk-based approach*) ou uma abordagem baseada em direitos (*rights-based approach*), ainda existe no âmbito europeu um certo debate a respeito de qual das referidas metodologias seria mais compatível para atender as finalidades pretendidas pelo RGPD. Ademais, essa discussão se intensificou a recente publicação da proposta de regulação da inteligência artificial pela Comissão Europeia[50], a qual parte de uma estrutura baseada em risco.

Nesse sentido, Ansgar Koene (2022) pondera que a regulamentação da IA (o que envolve os sistemas automatizados de decisão) está em um estágio muito inicial e há uma tendência de adoção de uma abordagem baseada em risco. Ademais, embora exista posições contrárias a regulamentação orientada pela análise de risco, exigindo uma abordagem baseada em direitos, as duas abordagens não são

---

disponível em: https://direitosnarede.org.br/2021/06/29/carta-a-respeito-da-composicao-da-lista-de-expositores-das-reunioes-tecnicas-sobre-relatorio-de-impacto-a-protecao-de-dados-pessoais/.

[50] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussels, COM(2021) 206 final, 21 Apr 2021, p. 7.

necessariamente mutuamente exclusivas, até porque uma abordagem baseada em risco pode centralizar sobre a análise a violação de direitos e como evitar essas violações (KOENE, 2022). Exemplo disso, é o item 2 do artigo 7º da proposta da Lei de IA da União Europeia, que inclui "risco de dano aos direitos fundamentais" entre os critérios estabelecer é o uso pretendido de um sistema de IA deve ser classificado como “alto risco” (KOENE, 2022).

De igual modo, o WP29 em um documento denominado *Statement on the role of a risk-based approach in data protection legal frameworks* (declaração sobre o papel de uma abordagem baseada em risco nos quadros jurídicos de proteção de dados), afirmou que sempre apoiou a inclusão de uma abordagem baseada em risco no quadro jurídico de proteção de dados da União Europeia e que os titulares dos dados devem ter o mesmo nível de proteção, sendo inadequada qualquer interpretação que apresente a gestão de riscos como uma medida alternativa à observância dos direitos e princípios de proteção de dados (*EUROPEAN COMMISSION*, 2014).

Seguindo o mesmo raciocínio, Raphäel Gellert (2016) aponta que as abordagens baseadas nos direitos e baseadas no risco são muito mais semelhantes do que discrepantes, porquanto ambas visam gerenciar os riscos das operações de processamento de dados, na busca de equilíbrio dos danos e benefícios associados a tais operações e a aplicação de medidas de mitigação. Ademais, o contexto da abordagem baseada em risco parece ser mais interessante na tutela dos dados pessoais, porquanto permitiria a determinação de quais salvaguardas são mais adequadas para cada operação de processamento, tal como ocorre na proteção contida no art. 22 do RGPD europeu que prevê salvaguardas dos direitos e liberdades do titular dos dados: obtenção de intervenção humana, manifestação do seu ponto de vista e possibilidade de contestação da decisão (GELLERT, 2016).

Segundo Raphäel Gellert:

> [...] se as abordagens baseadas em risco e baseadas em direitos são práticas gêmeas, elas não são idênticas. A contribuição, portanto, concentra-se em sua principal diferença. Ou seja, a abordagem baseada em risco gerencia os riscos de uma maneira contextual e personalizada. A abordagem baseada em direitos gerencia os riscos desde o início (por meio dos princípios básicos de proteção de dados) e não está sujeita a alterações adicionais. (GELLERT, 2016, p. 482)

Portanto, é possível aferir que a adoção de metodologias com análise de fatores de risco (*risk-basead approaches*) não só afasta não a possibilidade da aplicação de metodologias baseadas em direito (*rights based approaches*) como acaba por exigir que ambas sejam empregadas em sintonia com a LGPD. As metodologias baseadas em direito servem de estruturas normativas essenciais para os programas de conformidade e *accountability* conforme exposto no tópico 3.1.1. do presente trabalho, quando se abordou os guias deontológicos da LGPD.

Por essa razão, pode-se extrair desse pensamento a conclusão de que “na tutela dos dados pessoais, não basta ao agente de tratamento o cumprimento das regras previstas na Lei, devendo sempre atuar com vistas à promoção dos valores que se definem insculpidos no seu sistema” (MULHOLLAND; GOMES, 2022, p. 162). E esses valores são representados pelo contexto axiológico que envolve a constituição da estrutura principiológica da LGPD e do próprio efeito irradiante da dimensão objetiva do direito fundamental de proteção de dados.

Desse modo, entende-se que todas as abordagens de governança trabalhadas no segundo capítulo[51] devem ser aplicadas de forma conjunta, porquanto possuem uma intersecção inevitável e seu entrelaçamento significa um reforço à proteção da autodeterminação informacional e do livre desenvolvimento da personalidade, de modo a criar mecanismos que permitam a responsabilização e prestação de contas pelo uso inadequado do tratamento de dados nos sistemas automatizados de decisão.

Assim, a ideia central é explorar os caminhos normativos que consolidam o estabelecimento de mecanismos de *accountability* e *compliance* vinculados à governança de algoritmos dentro de uma abordagem baseada em riscos, na qual seja possível calibrar as obrigações dos controladores de dados em conformidade com as diretrizes da LGPD, por meio da ação de medidas concretas de mitigação de risco. Para tanto, passa-se à análise do Relatório de Impacto à Proteção de Dados (RIPD) e dos mecanismos de governança relacionados à avaliação de risco.

5.4 METODOLOGIAS DO RIPDP: ESTABELECIMENTO DE CRITÉRIOS OBJETIVOS E *STANDARDS* PARA AVALIAÇÃO DO RISCO

[51] Abordagens de governança: i) abordagem principiológica com valores éticos; ii) uma abordagem com transparência e *accountability,* e iii) abordagem com análise de fatores de risco (*risk-basead approach*), e iv) abordagem baseada em direitos humanos.

A definição do Relatório de Impacto à Proteção de Dados (RIPD) foi diretamente inspirada pelo RGPD da União Europeia. Portanto, torna-se relevante trazer alguns apontamentos sobre a compreensão do tema a nível europeu.

Nesse contexto, o artigo 35 do RGPD europeu aborda o conceito inicial de uma Avaliação de Impacto da Proteção de Dados (ou em inglês *Data Protection Impact Assesment* – DPIA):

> 1 Sempre que um tipo de tratamento, em particular que utilize novas tecnologias, e tendo em conta a natureza, âmbito, contexto e finalidades do tratamento, possa resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve, previamente ao tratamento, proceder a uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais. 2 Uma única avaliação pode abordar um conjunto de operações de processamento semelhantes que apresentam riscos elevados semelhantes. (UNIÃO EUROPEIA, 2016).

Com efeito, Carlos Monteiro Filho e Nelson Rosenvald (2020, não paginado) elogiam o conteúdo dessa cláusula geral constante no RGPD europeu, “na medida em que o alto/elevado risco da atividade será detectado conforme a aptidão da nova tecnologia para instrumentalizar a pessoa humana, afetando a sua dignidade e direitos fundamentais, por violar a sua liberdade ou igualdade, introduzindo injustificáveis discriminações”.

Da leitura do referido dispositivo observa-se que há uma obrigação da realização do DPIA sempre que o processamento de dados possa resultar em alto risco aos direitos e liberdades das pessoas. Ademais, essa avaliação não se limita apenas ao âmbito individual, devendo serem considerados os riscos para a sociedade em geral. Portanto, o próprio texto do RGPD reforça a ideia de entrelaçamento entre as metodologias com análise de fatores de risco (*risk-basead approaches*) e baseadas em direito (*rights based approaches*).

Nesse sentido, Luca Belli aponta que:

> Os DPIAs devem levar em conta riscos de conformidade com as normas estabelecidas pelo GDPR, mas também riscos mais amplos para os direitos e liberdades dos indivíduos, incluindo o potencial para qualquer desvantagem social ou econômica significativa. Portanto, o foco da análise está na avaliação da existência de potenciais danos não somente para os indivíduos titulares de dados, mas também para sociedade em geral. (BELLI, 2021, p. 392)

Por isso, o DPIA representa um instrumento importante na responsabilização, ao auxiliar os agentes de tratamento em demonstrar que as medidas adotadas asseguram a conformidade com o RGPD europeu. Com efeito, o WP29 esclarece que o DPIA (*Data Protection Impact Assesment*) é um processo concebido para o tratamento de dados que possui a finalidade de avaliar e gerenciar os riscos para os direitos e liberdade das pessoas, de modo a garantir o estabelecimento de medidas necessárias para contornar esses riscos de forma proporcional (*EUROPEAN COMMISSION*, 2017b).

Estabelecido que o RGPD e a LGPD consagram uma abordagem baseada em risco, tendo como uma de suas principais ferramentas o Relatório de Impacto à Proteção de Dados (RIPDP), remanesce o questionamento a respeito do que seria considerado um tratamento de dados de “alto risco” e quais casos haveria uma obrigatoriedade da elaboração do RIPDP.

Nesse ponto, a LGPD apresenta diversas omissões, dentre as mais relevantes destacam-se: i) a ausência do conceito de risco; ii) a ausência de definição do que poderia ou não ser classificado como processo de tratamento de dados de alto risco, e iii) ausência de diretrizes quanto às hipóteses em que o RIPDP deve ser obrigatório.

No que diz respeito à inexistência do conceito de risco na LGPD, Maria Gomes (2020) entende que essa foi uma decisão correta, especialmente porque uma definição equivocada poderia trazer mais prejuízos do que efetivamente colaborar com a compreensão da noção desse conceito. Desse modo, cabe à Autoridade Nacional de Proteção de Dados (ANPD) regular o assunto em termos de elaboração de orientações sobre o tema (GOMES, 2020).

Para Raphael Gellert (2016) o risco possuiria dois elementos: prever o futuro, através de estatísticas e probabilidade, e tomar decisões com base nele. Ademais, embora o risco seja uma medição e previsão sobre a tomada de decisão, “continua sendo uma técnica abstrata que necessita de metodologias que o implementem concretamente” (GELLERT, 2016, pp. 483-484). Essas metodologias serão abordadas em tópico específico quando forem explorados os *standards* para a avaliação de risco.

Por sua vez, no que se refere à ausência de definição do que poderia ou não ser classificado como processo de tratamento de dados de alto risco e, consequentemente, as hipóteses em que o RIPDP deve ser obrigatório, a ANPD

ainda não se pronunciou oficialmente. Para tanto, na próxima seção serão abordados alguns pontos quanto ao tema.

5.4.1 Estabelecimento de critérios objetivos baseados na experiência europeia e nas iniciativas normativas nacionais

Durante as reuniões técnicas realizadas pela Autoridade Nacional de Proteção de Dados, em junho de 2021, foi abordado o tema a respeito da discricionariedade da ANPD para a elaboração de listas (*blacklists e whitelists*)[52], enumerando quando os processos de tratamento de dados implicariam na obrigatoriedade de elaboração do RIPDP e quando isso não seria necessário, diante da ausência de risco elevado a liberdades civis e direitos fundamentais (BIONI *et al*., 2021).

Essas listas são adotadas no contexto europeu de forma não exaustivas e elaboradas pelas autoridades nacionais dos países sujeitos ao RGPD, contudo, durante as reuniões técnicas foi consignado que o estabelecimento de uma lista taxativa poderia prejudicar a aplicação da LGPD diante das rápidas e constantes transformações tecnológicas que poderiam tornar essas listas obsoletas (BIONI *et al*., 2021).

No âmbito europeu esse tema encontra-se em um estágio mais avançado. Nesse sentido, o Considerando 90 do RGPR registra que “uma avaliação do impacto na proteção de dados deve ser realizada pelo controlador antes do processamento a fim de avaliar a probabilidade e gravidade particular do alto risco, levando em consideração a natureza, escopo, contexto e finalidades do processamento e as fontes do risco” (UNIÃO EUROPEIA, 2016).

Com efeito, o item 3 do art. 35 do RGPD apresenta um rol exemplificativo de atividades que podem ensejar riscos elevados aos titulares de dados. Dentre os casos elencados pela legislação europeia, destaca-se o uso de sistemas automatizados de decisão que produzam efeitos jurídicos sobre as pessoas. Diante

[52] As *blacklists* consistem em enumerações de processos que implicam no requerimento de elaboração de RIPDP, sendo as *Whitelists* as suas antípodas. Significa dizer que nas *whitelists* constam processos de tratamento de dados pessoais que não demandam a elaboração de relatório de impacto, isto é, que não representam risco elevado a liberdades civis e direitos fundamentais. (BIONI *et al*., 2021, p. 03).

da relevância do referido dispositivo legal torna-se necessário trazer seu inteiro teor, a saber:

> 3. É exigida uma avaliação do impacto na proteção de dados referida no n.º 1, em especial no caso de:
> (a) uma avaliação sistemática e abrangente dos aspectos pessoais relativos às pessoas singulares que se baseie no tratamento automatizado, incluindo a definição de perfis, e em que se baseiem decisões que produzam efeitos jurídicos sobre a pessoa singular ou que afetem de forma semelhante significativamente a pessoa singular;
> (b) o tratamento em grande escala de categorias especiais de dados referidas no nº 1 do artigo 9º, ou de dados pessoais relativos a condenações penais e infracções referidas no artigo 10º; ou
> (c) um monitoramento sistemático de uma área acessível ao público em grande escala. (UNIÃO EUROPEIA, 2016)

Nesses casos, o RGPD aponta como obrigatória a realização de DPIA, porquanto seriam hipóteses em que o tratamento é suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. Ademais, o *29 Working Party Group* (WP29) faz questão de registrar que a lista apresentada pelo item 3 do art. 35 do RGPD não é exaustiva, podendo existir operações de tratamento de elevado risco que não estejam incluídas no mencionado rol (EUROPEAN COMMISSION, 2017b).

Seguindo essa mesma linha de raciocínio, o Considerando 75 do RGPD apresenta uma lista extensa de atividades de processamento que são enquadradas como de maior risco para os direitos e liberdades, dentre as quais destacam-se: i) discriminação; ii) qualquer outra desvantagem econômica ou social significativa; iii) onde os titulares dos dados possam ser privados dos seus direitos e liberdades ou impedidos de exercer o controlo sobre os seus dados pessoais; iv) onde são avaliados aspectos pessoais, em particular analisando ou prevendo aspectos relativos ao desempenho no trabalho, situação econômica, saúde, preferências ou interesses pessoais, confiabilidade ou comportamento, localização ou movimentos, para criar ou usar perfis pessoais.

Ademais, com vistas a fornecer um conjunto mais concreto de operações de tratamento de dados que demandem a elaboração prévia de DPIA (*Data Protection Impact Assesment*), o WP29, através das *Guidelines on data protection impact assessment* (diretrizes sobre avaliação de impacto na proteção de dados) estruturou nove critérios que permitem incluir as atividades de tratamento como suscetível de

implicar um elevado risco, o que sem dúvida “solidificou o cenário das hipóteses nas quais o DPIA seria mandatório” (GOMES, 2019, p. 142).

Os referidos critérios podem ser sintetizados nos seguintes pontos: i) avaliação ou classificação, incluindo definição de perfis e previsão (em especial de aspectos relacionados com o desempenho profissional, a situação econômica, saúde, preferências ou interesses pessoais, confiabilidade ou comportamento, localização ou movimentos); ii) decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar; iii) monitoramento sistemático (processamento usado para observar, monitorar ou controlar os titulares dos dados); iv) dados sensíveis ou dados de natureza altamente pessoal; v) dados tratados em grande escala; vi) estabelecer correspondências ou combinar conjunto de dados, excedendo as expectativas razoáveis do titular dos dados; vii) dados relativos a titulares vulneráveis; viii) uso inovador ou aplicação de novas soluções tecnológicas ou organizacionais, como combinar o uso de impressão digital e reconhecimento facial para controle de acesso físico aprimorado, etc, e ix) quando o tratamento em si “impedir que os titulares dos dados exerçam um direito ou usem um serviço ou um contrato” (*EUROPEAN COMMISSION*, 2017b).

Nesse ponto, conforme as orientações firmadas pelo WP29 caso o tratamento de dados satisfaça apenas dois dos critérios apresentados, seria o suficiente para tornar compulsória a realização de um DPIA pelo responsável de tratamento de dados, sendo “que quantos mais critérios forem satisfeitos pelo tratamento maior é a probabilidade de este implicar um elevado risco para os direitos e as liberdades dos titulares de dados”, independentemente das medidas que o responsável pelo tratamento pretende adotar (*EUROPEAN COMMISSION*, 2017b, p. 11).

Transportando esses critérios para a seara brasileira, evidencia-se que os sistemas automatizados de decisão que realizam inferências e a criação de perfis, a depender do caso concreto, poderiam se enquadrar em diversos dos critérios apresentados, principalmente em relação aos seguintes: a) avaliação ou classificação, incluindo definição de perfis e previsão; b) decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar[53]; c)

[53] ‘Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar: tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza “efeitos jurídicos relativamente à pessoa singular” ou que “a afetem significativamente de forma similar” (artigo 35.º, n.º 3, alínea a). Por exemplo, o tratamento pode implicar a exclusão ou a discriminação de indivíduos.’ (*EUROPEAN COMMISSION*, 2017b, p. 09).

estabelecer correspondências ou combinar conjunto de dados, excedendo as expectativas razoáveis do titular dos dados; d) quando o tratamento em si “impedir que os titulares dos dados exerçam um direito ou usem um serviço ou um contrato”.

Nesse ponto, observa-se que as orientações adotadas pela comunidade europeia, na adoção de listas não exaustivas, permitem maior segurança jurídica aos responsáveis pelo tratamento de dados, bem como garantem maior transparência no sistema de gestão de *compliance* e *accountability*. Não é por outro motivo, que o WP29 afirma que:

> Os riscos, que estão relacionados com o potencial impacto negativo nos direitos, liberdades e interesses do titular dos dados, devem ser determinados levando em consideração critérios objetivos específicos, como a natureza dos dados pessoais (por exemplo, sensíveis ou não), a categoria do titular dos dados (por exemplo, menor ou não), o número de titulares de dados afetados e a finalidade do processamento. A gravidade e a probabilidade dos impactos nos direitos e liberdades do titular dos dados constituem elementos a ter em consideração para avaliar os riscos para a privacidade do indivíduo. (*EUROPEAN COMMISSION*, 2014, p. 04).

Desse modo, constatados riscos oriundos de externalidades negativas do tratamento de dados, tal como o enviesamento discriminatório nos sistemas automatizados de decisão, torna-se relevante o estabelecimento de critérios objetivos específicos que permitam a sua delimitação, tal como o WP29 fez através das *Guidelines on data protection impact assessment*, nas quais estruturou nove critérios para aferir o “alto risco”. De igual modo, a gravidade e a probabilidade dos impactos nos direitos e liberdades do titular dos dados constituem *standards* para a avaliação dos riscos.

Danilo Doneda, ao abordar a questão do risco oriundo do tratamento de dados pessoais, em especial por processos automatizados, pondera que:

> O tratamento de dados pessoais, em particular por processos automatizados, é uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais; na eventualidade de esses dados não serem corretos e representarem erroneamente seu titular; pela sua utilização por terceiros sem o conhecimento ou autorização de seu titular, somente para citar algumas hipóteses concretas. Daí a necessidade de mecanismos que proporcionem ao cidadão efetivo conhecimento e controle sobre seus próprios dados, dados estes que são expressão direta de sua própria personalidade. Por esse motivo, a proteção de dados pessoais é tida em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e é considerada um direito fundamental. (DONEDA, 2021, pp. 677-678)

Para exemplificar uma aplicação prática do uso de Relatório de Impacto à Proteção de Dados (RIPDP), Bioni e Luciano (2018) destacam que no cenário europeu, o controlador é obrigado a executar um RIPDP[54] sempre que houver um alto risco em jogo, tal como no caso do uso de perfis como ponto de apoio para tomada de decisões. Desse modo, no âmbito nacional, o uso de sistemas automatizados de decisão para a concessão de crédito, planos de saúde, seleção de candidatos, elegibilidade a programas de assistência social deveriam ser antecedidas pela elaboração de um RIPDP (BIONI; LUCIANO, 2018).

Nesse sentido, embora a ANPD ainda não tenha se manifestado oficialmente sobre o tema, cumpre trazer alguns apontamentos constantes no Guia de Boas Práticas elaborado pelo Comitê Central de Governança de Dados, que “tem como objetivo fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para as operações de tratamento de dados pessoais, conforme previsto no art. 50 da LGPD” (BRASIL, 2020, p. 35).

No referido documento, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

> • uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
> • rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada; (LGPD, art. 12 § 2º);
> • tratamento de dado pessoal sobre “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (LGPD, art. 5º, II);
> • processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);
> • tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);
> • tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral,
> individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);

[54] No âmbito do RGPD europeu o Relatórios de Impacto à Proteção de Dados (RIPDP) é denominado *Data Protection Impact Assesment* (DPIA).

> • tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);
> • tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);
> • alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e
> • reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades. (BRASIL, 2021, p. 35).

Portanto, constata-se a existência de expressa orientação para realização de RIDPD quando o "processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade". Embora essa regulamentação seja menos precisa que as diretrizes europeias, já há sinais no âmbito nacional da necessidade da elaboração do Relatório de Impacto, quando envolver o emprego de sistemas automatizados de decisão, em especial os que utilizem inferências e criação de perfis.

Reforçando esse raciocínio, a proposta de Resolução do CNMP (Proposição 01.00415/2021-60)[55], abordada no item 4.1 do terceiro capítulo, prevê em seu art. 59 um rol de práticas que poderiam configurar violação a direitos e garantias individuais e a autodeterminação informacional, dentre as quais destacam-se o emprego de: i) tratamentos automatizados de dados pessoais, inclusive sensíveis; ii) uso de instrumentos de inteligência artificial, e iii) análises de perfis de titulares, inclusive por meio de agregações de dados históricos.

Diante disso, ainda que não exista pronunciamento oficial pela ANPD quanto ao estabelecimento de listas ou critérios objetivos para analisar quais atividades de tratamento estariam sujeitas ao RIDPD, tendo como base a experiência europeia (RGPD e as diretrizes apresentadas pelo WP29) e levando em consideração as iniciativas embrionárias em âmbito nacional (Guia de Boas Práticas do CCGD e proposta de Resolução do CNMP) é possível afirmar que o tratamento de dados pessoais por sistemas automatizados de decisão, quando empreguem a realização de inferências e a criação de perfis, deve ser considerado uma atividade de alto risco e sujeito à elaboração obrigatória do RIPDP. Além disso, as exigências da avaliação de risco devem ser feitas proporcionalmente à probabilidade de impacto

[55] Que visa instituir a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais do Ministério Público brasileiro.

que os sistemas possam apresentar para os direitos e as liberdades dos titulares de dados conforme será analisado quanto à ponderação do risco. Vencida essa etapa, cumpre analisar alguns pontos a respeito dos *standards* de avaliação de riscos relacionados a quantificação do risco na LGPD.

5.4.2 *Standards* de avaliação de risco

A respeito do tema, novamente a LGPD é omissa e ainda não existe manifestação oficial da ANPD sobre o tema. Segundo Raphael Gellert (2016), a análise do risco pode ser classificada em dois testes de balanceamento, que se desdobram em duas etapas da análise de risco: avaliação de risco e gerenciamento de risco.

O objetivo do primeiro teste seria determinar se existe algum risco na atividade, o que é facilitado no âmbito europeu através das listas não exaustivas constantes no RGPD e na análise dos nove critérios apresentados pelo WP29, que permitem incluir as atividades de tratamento como suscetível de implicar um elevado risco (conforme foi exposto na seção anterior). Dentro dessa primeira etapa, após que fosse delimitado os contornos dos riscos encontrados no processamento de dados, o risco deve ser avaliado em termos de gravidade e probabilidade, este seria o objetivo final da avaliação de risco (GELLERT, 2016). No segundo teste de balanceamento estariam as medidas, salvaguardas e mecanismos necessários para gerenciar o risco.

Nesse sentido, da leitura conjunta do art. 5º, XVII, e do art. 38, parágrafo único, ambos da LGPD, é possível extrair elementos fazendo referência a esses dois testes de balanceamento. No parágrafo único do art. 38 da LGPD há menção expressa que o RIDPD deverá conter a “metodologia” utilizada para a coleta e para a garantia da segurança das informações. De igual modo, no inciso XVII do art. 5º da LGPD há a menção que o RIDPD consiste em uma “documentação” que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos. Assim, embora dependam de regulamentação da ANPD, tais expressões servem como palavras-chaves para conectar a importância da primeira etapa da análise de risco.

Em relação ao segundo teste de balanceamento, em ambos os dispositivos supramencionados, fica clara a necessidade da adoção de ferramentas que

contornem os riscos através da adoção de “medidas, salvaguardas e mecanismos de mitigação de risco” (conteúdo expressamente previsto no inciso XVII do art. 5º e no parágrafo único do art. 38)[56].

Ademais, tendo em vista que a avaliação de riscos está intimamente conectada com o sistema de gestão de *compliance* (SAAVEDRA, 2021), na seção dedicada às boas práticas e à governança, a LGPD apresenta diversos requisitos mínimos que devem conter um programa de governança em privacidade (conforme abordado no terceiro capítulo). Dentre esses parâmetros mínimos, destacam-se: i) a necessidade da observância dos princípios da segurança e prevenção (art. 50, §2º, I); ii) a necessidade de o agente de tratamento de dados se atentar para a probabilidade e a gravidade dos danos para o titular (art. 50, §2º, I) e, iii) a necessidade do estabelecimento de políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade (art. 50, §2º, I, “d”).

Portanto, é possível extrair da própria legislação as diretrizes responsáveis pela delimitação do risco, consistentes na análise da gravidade e probabilidade do dano, tendo em vista que a gestão de *compliance* tem o risco como seu objeto, sendo que a análise e o gerenciamento de riscos é a razão de existência de sistemas de gestão de *compliance* (SAAVEDRA, 2021).

Essa mesma linha de raciocínio consta no Guia de Boas Práticas[57], elaborado pelo Comitê Central de Governança de Dados, que ao interpretar o inciso XVII do art. 5º da LGPD, aponta a imprescindibilidade da identificação dos riscos que geram impacto potencial sobre o titular de dados antes da definição das medidas, salvaguardas e mecanismos necessários (BRASIL, 2020). Embora o guia não enfrente o tema inicial a respeito da “identificação e delimitação das hipóteses que

---

[56] Art. 5º [...] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
Art. 38 [...] Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. (BRASIL, 2018)

[57] O Guia de Boas Práticas “tem como objetivo fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para as operações de tratamento de dados pessoais, conforme previsto no art. 50 da LGPD” (BRASIL, 2020).

podem envolver risco elevado" para o setor privado[58] (o que poderia se dar através das orientações europeias em razão da interoperabilidade das legislações conforme exposto na seção anterior), o referido documento apresenta diretrizes para delimitar o "como" o risco deve ser avaliado em termos de gravidade e probabilidade.

Nesse sentido, verifica-se que o Guia de Boas Práticas, refinando o conteúdo constante no art. 50, §2º, da LGPD, apresenta-se em consonância com as diretrizes europeias na qual a gestão de risco se dá através de uma abordagem escalável e proporcional[59] (*EUROPEAN COMMISSION*, 2014). "Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento" (BRASIL, 2020, p. 39).

Conforme o Guia de Boas Práticas do Comitê Central de Governança de Dados, os responsáveis pelo tratamento de dados, na realização da avaliação de risco, podem utilizar parâmetros escalares, que representam "os níveis de probabilidade de impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança" (BRASIL, 2020, p. 39). A partir disso, cria-se uma matriz de probabilidade x impacto, como um instrumento de apoio para a definição dos critérios de classificação de risco (BRASIL, 2020).

No intuito de viabilizar melhor compreensão sobre o tema, torna-se oportuno apresentar as imagens referentes aos parâmetros escalares e a matriz probabilidade x impacto:

---

[58] Tendo em vista que se trata de um documento voltado para a Administração Pública Federal, a identificação na necessidade de elaborar o Relatório de Impacto baseou-se no art. 4º, inciso III da LGPD, não abrangendo, em regra atividades da seara privada. Contudo, conforme exposto na seção anterior, além dos casos específicos relacionados a Administração Pública, existe uma lista exemplificativa em que há a indicação da elaboração do RIPD e que poderia ser utilizada, por analogia, as empresas privadas até pronunciamento oficial da ANPD sobre o tema.

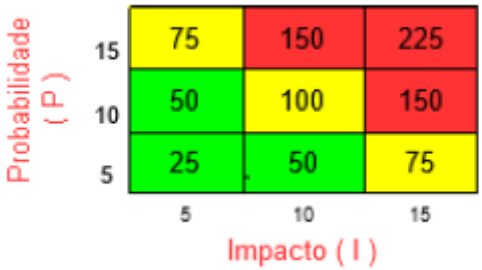
[59] No âmbito da governança pública, a Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016, ao dispor sobre a estrutura do modelo de gestão de riscos na seara da administração pública federal, apresenta a avaliação de risco também numa abordagem escalável e proporcional, ao dispor que "os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência" (BRASIL, 2016). Ademais, a "avaliação de riscos deve ser feita por meio de análises qualitativas, quantitativas ou da combinação de ambas" e "os riscos devem ser avaliados quando à sua condição de inerentes e residuais" (BRASIL, 2016).

Figura 1 - Parâmetros escalares

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

Fonte: (BRASIL, 2020, p. 39)

Figura 2 - Matriz probabilidade x impacto



Fonte: (BRASIL, 2020, p. 39)

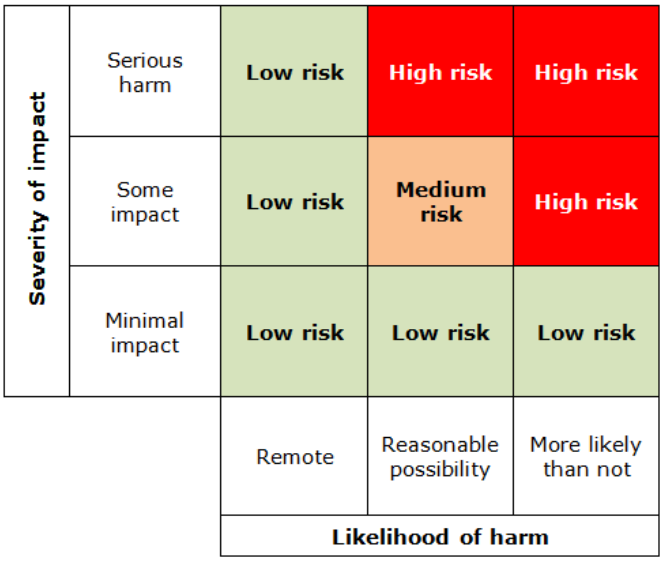
Em uma análise comparativa, o Guia de Boas Práticas elaborado pelo Comitê Central de Governança de Dados adota *standards* de avaliação de risco muitos similares ao Guia do Regulamento Geral de Proteção de Dados do Reino Unido (*Guide to the General Data Protection Regulation* – GDPR), elaborado pela *Information Commissioner's Office* – ICO (Autoridade Independente do Reino Unido). As publicações da ICO recentemente inspiraram a elaboração do Guia de Resposta a Incidentes de Segurança confeccionado pela Secretaria de Governo Digital da Secretaria[60].

Dentre os critérios apresentados pela ICO, destaca-se a verificação do potencial impacto e do tipo de dano ou prejuízo que o tratamento de dados pode causar (*INFORMATION COMMISSIONER'S OFFICE*, 2021b). Ademais, a avaliação do grau do risco considera probabilidade x severidade do impacto (*INFORMATION COMMISSIONER'S OFFICE*, 2021b). Portanto, a proposta adotada pelo Guia de Boas Práticas possui similaridades com as orientações oferecidas pela ICO.

[60] "[...] a Secretaria de Governo Digital (SGD) do Ministério da Economia elaborou o presente guia, que contém diversas referências a publicações e a outros documentos técnicos já existentes. Destacam-se as publicações do *National Institute of Standards and Technology* (NIST); de entidades que atuam como autoridade de proteção de dados da União Europeia (EDPS), da França (CNIL) e do Reino Unido (ICO); e da autoridade de proteção de dados do Brasil (ANPD)." (BRASIL, 2021)

Nesse sentido, torna-se relevante apresentar a matriz estruturada para a avaliação do risco:

Figura 3 - Matriz estruturada para avaliar o risco



Fonte: (INFORMATION COMMISSIONER'S OFFICE, 2021b, p. 09)

Com efeito, estabelecidas algumas regras no intuito de parametrizar a avaliação de riscos com embasamento na gravidade e probabilidade dos danos, é possível trazer outros apontamentos que reforçam os referidos *standards*. Diante disso, para fins de um complemento adicional dessa problemática, impõe-se analisar alguns aspectos da gestão de risco de sistemas que utilizam inteligência artificial que estão relacionados aos sistemas automatizados de decisão.

O desenvolvimento e a implementação de sistemas automatizados de decisão, geralmente estão associados ao emprego de aprendizado de máquina, enquadrando-se, dessa forma, dentro da esfera da inteligência artificial, tema não abordado diretamente pela LGPD. Contudo, os problemas envolvendo a abordagem baseada na gestão de risco da LGPD estão intrinsecamente conectados com as questões envolvendo a abordagem de gestão de risco dos sistemas tecnológicos que usam da inteligência artificial.

Nesse ponto, Ana Frazão (2022) pondera que nos temas envolvendo a inteligência artificial ainda existem diversos debates que não foram endereçados diretamente pela LGPD, razão pela qual há vários campos em que bons programas de *compliance* podem antecipar legislações supervenientes. Esse mesmo raciocínio

se aplica aos sistemas automatizados de decisão que empregam aprendizado de máquina com a realização de inferências e criação de perfis.

No cenário brasileiro tramita perante o Congresso Nacional o Projeto de Lei nº 21/2020 (PL nº 21/2020) que cria o marco legal do desenvolvimento e uso da inteligência artificial pelo poder público, empresas, entidades diversas e pessoas físicas[61]. No inciso III do art. 6º do referido PL há a menção da "gestão baseada em risco", na qual o desenvolvimento e o uso dos sistemas de inteligência artificial deverão considerar os riscos concretos, de modo que as intervenções regulatórias terão a incumbência de ser proporcionais aos riscos concretos oferecidos por cada sistema e à probabilidade de ocorrência desses riscos. O tema ainda possui pouca repercussão na seara nacional, dependendo de maior abertura do legislativo brasileiro aos setores interessados, dentro da perspectiva de uma abordagem multissetorial, envolvendo a participação das sociedades civis, da academia e pesquisadores, dos empresários e da população em geral.

Por sua vez, em abril de 2021 a Comissão Europeia publicou uma proposta de regulamento sobre Inteligência Artificial, a qual estabelece uma estrutura para classificar os sistemas de IA baseados em uma abordagem de risco, com obrigações legais específicas correspondentes a cada categoria de risco (KOENE; 2022). Os sistemas de alto risco estão sujeitas à observância de obrigações legais previstas no regulamento que estabelecem requisitos obrigatórios para que esses sistemas sejam considerados confiáveis, incluindo avaliações de conformidade e práticas relacionadas à avaliação de risco e gestão (KOENE, 2022).

Ademais, segundo KOENE, estão previstos outros requisitos para os sistemas de IA de alto risco que compreendem: i) dados de alta qualidade; ii) documentação e rastreabilidade; iii) transparência; iv) supervisão humana; v) precisão e robustez para mitigar os riscos aos direitos fundamentais, e vi) segurança.

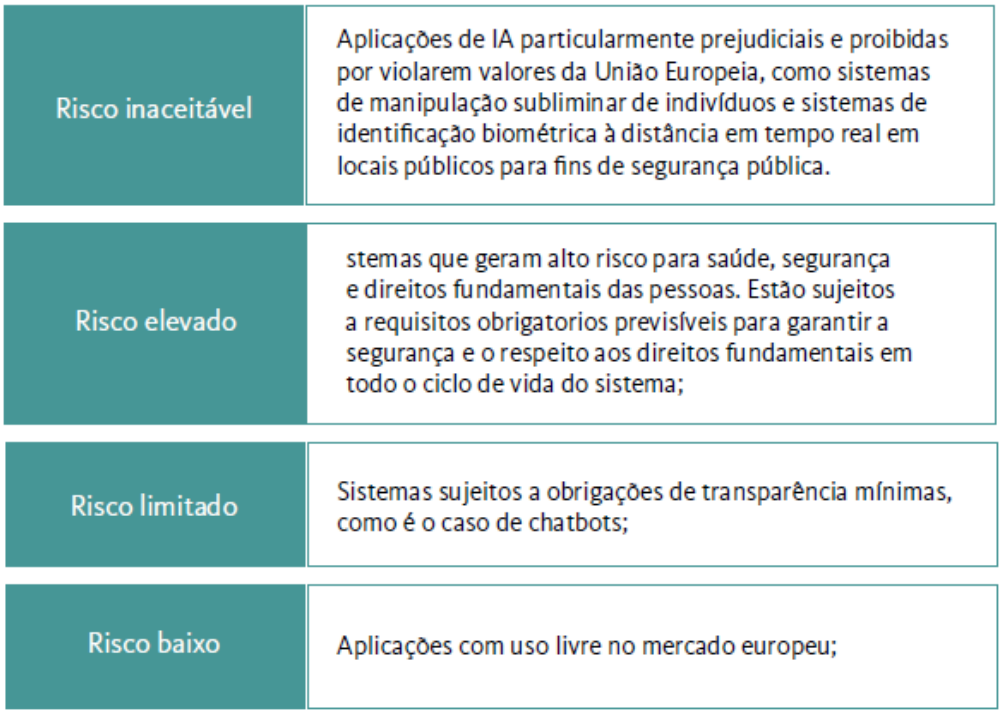
Nesse sentido, a proposta de regulamento de inteligência artificial da União Europeia (*Artificial Intelligence Act* – AIA) traz uma abordagem baseada em riscos preocupada que o desenvolvimento da IA seja confiável, segura, que respeite as regras jurídicas e que gere benefícios aos cidadãos europeus (MAGRANI; OLIVEIRA; CAMPELLO, 2021). Por essa razão, a proposta busca lidar com os

[61] Para maiores informações sobre o tema, recomenda-se a consulta no sítio eletrônico da Câmara dos Deputados: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340.

riscos específicos de aplicações de IA e definir quais sistemas são de lato risco e quais requisitos deveriam ser obedecidos, dentro de uma estrutura de governança (MAGRANI; OLIVEIRA; CAMPELLO, 2021).

Para tanto, cumpre trazer uma análise sintética realizada por Magrani, Oliveira e Campello (2021) a respeito dos quatro níveis de riscos que foram previstos na proposta europeia:

Figura 4 - Níveis de risco propostos na *Artificial Intelligenc Act*



Fonte: (MAGRANI; OLIVEIRA; CAMPELLO, 2021, p. 48)

Em recente relatório desenvolvido por Ansgar Koene (2022), houve o levantamento e avaliação do ecossistema das metodologias de Avaliação de Risco da Inteligência Artificial (*AI risk assessment* – AIRA), com o objetivo de fornecer um retrato atual e orientar os formuladores de políticas sobre a avaliação da AIRA. No referido estudo há uma distinção entre avaliação dos riscos decorrentes do uso de IA e a classificação da IA por sistemas ou aplicações por risco (KOENE, 2022).

A diferença entre ambos é apresentada de forma objetiva e sintética no relatório, a saber:

> (1) avaliação dos riscos decorrentes do uso de IA: estes podem incluir parcialidade, falta de transparência, discriminação, invasão de privacidade,

> uso indevido de pessoal dados e confiança prejudicial e (2) classificação da IA sistemas ou aplicações por risco: o avaliador procura aos riscos decorrentes do uso de IA, a fim de classificar o sistema em uma categoria de risco (por exemplo, alto risco ou de baixo risco). Este segundo tipo de AIRA é especificamente relevante no contexto da lei quando o nível de risco AI determina as obrigações legais aplicáveis. (KOENE, 2022, p. 05)

Nesse ponto, Ansgar Koene (2022) aponta que a avaliação de risco AI, avaliação de impacto e gestão de risco são conceitos intimamente relacionados no contexto da governança da Inteligência Artificial. Portanto, no primeiro tipo de avaliação de risco de IA há a identificação dos riscos específicos que envolvem a ausência de transparência, discriminação, a invasão de privacidade, aumento das assimetrias de poder, por exemplo, enquanto no segundo tipo de avaliação há uma classificação de um nível geral de risco, sistemas de baixo, médio e alto risco, por exemplo, no intuito de avaliar as obrigações legais aplicáveis ao caso concreto.

Assim, analisados os elementos que permitem avaliar os termos de gravidade e probabilidade, torna-se necessário a verificação do da segunda etapa da análise de risco, que consistiria no teste de balanceamento voltado ao gerenciamento do risco (GELLERT, 2016). Nesse viés, “conforme definido pela ISO 31000, o gerenciamento de risco é a identificação, avaliação e priorização de riscos, e a subsequente aplicação coordenada e econômica de recursos para minimizar, monitorar e controlar a probabilidade de eventos não intencionais” (KOENE, p. 06).

Nesse ponto, destacam-se as medidas, salvaguardas e mecanismos que estão expressamente alocadas no final do art. 5º, inciso XVII e art. 38, parágrafo único, ambos da LGPD, a saber:

> Art. 5º [...] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> Art. 38. [...] Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. (BRASIL, 2018)

Essas medidas, salvaguardas e mecanismos representam o conjunto de ferramentas que podem ser extraídas da LGPD dentro de uma perspectiva de *compliance*. No caso específico dos sistemas automatizados de decisão deve ser

observada a estrutura normativa lastreada no direito a inferências razoáveis e no devido processo legal em sua vertente substancial.

Assim, a abordagem baseada em risco abarca requisitos legais para os controladores de dados calibrarem suas obrigações à luz dos perigos que um determinado tratamento de dados pode representar para os direitos e liberdades dos titulares de dados. (QUELLE, 2018), muito similar à etapa do teste multifatorial de legítimo interesse responsável pelo balanceamento dos impactos sobre o titular dos dados e suas legítimas expectativas (art. 10, II, da LGPD). Portanto, exige-se uma interpretação conforme os direitos e liberdades como elemento chave para a abordagem orientada à prestação de contas (QUELLE, 2018).

Nesse viés, compartilha-se do mesmo raciocínio delineado por Maria Gomes (2020) ao apontar para adoção das ferramentas previstas na LGPD como meios para o gerenciamento de riscos, a saber:

> Se não é possível zerar o risco, então, o que é possível fazer? Utilizar ferramentas previstas na LGPD para adotar medidas que visem ao gerenciamento do risco. Nesse sentido, foram previstas na LGPD algumas dessas ferramentas, como Código de Conduta, Certificações, Relatórios de Impacto à Proteção de Dados Pessoais, *Privacy by Design, Privacy by Default*, Programa de Governança. E, nesse caso, voltamos ao início desse tópico para afirmar que as ferramentas são parte da Governança de Proteção de Dados, elas podem estar previstas em Lei, ou ainda, serem criadas para contribuir com a gestão dos procedimentos. No final, o gerenciamento de risco se resume a método e a procedimento. (GOMES, 2020, p. 267)

Nesse ponto, conforme pondera Ana Frazão (2022) no tema envolvendo a inteligência artificial (o que inclui os sistemas automatizados de decisão) ainda existem diversas questões que não foram endereçadas diretamente pela LGPD, razão pela qual há vários campos em que bons programas de *compliance* podem antecipar legislações supervenientes.

Com efeito, para operacionalizar o direito à explicação nos sistemas automatizados de decisão, FRAJHOF (2022) defende o desenvolvimento de instrumentos e mecanismos apoiados na gestão de *compliance.* Desse modo, “impõe-se uma análise *ex ante* relacionada aos potenciais riscos e adequação de se implementar uma decisão algorítmica a um dado contexto e, nesse momento, devem ser definidos quais são os métodos disponíveis para fornecer explicações sobre a decisão automatizada (*ex post*)” (FRAJHOF, 2022, p. 479).

Dentro dessa concepção desenvolvida pela autora, o RIPDP, Códigos de Boas Práticas e Códigos de Conduta representariam mecanismos *ex ante*, enquanto a documentação, auditoria e métodos de interpretação e explicação dos comportamentos e resultados dos algoritmos representariam uma análise *ex post* (FRAJHOF, 2022). Em complemento às diretrizes estabelecidas pela autora, o presente trabalho propõe uma cadeia de mecanismos que consolidam um panorama amplo de proteção da autodeterminação informacional e do livre desenvolvimento da personalidade dos indivíduos sujeitos aos sistemas automatizados de decisão conforme foi detalhado no terceiro capítulo do trabalho.

Contudo, as contribuições de Isabella Frajhof tornam-se relevantes para encerrar o presente capítulo diante da necessidade da análise dos mecanismos da documentação e auditoria que representam instrumentos importantes para: i) o efetivo exercício dos direitos à explicação e à revisão; ii) a análise da proporcionalidade do balanceamento entre o legítimo interesse e a legítima expectativa dos titulares dos dados; iii) o exercício do direito de oposição no tratamento de dados baseado no legítimo interesse; iv) a fiscalização quanto à eficácia dos Relatório de Impacto à Proteção de Dados (RIPDP) na mitigação dos riscos aos direitos fundamentais.

5.5 DA IMPORTÂNCIA DA DOCUMENTAÇÃO NA EFETIVAÇÃO DA *ACCOUNTABILITY* ALGORÍTMICA

A exigência de relatórios de risco está intrinsecamente associada a mecanismos de corregulação, na qual há uma estrutura regulatória colaborativa entre a LGPD e os controladores de dados, conforme tema desenvolvido no item 5.1 do presente capítulo. Além disso, o art. 50 da LGPD prevê a necessidade de “mecanismos internos de supervisão e de mitigação de riscos”. Portanto, avaliar os riscos acaba sendo uma necessidade para verificação da conformidade com a lei e a demonstração de *accountability*.

Segundo Luca Belli:

> A análise de impacto e o consequente relatório tornam-se, portanto, elementos instrumentais pela implementação dos princípios de segurança e prevenção, explicitamente protegidos pelo art. 6.º da LGPD e condição prévia pela implementação de boas práticas de governança de dados que

> podem ser formuladas pelos controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais. (BELLI, 2021, p. 394)

Nessa mesma linha de raciocínio, Carvalho, Mattiuzzo e Ponce (2021) apontam alguns pontos que consideram no desenvolvimento de uma política de governança de dados pessoais robustas, dentre as quais, destacam-se para o presente trabalho: i) mapeamento; ii) identificação de riscos; iii) adequação de sistemas e, iv) adequação de documentos.

O mapeamento interno está nitidamente relacionado à definição de uma estratégia, na medida que um controlador de dados se propõe a utilizar sistemas automatizados de decisão, com a realização de inferências e a criação de perfis, deve realizar um mapeamento de todos os processos de tratamento de dados pessoais da entidade para avaliação dos riscos (CARVALHO; MATTIUZZO; PONCE, 2021).

Segundo Magrani, Oliveira e Campello:

> Antes de aplicar mudanças e incluir novas tecnologias, é indispensável analisar quais são os objetivos buscados, quais estratégias serão adotadas para alcançá-los, quais as ferramentas e a infraestrutura disponíveis, qual o nível de qualificação e formação da equipe que já integra a empresa, e, principalmente, quais os problemas enfrentados ao longo dos processos. (MAGRANI; OLIVEIRA; CAMPELLO, 2021, p. 43)

Vencida essa etapa, torna-se necessário a identificação dos riscos, pois a partir do mapeamento das atividades da empresa, será possível “analisar a adequação das práticas de tratamento de dados pessoais com relação à LGPD”. Portanto, nesse ponto de análise de risco, além da importância da construção de um cenário em que a matriz de risco é desenhada, devem ser criados cronogramas para a adequação da empresa aos elementos normativos oriundos do substrato do direito a inferências razoáveis, de modo a serem operacionalizadas medidas de segurança e minimização dos riscos verificados.

No cenário brasileiro, embora ainda não exista uma lista de formas de tratamento que podem ser consideradas de alto risco, o Guia de Boas Práticas elaborado pelo Comitê Central de Governança de Dados pode ser usado como parâmetro, bem como os controladores de dados podem se valer das orientações firmadas no âmbito europeu constantes no *Guidelines on data protection impact assessment* (diretrizes sobre avaliação de impacto na proteção de dados) do WP29,

porquanto, conforme exposto no início do presente capítulo, existem pontos convergentes entre o RGPD e a LGPD que garantem uma interoperabilidade entre a proteção de dados em âmbito nacional ou transnacional.

Por sua vez, o responsável pelo tratamento de dados ao analisar a adequação dos sistemas em conformidade com os direitos e liberdades das pessoas, deve garantir o estabelecimento de medidas necessárias para contornar esses riscos de forma proporcional, cuja orientação estará baseada em toda a estrutura normativa constante na LGPD e que pode ser inferida a partir do direito a inferências razoáveis.

Nesse ponto, um planejamento estratégico com a execução de projetos-piloto revela-se interessante para adequar os sistemas tecnológicos aos resultados esperados (conformidade com a LGPD) e viabilizar o próprio aprimoramento antes da execução em si (MAGRANI; OLIVEIRA; CAMPELLO, 2021). Trata-se de “um projeto a ser pensado e aplicado com cautela, mapeando e minimizando riscos” (MAGRANI; OLIVEIRA; CAMPELLO, 2021). Nesse sentido, o art. 49 da LGPD prevê que “os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares” (BRASIL, 2018).

Ademais, “a documentação no desenvolvimento de um sistema é fundamental para que outras pessoas, que não apenas os seus desenvolvedores, compreendam o seu funcionamento” (FRAJHOF, 2022, pp. 484-485). Nesse viés, o WP 29 aponta que a forma de documentação das atividades de processamento pode mudar de acordo com o risco do processamento, no entanto, todos os controladores de dados devem documentar suas atividades de processamento para aumentar a transparência e a responsabilidade (*EUROPEAN COMMISSION*, 2014).

Assim, dentro de uma ideia de *compliance* e *accountability* a elaboração de relatórios detalhando como os sistemas foram desenvolvidos e quais os processos de sua implementação representam uma atuação necessária para que o responsável pelo tratamento de dados atue em conformidade com o princípio da transparência, garantindo visibilidade dos procedimentos aos titulares dos dados, a ANPD e outros interessados (diante da perspectiva multissetorial que envolve o DNA da LGPD). “Quanto maior o arcabouço de evidências que forem geradas em relação ao cumprimento da lei e do dia a dia do Programa de Privacidade, melhores são as

chances de a organização evitar sanções, atender satisfatoriamente auditorias etc" (VAINZOF; MORAES, 2021, p. 725).

Por essa razão, Bruno Bioni *et al*. (2021), partindo de uma interpretação sistemática da LGPD e considerando a natureza do instituto do RIPDP, defendem que seria obrigatória a publicização do Relatório de Impacto. Reforçando esse raciocínio, a própria LGPD, em seu art. 32, prevê que "a autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais".

No mesmo sentido, Wolfgang Hoffmann-Riem (2021, p. 116), ao abordar sobre as avaliações de impacto, afirma que "o procedimento e o resultado devem estar sujeitos ao escrutínio público, envolvendo também representantes da sociedade civil", o que estaria em conformidade com a "possibilidade de controle democrático e constitucional de sistemas inteligentes" (HOFFMANN-RIEM, 2021, p. 129).

Segundo Bruno Bioni *et al*.:

> As normas de regulamentação de proteção de dados ao redor do mundo cada vez mais têm como norte processos de gerenciamento dos riscos das atividades de tratamento de dados, centrando-se em mecanismos de identificação e mitigação dos riscos e no princípio de *accountability* como medidas de democratização do processo de regulação das tecnologias. Com a evolução de novas tecnologias de informação, ampliam-se os efeitos adversos das atividades de tratamento de dados pessoais ao mesmo tempo em que se cria uma maior assimetria informacional sobre o funcionamento de tais tecnologias. A prestação de contas, na forma da publicização do RIPD, permite a participação pública na definição de que riscos oriundos do tratamento de dados são toleráveis. (BIONI, *et al*., 2021, p. 07)

Portanto, dentro dessa perspectiva de democratização do processo de regulação das tecnologias, a documentação (através da elaboração de relatórios e manutenção de documentos) torna-se essencial para avaliar a legitimidade e a conformidade dos sistemas automatizados de decisão, sendo um "ponto benéfico para eventual auditoria" a ser realizado pela ANPD (de ofício, em razão do seu poder-dever de fiscalização[62], ou quando solicitado por algum interessado, a

[62] "Lei nº 13.709/2018. Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019): [...] II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019) [...] IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019) [...] XVI - realizar auditorias, ou determinar sua realização, no âmbito da

exemplo do que consta no §2º do art. 20 da LGPD[63]) e “para atender a exigências de *accountability*” (MAGRANI, OLIVEIRA; CAMPELLO, 2021). Nesse sentido, o WP29 assinala que a documentação é indispensável para que os controladores gerenciem a responsabilidade de forma eficaz e para que seja possível um controle *ex post* pelas Autoridades Independentes, bem como para o exercício dos direitos pelos titulares de dados (*EUROPEAN COMMISSION*, 2014).

Wolfgang Hoffmann-Riem (2021, p. 130) aponta a necessidade de “um monitoramento contínuo e avaliações de impacto retrospectivas, realizadas como verificações internas e/ou externas”, o que poderia ser materializado através de obrigações que deem suporte para documentação e para expedição de relatórios e informações (HOFFMANN-RIEM, 2021, p. 130).

Não é por outra razão que Bruno Bioni também defende a obrigatoriedade em documentar o teste de ponderação do legítimo interesse (*Legitimate Interests Assessment* – LIA), a partir de uma interpretação sistemática da LGPD e do princípio da *accountability*, a saber:

> No entanto, doutrinariamente, uma parcela dos órgãos reguladores já tem se posicionado acerca da obrigatoriedade do LIA. A partir do princípio da *accountability*, argumenta-se que os controladores de dados deveriam demonstrar a sua responsabilidade em balancear seus interesses diante dos titulares por meio dessa documentação em específico.
> No âmbito da LGPD, a moldura normativa é substancialmente distinta:
> a) primeiro, porque as fases do LIA estão talhadas no próprio texto duro da lei, estando distribuídas ao longo dos incisos e parágrafos do art. 10. Ou seja, não se trata de uma diretriz interpretativa, mas, efetivamente, do próprio conteúdo normativo em torno da licitude de tal base legal;
> b) segundo, porque não apenas o dever de informação é reforçado como corolário do princípio da transparência, mas, também e principalmente, o dever de registro das atividades de tratamento de dados. Com isso, a racionalidade da LGPD aponta para uma documentação especial, que nos parece ser justamente o LIA. (BIONI, 2021, p. 172).

Esse dever de registro das atividades de tratamento de dados consta expressamente previsto no art. 37 da LGPD, o qual prevê que “o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse”. Portanto,

---

atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019).” (BRASIL, 2018)

[63] “Lei nº 13.709/2018. Art. 20 [...] § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.” (BRASIL, 2018)

resta nítida a conexão do dispositivo com a estrutura deontológica consagrada como núcleo duro da LGPD, demandando à observância aos princípios da transparência e da responsabilização e prestação de contas (*accountability*) quando da realização de tratamento de dados.

Nesse viés, a obrigatoriedade em documentar o teste de ponderação do legítimo interesse também se torna necessária para o próprio exercício do direito de oposição, que constituiria a principal salvaguarda nos casos de sistemas automatizados de decisão que empregam a realização de inferências ou criação de perfis, diante da necessidade de adoção de mecanismos de transparência que permitam ao titular dos dados se opor a tal tipo de tratamento (*opt-out*).

De igual modo, a documentação é fundamental para os incidentes de segurança da LGPD, "a qual indica uma série de informações mínimas que deverão ser tratadas na comunicação da organização para os titulares de dados pessoais eventualmente afetados por incidentes (art. 48, §1º)[64]" (CARVALHO; MATTIUZZO; PONCE, 2021, p. 370). Nesse sentido, conforme dispõe o Guia de Resposta a Incidentes de Segurança elaborado pela Secretaria de Governo Digital (SGD) do Ministério da Economia, "é importante que todas as informações e evidências coletadas e as ações do processo de tratamento de incidente de segurança à proteção de dados sejam documentadas, de modo a possibilitar a elaboração de um relatório final do incidente" (BRASIL, 2021).

Por sua vez, é através da documentação e da elaboração de relatórios que será possível a realização de auditoria, a qual "tem sido uma solução que tem ganhado certa aceitação para investigar resultados e predições algorítmicas, pois seria uma forma de assegurar transparência qualificada (*qualified transparency*)" (FRAJHOF, 2022, p. 486). Segundo Magrani, Oliveira e Campello (2021) a auditoria tem como objeto garantir o respeito das regras jurídicas, a proteção de dados, a

---

[64] "Lei nº 13.709/2018. Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
I - a descrição da natureza dos dados pessoais afetados;
II - as informações sobre os titulares envolvidos;
III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV - os riscos relacionados ao incidente;
V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo." (BRASIL, 2018)

observância de padrões éticos e a adequação das técnicas com as demandas da cibersegurança, tratando-se de um importante mecanismo de governança e de *compliance* direcionado a analisar o comportamento da IA.

Segundo Mokander e Floridi (2021, p. 02), “embora os padrões ainda não tenham surgido, já existe uma variedade de abordagens diferentes para a auditoria de IA baseada em ética: as auditorias de funcionalidade focam na razão por trás da decisão, as auditorias de código envolvem a revisão do código-fonte e as auditorias de impacto investigam os efeitos de um algoritmo saídas”. Nesse sentido, Mokander e Floridi (2021) propõem uma auditoria baseada na ética, a qual teria como finalidades: i) viabilizar um suporte à tomada de decisões permitindo o monitorando dos resultados; ii) informar as pessoas porque uma decisão foi tomada e como contestá-la; iii) permitir uma a abordagem específica do setor para governança de IA; iv) tutelar os direitos humanos, antecipando e mitigando os danos; v) atribuir responsabilidade dentro de estruturas de governança existentes, e vi) balancear os conflitos de interesse.

Ademais, segundo os autores (2021) para que uma auditoria baseada na ética seja viável é imprescindível: i) a realização de um monitoramento e avaliação contínuos a respeito das saídas dos sistemas, bem como a documentação dos processos; ii) constituir-se um dos elementos de governança, portanto, fazer parte de um sistema sociotécnico dentro de uma abordagem holística na qual se leva em consideração o conhecimento de outras alternativas disponíveis para avaliar os sistemas de IA; iii) ser vista como um processo dialético; iv) promover o alinhamento de valores estratégicos das estruturas de fiscalização com a harmonização das políticas organizacionais, e vi) fornecer um feedback ativo ao processo contínuo de *(re-)design*, para tanto exige-se a implementação de uma regulamentação baseada no projeto (em *design*) que implique no incentivo de implementação de transparência no desenvolvimento das tecnologias.

Dentre os apontamentos realizados por Mokander e Floridi observa-se um reforço em registrar que a auditoria é apenas um dos mecanismos de governança de algoritmos, devendo ser aplicado em conjunto com os demais mecanismos, conforme a construção proposta no presente trabalho. Reforçando essa compreensão, pode-se afirmar que a auditoria se revela como um “mecanismo fundamental que se relaciona fortemente com a ideia de transparência, mas que deve ser uma dentre diversas medidas e boas práticas adotadas pela empresa para

assegurar uso ético, responsável e confiável da IA" (MAGRANI, OLIVEIRA; CAMPELLO, p. 49).

Nesse contexto, a realização de auditoria está expressamente prevista no parágrafo segundo do art. 22 da LGPD, ao prever que em caso de não oferecimento de informações aos titulares de dados, com fundamento na proteção dos segredos comercial e industrial, a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Além disso, dentro das atribuições da ANPD de fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento a LGPD, a legislação confere a autoridade nacional competência de realizar auditoria ou determinar a sua realização, desde que observe os segredos comercial e industrial.

Esse raciocínio pode ser extraído da leitura conjunta dos incisos II, IV e XVI, todos do art. 55-J da Lei 13.709/2018, a saber:

> Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019): [...]
> II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)
> [...] IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)
> [...] XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019). (BRASIL, 2018)

Desse modo, observa-se que a ANPD possui o dever-poder de realizar auditorias externas independentes para "exercer o papel de atestar a idoneidade do sistema algorítmico ou de conformar os principais aspectos que estariam sob discussão" (FRAZÃO, 2021b, p. 04). Por esses motivos, Frazão (2018b) registra o inequívoco papel central da autoridade nacional na questão de governança e do *compliance*, porquanto o referido órgão teria o poder de determinar uma política adequada de proteção de dados, considerando os impactos e riscos para os usuários do uso de sistemas decisórios automatizados.

Nesse ponto, reforçam-se os argumentos elencados na seção 5.1 deste capítulo quanto à importância da transformação da ANPD em uma agência

reguladora. Isso decorre da necessidade de assegurar que a instituição tenha autonomia e independência, não só administrativa, mas como financeira, suficientes para estabelecer mecanismos mais propícios ao estímulo da corregulação e ao cumprimento de suas competências legais, tal como, a realização de auditorias externas, o que demandaria a constituição de um quadro pessoal técnico altamente qualificado para o exercício das referidas atribuições e uma estrutura mais robusta que um órgão vinculado à Presidência da República.

Nesse panorama, deve-se observar que a auditoria não precisa ficar exclusivamente ao encargo da ANPD, pois conforme dispõe o inciso XVI do art. 55-J da LGPD, a autoridade nacional pode determinar a sua realização, com a terceirização dessa função. Contudo, aqui deve-se realizar uma interpretação mais ampla, permitindo que essa tarefa também possa ser atribuída especificamente a "organizações multilaterais" (MAGRANI, OLIVEIRA; CAMPELLO, p. 49) e que talvez possuam maiores mecanismos de publicização e transparência do que empresas contratadas pela ANPD. Tal raciocínio se faz em razão do caráter essencialmente multissetorial que envolve a estrutura de proteção de dados.

Por fim, a documentação também é relevante para a implementação de outras propostas relacionadas com a governança dos sistemas de decisão algorítmica, tais como a certificação. A adoção de mecanismos de certificação interna e externa, representa uma ferramenta em conformidade com os princípios da prevenção, responsabilização e prestação de contas.

Nesse sentido, a LGPD, nos parágrafos terceiro e quarto do art. 35, aponta que autoridade nacional poderá designar organismos de certificação para a realização, dentre outras atribuições, dos códigos de conduta para transferência internacional por controlador de dados pessoais, que permanecerão sob sua fiscalização nos termos definidos em regulamento. Ademais, "os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados" (BRASIL, 2018).

Com a publicação do Decreto nº 10.474/2020, regulamentando a LGPD, conferiu-se ao Conselho Diretor da ANPD a competência para designar e fiscalizar organismos de certificação, bem como para definir o conteúdo de cláusulas padrão e verificar o conteúdo dos certificados e códigos de conta para transferência internacional por controlador de dados pessoais. Ademais o referido conselho poderá rever os atos realizados por organismos de certificação e no caso de

descumprimento da LGPD anular os referidos atos (art. 4, incisos XII, “a”, XIII e XIV, do Decreto nº 10.474/2020).

No âmbito europeu[65], o RGPD dispõe sobre a certificação em seu art. 42, a saber:

> Os Estados-Membros, as autoridades de supervisão, o Conselho de Administração e a Comissão devem incentivar, em especial a nível da União, o estabelecimento de mecanismos de certificação da proteção de dados e de selos e marcas de proteção de dados, a fim de demonstrar o cumprimento do presente regulamento das operações de tratamento por controladores e processadores. 2 Devem ser consideradas as necessidades específicas das micro, pequenas e médias empresas. (UNIÃO EUROPEIA, 2016)

Portanto, observa-se da referida disposição legal que, diferentemente da LGPD, o regulamento europeu possui uma abordagem mais clara e precisa ao recomendar expressamente a “criação de procedimentos de certificação em matéria de proteção de dados” que conferirão a comprovação da conformidade, reforçando a estruturação de mecanismos de *compliance* e *accountability*.

Seguindo essa linha de raciocínio, o Considerando 77, que aborda o tema sobre as “diretrizes de avaliação de risco”, menciona o uso de “certificações aprovadas” como um mecanismo de *compliance* na identificação e mitigação dos riscos encontrados nos sistemas. De igual modo, no Considerando 81 há expressa previsão que a “certificação” pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento.

Por sua vez, o Considerando 100 é destinado exclusivamente ao tema da “certificação” e dispõe que: “a fim de aumentar a transparência e o cumprimento do presente regulamento, deve ser incentivado o estabelecimento de mecanismos de certificação e selos e marcas de proteção de dados, permitindo que os titulares dos

---

[65] No estudo publicado pelo Parlamento Europeu, denominado *A governance framework for algorithmic accountability and transparency*, há o registro da proposta realizada por Matthew Scherer, em sua obra *Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies*, da constituição de uma agência encarregada de certificar a segurança dos sistemas de decisão algorítmica em combinação com uma estrutura de responsabilidade legal sob a qual os “projetistas, fabricantes e vendedores de sistemas certificados pela agência” estariam sujeitos a responsabilidade civil limitada, enquanto os sistemas não certificados estariam sujeitos a responsabilidade conjunta e solidária (KOENE, *et a*l., 2019). A ideia seria criar um ambiente regulatório propício para que os projetistas e fabricantes internalizem os custos associados aos danos causados por decisões algorítmicas, forçando uma atuação preventiva e voltada a segurança no desenvolvimento das tecnologias (KOENE, *et al*., 2019).

dados avaliem rapidamente o nível de proteção de dados de produtos e serviços relevantes" (UNIÃO EUROPEIA, 2016).

Ademais, deve-se registrar que no âmbito europeu a presunção de regularidade do sistema de AI e do próprio algoritmo certificado é relativa e tem uma finalidade eminentemente preventiva, porquanto a certificação não reduz a responsabilidade do agente de tratamento pelo cumprimento das demais regras do RGPD europeu e não prejudica as funções e poderes das autoridades de controle (art. 42, item 4, do RGPD). Essa percepção é reforçada pela LGPD que permite que a autoridade nacional revise os atos de certificação, bem como proceda à anulação dos casos em desconformidade com a lei (art. 35, §4º). Ademais, a "transferência internacional de dados pessoais" depende que o controlador comprove a observância dos princípios e do regime de proteção de dados previstos na LGPD através de "selos, certificados e códigos de conduta regularmente emitidos".

Por fim, a normas técnicas ISO/IEC[66] revelam-se como importantes diretrizes para o estabelecimento de boas práticas e padrões que podem ser operacionalizados tanto no setor público quanto no setor privado, especialmente pela possibilidade da combinação dos mecanismos de governança, na qual a entidade de tratamento obtém a certificação mediante a realização de auditoria, tal como previsto na Norma Técnica ABNT NBR ISSO/ESC 27001:2013 (JIMENE; ZANI, 2021). Além disso, também podem ser empregadas para a definição de código de boas práticas, tal como a ABNT NBR ISSO/IEC 27002:2013 (JIMENE; ZANI).

Nesse sentido, Ansgar Koene (2022, p. 08) afirma que a "comunidade técnica está fazendo um bom progresso no desenvolvimento de padrões e orientações para a implementação técnica da avaliação de risco de IA". Ademais, para fins de relevância em relação a Avaliação de Risco da Inteligência Artificial (*AI risk assessment* – AIRA), existem diversos projetos de normas técnicas interessantes (KOENE, 2022).

Embora ainda não existam diretrizes oficiais da ANPD quanto ao mecanismo de certificação, deve-se observar que o seu emprego é relevante como mecanismo de controle da autorregulação, especialmente quando relacionado com a elaboração

[66] "As organizações ISO – International Organization for Standardization e IEC – International Electrotechnical Commission são entidades internacionais, ambas sediadas na Suíça e formadas por representantes de diversos países, cujo objetivo é criar regras e diretrizes em diversas áreas de interesse técnico e econômico" (JIMENE; ZANI, 2021, p. 465)

dos Códigos de Conduta dentro de uma perspectiva de estruturação de mecanismos de *compliance* e *accountability*. Contudo, as mesmas observações realizadas para o mecanismo de auditoria valem para a certificação, que demanda a estruturação de uma autoridade nacional autônoma e independente na formatação de uma agência reguladora.

Nessa seara, a criação de programas de conformidade de dados é essencial para enfrentar as externalidades negativas oriundas dos sistemas automatizados de decisão. Segundo Caitlin e Gomes (2022, pp. 173-174) a criação de programas de conformidade de dados decorre da aplicação dos princípios estruturantes da LGPD, assim como no caso do GDPR, sendo fundamental a construção de modelos transparentes de sistemas de IA garantindo-se "ao titular de dados pessoais informações claras sobre o uso de IA no tratamento de seus dados pessoais e quais as finalidades e os resultados esperados em tais aplicações".

Os programas de *compliance* ganham destaque como mecanismos ideais para conduzir que os agentes econômicos cumpram os comandos legais e éticos, tendo um papel central na implementação e suplementação da LGPD (FRAZAO, 2022). Nesse ponto, os programas de conformidade são responsáveis por atestar a própria legitimidade para o tratamento de dados pessoais que devem estar de acordo com uma base legal dentro da perspectiva da racionalidade *ex ante* de proteção de dados.

Dentro do raciocínio de corregulação, a LGPD apresenta diretrizes gerais sobre as operações de tratamento de dados pessoais – incluídas operações de coleta, armazenamento ou modificação que envolvam a realização de inferências e a criação de perfis (art. 5º, X)[67]. Diante disso, é possível afirmar que a LGPD cria uma série de obrigações aos responsáveis pelo tratamento de dados pessoais que devem desenvolver e aplicar os sistemas automatizados de decisão em conformidade com a lei.

[67] "Lei 13.709/2018. Art. 5º. Para os fins desta Lei, considera-se: [...] X - tratamento: 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." (BRASIL, 2018)

6 CONCLUSÃO

Na atual estrutura social contemporânea os algoritmos julgam decisões cada vez mais importantes nas vidas dos indivíduos e isso decorre da constatação de uma dependência cada vez maior da humanidade de sistemas automatizados de decisão, que empregam o uso de inteligência artificial, em especial o aprendizado de máquina. Sem dúvida que o avanço tecnológico gera diversos impactos positivos para as sociedades, contudo, os aplicativos de IA também podem gerar consequências inesperadas e não intencionais, representando novas formas de riscos que precisam ser contornadas.

A presente pesquisa buscou investigar os desafios técnicos oriundos da mecânica de funcionamento dos sistemas automatizados de decisão, que empregam métodos de análise inferenciais e criação de perfis, no intuito de revelar que esses sistemas não são neutros e demandam o desenvolvimento de estratégias na consolidação de mecanismos de governança de algoritmos. Dentre os principais desafios a serem contornados por essas ferramentas está a ausência de transparência, que cria barreiras quanto às informações úteis a respeito dos critérios utilizados no tratamento de dados pelas empresas. Além disso, essa opacidade afeta o exercício do contraditório e da ampla defesa dos destinatários dos sistemas, que acabam tendo seus direitos afetados sem a possibilidade de se opor.

No primeiro capítulo do presente trabalho, buscou-se trazer a compreensão de como a mediação tecnológica promovida pela governamentalidade algorítmica impacta na vida das pessoas. De igual modo, foram realizados apontamentos no intuito de investigar algumas estruturas invisíveis que compõem a mineração de dados (*data mining*), principal ferramenta de análises da big data, e sua relação na criação de perfis e na realização de inferências.

Nesse contexto, observou-se que a lógica dos sistemas automatizados de decisão, muitas vezes não está preocupada entre a obtenção de verdades, provas ou fatos dentro de uma análise causal, mas sim, em produzir padrões de dados estatísticos que viabilizem o maior grau de predição possível através de correlações. Embora atos de generalização sejam aceitos socialmente, a preocupação do presente estudo é de buscar mecanismos que propiciem maior transparência e *accountability* nos algoritmos de forma a viabilizar mecanismos de controle de

conformidade e adequação dos tratamentos de dados com as diretrizes da LGPD e da dignidade da pessoa humana.

Nesse panorama deve-se reconhecer que algoritmos tendenciosos e opacos repercutem em riscos sociais e ao direito fundamental de proteção de dados, em especial na sua vertente principiológica da autodeterminação informacional e do livre desenvolvimento da personalidade. Ademais, a falta de uma justificativa dos controladores de dados que viabilize que os destinatários possam compreender como suas informações estão sendo empregadas na construção de inferências e criação de perfis é fundamental para permitir a efetiva tutela dos direitos e garantias dos destinatários desses sistemas.

Diante disso, no segundo capítulo houve a proposição da ampliação do âmbito de proteção dos dados pessoais a partir do reconhecimento do direito a inferências razoáveis como um desdobramento da dimensão subjetiva do direito fundamental da proteção de dados. Segundo Ingo Sarlet, não há na Constituição Federal qualquer referência a posições jurídicas-subjetivas específicas quanto ao direito fundamental de proteção de dados, o que permite buscar uma ampliação extensiva dos direitos pessoais de forma que atendam também outros valores tutelados na esfera constitucional, tais como os princípios constitucionais implícitos do livre desenvolvimento da personalidade e da autodeterminação informacional, extraídos da dignidade da pessoa humana e dos valores da liberdade e igualdade consagrados na Constituição Federal.

Ademais, através de uma perspectiva da racionalidade *ex ante* de proteção de dados desenvolvida por Bruno Bioni e Laura Mendes (que possui como características a adoção de um conceito amplo de dado pessoal, da necessidade de base legal para o tratamento de dados e do balanceamento entre o legítimo interesse e a legítima expectativa do titular de dados) houve a proposição de uma estrutura normativa da LGPD com capacidade de dar suporte legal ao reconhecimento do direito a inferências razoáveis consoante análise sistemática realizada no art. 6º, V, art. 9º, art. 18, III e IV e art. 10, II, todos da LGPD.

De igual modo, o principal vetor para alcançar o livre desenvolvimento da personalidade e a autodeterminação informacional é assegurar que o fluxo informacional atenda às legítimas expectativas dos indivíduos, portanto, a legítima expectativa se apresenta como *standards* de comportamento do controlador do que razoavelmente pode ser esperado do titular.

Nessa linha de raciocínio, apresentaram-se diretrizes do que poderia ser entendido como “razoável” ao direito de inferências, tendo como eixo central a concepção desenvolvida por Humberto Ávila da aplicação do princípio da razoabilidade em suas três acepções: i) razoabilidade como equidade; ii) razoabilidade como congruência, e iii) razoabilidade como equivalência.

Por sua vez, a partir do reconhecimento de um direito a inferências razoáveis, se propôs a análise dos efeitos oriundos da dimensão objetiva do direito fundamental à proteção de dados, especialmente referente a construção de mecanismos de salvaguarda do direito à autodeterminação informacional e da tutela do livre desenvolvimento da personalidade, que constituiriam ferramentas estruturantes de um verdadeiro devido processo informacional, buscando alcançar a sua vertente substancial. Ao final do capítulo, foi apresentada uma estrutura de mecanismos de governança focados no fornecimento de uma justificativa *ex ante* que mitiguem as externalidades negativas de aplicações de IA de alto risco em sistemas automatizados de decisão.

No terceiro capítulo, deu-se prosseguimento aos desdobramentos da dimensão objetiva do direito fundamental de proteção de dados, desenvolvida ao final do segundo capítulo, apresentando-se uma cadeia de mecanismos que compõem a estrutura normativa da LGPD na tutela do direito a inferências razoáveis que é consolidada através de quatro pilares que foram divididos da seguinte maneira: i) guias deontológicos (art. 6º); ii) regras de boa governança (art. 50); iii) legítimo interesse (art. 7º, IX) e iv) direitos à explicação e à revisão (art. 20).

Tendo em vista que os direitos à revisão e à explicação possuem maior relevância concedida pelas legislações protetivas de dados, quando se fala em sistema automatizado de decisão, realizou-se uma ancoragem comparativa dos institutos constantes no RGPD europeu, no intuito de contornar as barreiras quanto à eficácia dos direitos à explicação e à revisão e impulsionar a sua procedimentalização de modo a atender aos guias deontológicos constantes no art. 6º da LGPD.

A partir disso, realizou-se a análise do legítimo interesse como instrumento de *accountability* algorítmica, especialmente diante da sua característica marcada pela mitigação dos riscos e uma abordagem essencialmente preventiva. Ademais, o teste multifatorial de legítimo interesse está intrinsecamente relacionado a uma

abordagem baseada em risco, ponto específico que foi explorado no quarto capítulo do trabalho.

Nesse contexto, foram desenvolvidos mais dois mecanismos de governança (estrutura principiológica e regras de boas práticas e governança de dados) que constituem o substrato normativo do direito a inferências razoáveis e que servem como verdadeiros guias no estabelecimento de diretrizes de conformidade (*compliance*) possuindo uma íntima conexão com a responsabilidade e prestação de contas (*accountability*) dos agentes responsáveis pelo tratamento de dados.

Da análise da estrutura deontológica é possível constatar a existência de diversos mecanismos que devem orientar a atuação dos responsáveis pelo tratamento de dados em sistemas automatizados de decisão, obrigando os agentes privados e públicos o desenvolvimento de tecnologias confiáveis e auditáveis, sob pena de responsabilização. De igual modo, as regras de boas práticas e governança de dados revelam a necessidade de uma atuação proativa dos agentes de tratamento de dados, estimulando o desenvolvimento por projeto de tecnologias que sejam mais receptivas à explicabilidade e à contestabilidade como forma de garantir a intelegibilidade e a *accountability* dos sistemas automatizados de decisão, especialmente aqueles que utilizem de aprendizado de máquina, com a realização de inferências e criação de perfis.

No quarto capítulo buscou-se delinear o papel da governança de algoritmos no contexto da LGPD, com o intuito de implementar uma transparência e *accountability* algorítmicas. Nesse sentido, considerando que o enfrentamento dos riscos oriundos dessas tecnologias demanda múltiplas soluções optou-se pela investigação da estrutura de governança focada na corregulação, porquanto essa demonstra ser o arranjo institucional revelado pela LGPD que aposta em um sistema de governança em rede com nítidas características do multissetorialismo, no qual as competências são distribuídas entre vários atores, como, por exemplo, setor privado, academia, sociedade civil, organizações sem fins lucrativos, centros de pesquisa e o Estado.

Ademais, ainda que existam mecanismos de autorregulação (por exemplo, Código de Conduta), a própria LGPD sempre será um componente-chave do modelo, pois conforme Mayntz a autorregulação no contexto da governança será sempre uma autorregulação regulada. Por sua vez, a autorregulação, para sua eficiência, demanda uma autoridade nacional de proteção de dados independente e

autônoma, não apenas administrativamente, mas com orçamento próprio que a conceda maior liberdade de iniciativa, essencial para o estímulo da corregulação. Por essa razão, defendeu-se a necessidade da transformação da ANPD em uma agência reguladora.

A implementação de *accountability* por meio de *compliance* tem como objetivo garantir a inclusão de parâmetros regulatórios preventivos, o que se daria em uma estrutura de governança da corregulação. Assim, em razão de atuar em um plano *ex ante*, a *accountability* funciona como um guia para os responsáveis pelo tratamento de dados, reforçando a estrutura normativa apresentada no terceiro capítulo, na qual as empresas que desenvolvem sistemas automatizados de decisão devem se orientar: i) pelos princípios; ii) pelo balanceamento entre o legítimo interesse e a legítima expectativa dos titulares de dados, com o fornecimento de justificativas prévias e informações úteis a respeito da lógica subjacente dos sistemas de modo a viabilizar o exercício do contraditório e da ampla defesa; iii) através da viabilização do exercício dos direitos de revisão, explicação e oposição, e; iv) pelo estabelecimento de códigos de boas práticas e uma gestão de governança interna voltada a assegurar a atuação em conformidade com as diretrizes da lei.

Nesse contexto, se insere o princípio *accountability* que está intimamente conectado com a abordagem baseada em risco, porquanto, traz consigo uma preocupação relacionada à necessidade da realização de um tratamento de dados com adequação, confiabilidade e segurança, de modo que os sistemas automatizados de decisão sejam implementados buscando minimizar os riscos e danos. Não é por outro motivo que um programa de *compliance* deve se basear na análise de risco da atividade.

Assim, nas últimas seções do quarto capítulo buscou-se investigar a abordagem baseada em risco, tendo como foco a análise dos pressupostos para a elaboração do Relatório de Impacto à Proteção de Dados (RIPDP). Embora o relatório de impacto não esteja minimamente procedimentalizado pela ANPD, através de um estudo comparado com o RGPD e as orientações fornecidas pelo extinto 29 *Working Party Group* (WP29), bem como levando em consideração as iniciativas embrionárias em âmbito nacional (como por exemplo Guia de Boas Práticas do Comitê Central de Governança de Dados e proposta de Resolução do CNMP) é possível afirmar que o tratamento de dados pessoais por sistemas

automatizados de decisão deve ser considerado uma atividade de alto risco e sujeito à elaboração obrigatória do RIPDP.

Da leitura do art. 35 do RGPD europeu constata-se que há uma obrigação da realização do DPIA (transpondo ao cenário nacional, realização do RIPDP) sempre que o processamento de dados possa resultar em alto risco aos direitos e liberdade das pessoas. Ademais, essa avaliação não se limita apenas ao âmbito individual, devendo ser considerado os riscos para a sociedade em geral. Portanto, o próprio texto do RGPD reforça a ideia de entrelaçamento entre as metodologias com análise de fatores de risco (*risk-basead approaches*) e baseadas em direito (*rights based approaches*).

Nessa perspectiva, ainda que os *standards* de avaliação de risco estejam sob estudos pós reuniões técnicas realizadas pela ANPD, da leitura combinada do art. 5º, XVII e do art. 38, parágrafo único, ambos da LGPD, é possível extrair elementos que fazem referência aos testes de balanceamento na avaliação do risco e gerenciamento do risco conforme acepção proposta por Raphael Gellert.

De igual modo, da leitura do art. 50, §2º, inciso I, alínea “d”, da LGPD, é possível constatar que a legislação apresenta diretrizes para a delimitação do risco, consistentes na análise da gravidade e probabilidade do dano, revelando uma abordagem escalável e proporcional em conformidade com as orientações europeias. Nesse sentido, o Guia de Boas Práticas do Comitê Central de Governança de Dados apresenta em seu relatório parâmetros escalares e a matriz probabilidade x impacto, o que também estaria em conformidade com o Guia do RGPD do Reino Unido elaborado pela ICO (autoridade independente do Reino Unido).

Por fim, deve-se observar que a regulamentação envolvendo a avaliação e gerenciamento de risco ainda está em um estágio muito inicial no âmbito nacional, contudo, pode e deve se valer das experiências que estão sendo acumuladas no âmbito europeu há vários anos, tendo a sua disposição várias pesquisas publicizadas no âmbito acadêmico e institucional a respeito do tema. Ademais, a LGPD não endereçou regulamentações envolvendo a inteligência artificial, tema ainda em estágios embrionários no cenário brasileiro.

No âmbito europeu, já existe uma proposta de regulamentação da inteligência artificial que foi apresentada pela Comissão Europeia em abril de 2021. Essa proposta segue a mesma linha do RGPD ao adotar uma abordagem baseada em

risco com obrigações e requisitos legais específicos correspondentes a cada categoria. Os sistemas de alto risco estão sujeitos a diversas restrições, sendo que os requisitos envolvendo sistemas de IA de alto risco foram sintetizados por Ansgar Koene nos seguintes: i) dados de alta qualidade; ii) documentação e rastreabilidade; iii) transparência; iv) supervisão humana; v) precisão e robustez para mitigar os riscos aos direitos fundamentais, e vi) segurança.

Assim, tendo em vista que o tema envolvendo sistemas automatizados de decisão, que utilizem métodos de análise inferencial e criação de perfis, possam ser enquadrados como inteligência artificial em razão do emprego de aprendizado de máquina, as preocupações lançadas pela comunidade europeia em relação ao desenvolvimento de uma IA confiável e auditável devem ser absorvidas pelo legislativo brasileiro de modo a viabilizar a construção de mecanismos de governança que garantam transparência e *accountability* aos sistemas automatizados de decisão.

Por fim, na última seção do quarto capítulo houve a análise da importância da documentação (ou elaboração de relatórios) para a efetivação da *accountability* algorítmica, porquanto tal procedimento é imprescindível para a avaliação e gerenciamento dos riscos e a verificação da conformidade do tratamento de dados com a LGPD. Desse modo, a exigência de relatórios está intimamente associada a mecanismos de corregulação, sendo um trabalho que pode ser desenvolvido em conexão com várias ferramentas de conformidade.

Em um primeiro momento a documentação é essencial para uma governança interna da empresa, tendo conexão com os mecanismos de boas práticas e governança, na qual haveria um mapeamento e identificação dos riscos, com a consequente adequação dos sistemas. Ademais, a ideia de *complicance* e *accountability* exige que os responsáveis pelo desenvolvimento e implementação de sistemas automatizados de decisão elaborem relatórios detalhando como os sistemas foram desenvolvidos e seus processos de implementação.

Nesse sentido, a documentação e a elaboração de relatórios estão relacionadas à própria viabilidade da realização de auditorias pela ANPD, por profissionais terceirizados ou organizações multilaterais, o que reforça a ideia de uma atuação proativa das empresas no intuito de desenvolverem seus sistemas tecnológicos em conformidade com as diretrizes da LGPD. De igual modo, existem outros mecanismos, como a própria certificação, com uso de normas técnicas

ISO/IEC, que representam importantes diretrizes para o estabelecimento de boas práticas e padrões que podem ser operacionalizados pelo setor público e privado, representando-se verdadeiras ferramentas de *compliance* que estariam em consonância com os princípios da prevenção e *accountability*.

A governança de algoritmos na percepção de *compliance* ganha cada vez mais destaque na seara nacional, especialmente considerando que os beneficiários das tecnologias, muitas vezes, não arcam com os custos de seus riscos, os quais atualmente são transferidos para a sociedade e aos governos. Ademais, eclode uma necessidade indispensável de reavaliar a eficácia tradicional dos métodos legais, demandando a estruturação da corregulação como um mecanismo essencial na consolidação de ferramentas de governança voltadas à garantia de transparência e de *accountability* nos sistemas automatizados de decisão.

Diante disso, pode-se afirmar que os programas de *compliance* representam uma estrutura importante na consolidação de mecanismos de governança voltados a orientar os agentes que observem as diretrizes legais. Além disso, diante da importância da corregulação como estrutura de governança, a atuação da ANPD é essencial para implementar e suplementar a LGPD, o que se dará de forma mais eficiente com uma coordenação multissetorial diante da complexidade dos desafios tecnológicos.

Assim, pode-se afirmar que independente de qualquer regulamentação da LGPD pela ANPD já existe uma estrutura normativa de comando e orientação de uma atuação proativa. Essa imposição pode ser extraída do substrato normativo do direito a inferências razoáveis o qual fundamenta uma estrutura de mecanismos que dão suporte a um verdadeiro processo legal na sua acepção substancial, através da consolidação dos quatro pilares desenvolvidos no terceiro capítulo.

O direito a inferências razoáveis pode ser compreendido como um *standard* de comportamento para o controlador de dados, tendo a capacidade para o estabelecimento de mecanismos de governança baseados na *compliance*, que permitam assegurar que o desenvolvimento ou implementação de sistemas automatizados de decisão sejam realizados com a adoção de medidas técnicas e organizacionais apropriados aos riscos envolvidos em suas atividades, viabilizando, o máximo possível, de transparência e *accountability* nessa procedimentalização.

A pretensão do trabalho é reforçar a importância da combinação de estruturas legais com os códigos de prática das empresas, implementando-se uma governança

algorítmica baseada na corregulação, tendo como epicentro valorativo o direito a inferências razoáveis para o desenvolvimento e implementação de sistemas automatizados de decisão.

A implementação de mecanismos de transparência e legibilidade em sistemas automatizados de decisão é necessária para mitigar as externalidades negativas sobre os destinatários desses sistemas. Nesse panorama, tanto a *accountability*, como a transparência, acabam, em última análise, servindo de orientações para o estabelecimento de mecanismos que mitiguem os riscos do uso de sistemas automatizados de decisão, que realizem inferências e criem perfis. Desse modo, a *accountability* representa uma garantia para o desenvolvimento responsável e o uso de sistemas algoritmos em conformidade com os direitos fundamentais.

Para alcançar a autodeterminação informacional e o livre desenvolvimento da personalidade dos indivíduos sujeitos aos sistemas automatizados de decisão, é imprescindível garantir a confiabilidade e auditabilidade dessas tecnologias em harmonia com a estrutura principiológica da LGPD. Portanto, o desenvolvimento de ferramentas de governança algorítmica busca reforçar a responsabilidade dos controladores de dados e a necessidade do desenvolvimento de sistemas automatizados de decisão que viabilizem tornar os dados de saída (*output*) mais inteligíveis à razão humana.

Assim, por meio de uma abordagem dedutiva e com base em referências bibliográficas, o objetivo da presente dissertação foi de propor um direito a inferências razoáveis, extraído da dimensão subjetiva do direito fundamental de proteção de dados, e como substrato normativo de um devido processo legal em sua vertente substancial, tendo como eixo central a consolidação de uma estrutura normativa extraída da LGPD que viabilize a implementação de diversas camadas de transparência durante o desenvolvimento, execução e fiscalização das tecnologias que usem sistemas automatizados de decisão, baseadas em aprendizado de máquina, que empreguem a análise inferencial e a criação de perfis, porquanto nitidamente representam tecnologias de elevado risco.

REFERÊNCIAS

AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. **Máquinas preditivas:** a simples economia da inteligência artificial. Rio de Janeiro: Alta Books, 2019.

ALBERS, Marion. A complexidade da proteção de dados. **Revista Brasileira De Direitos Fundamentais & Justiça**, 10(35), p. 19-45, 2016. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/93. Acesso em: 15 jul. 2020.

ALENCAR, Leandro Zannoni Apolinário. **O novo direito administrativo e governança pública:** responsabilidade, metas e diálogo aplicados à administração pública do Brasil. Belo Horizonte: Fórum, 2018.

ALMEIDA; Virgilio; DONEDA, Danilo; MONTEIRO, Marília. *Governance Challenges for the Internet of Things.* ***IEEE Computer Society*** 1089-7801/15, 2015. Disponível em: https://www.researchgate.net/publication/282493702_Governance_Challenges_for_the_Internet_of_Things/link/5a6de6dba6fdcc317b1906fb/download. Acesso em: 11 nov. 2020.

ALVES, Marco Antônio Sousa. Cidade inteligente e governamentalidade algorítmica: liberdade e controle na era da informação. **Philósophos** - Revista De Filosofia, 23(2), 2019. Disponível em: https://revistas.ufg.br/philosophos/article/view/52730. DOI: https://doi.org/10.5216/phi.v23i2.52730. Acesso em: 23 mar. 2021.

AMOORE, Louise. *Why 'Ditch the algorithm' is the future of political protest.* ***The Guardian***, 19 de Agosto de 2020. Disponível em: https://www.theguardian.com/commentisfree/2020/aug/19/ditch-the-algorithm-generation-students-a-levels-politics. Acesso em: 02 jul. 2021.

ARAS, Vladimir. *Compliance* de proteção de dados no ministério público brasileiro. *In:* SCHNEIDER, Alexandre; ZIESEMER, Henrique da Rosa (Coord.). **Temas atuais de *compliance* e ministério público** – uma nova visão de gestão e atuação institucional. Belo Horizonte: Fórum, 2022.

ARBIX, Daniel. A importância da privacidade por deign e por default (privacy by design and by default). *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord). **Lei geral de proteção de dados (Lei nº 13.709/2018). A caminho da efetividade:** contribuições para implementação da LGPD. São Paulo: Revista dos Tribunais, 2020.

ÁVILA, Humberto. **Teoria dos princípios:** da definição à aplicação dos princípios jurídicos. São Paulo: Malheiros Editores, 2005.

BABUTA, Alexander; OSWALD, Marion. *Data Analytics and Algorithmic: bias in Policing.* ***Royal United Services Institute for Defense and Security Studies***, 2019. Disponível em: https://rusi.org/explore-our-research/projects/data-analytics-and-algorithms-in-policing. Acesso em: 10 fev. 2022.

BAYAMLIOĞLU, Emre. *The right to contest automated decisions under the general data protection regulation: beyond the so-called "right to explanation"*. ***Regulation & Governance***, 14 de março de 2021. Disponível em: https://onlinelibrary.wiley.com/toc/17485991/0/0. DOI: https://doi.org/10.1111/rego.12391, Acesso em: 12 jan. 2021.

BAROCAS, Solon; SELBST, Andrew. Big data's disparate impact. California Law Review 671 (2016). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899. DOI: http://dx.doi.org/10.15779/Z38BG31. Acesso em: 25 set. 2020.

BECKER, Daniel; RODRIGUES, Roberta de Brito. Capítulo III – Direitos do titular. In: FEIGELSON, Bruno; BECKER, Daniel. CAMARAINHA, Sylvia M. F. **Comentários à lei geral de proteção de dados**. São Paulo: Revista dos Tribunais, 2020. Livro Eletrônico.

BEER, David. *The social power of algorithms*. ***Information, Communication & Societ***, 2017, Vol. 20, nº 1, p. 1-13. Disponível em: https://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1216147. Acesso em: 22 abr. 2020.

BELLI, Luca. Como implementar a LGPD por meio de avaliação de impacto sobre privacidade e ética de dados (AIPED). *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.); BIONI, Bruno (Coord. executivo). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

BELLI, Luca; DONEDA, Danilo. O que a regulação da inteligência artificial pode aprender da proteção de dados? **Jota**, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/inteligencia-artificial-protecao-dados-governanca-internet-05112021. Acesso em: 21 jan. 2021.

BENANTI, Paolo. **Oráculos: entre ética e governança dos algoritmos.** Tradução Luisa Rabolini. São Leopoldo: Unisinos, 2020.

BINENBOJM, Gustavo. **Poder de polícia, ordenação, regulação:** transformações político-jurídicas, econômicas e institucionais do direito administrativo ordenador. Belo Horizonte: Fórum, 2020.

BIG BROTHER WATCH. ***Big Brother Watch briefing on Algorithmic Decision-Making in the Criminal Justice System****, January, 2020. Disponível* em: https://bigbrotherwatch.org.uk/wp-content/uploads/2020/02/Big-Brother-Watch-Briefing-on-Algorithmic-Decision-Making-in-the-Criminal-Justice-System-February-2020.pdf. Acesso em: 05 fev. 2022.

BIGONHA, Carolina. Inteligência Artificial em perspectiva. Ano X Nº 2. **Inteligência Artificial e ética.** Panorama Setorial publicado por CGI.BR/NIC.BR, 22 de nov. 2018. Disponível em: https://nic.br/media/docs/publicacoes/1/Panorama_outubro_2018_online.pdf. Acesso em: 26 set. 2019.

BIONI, Bruno; GARROTE, Marina Gonçalves; PASCHOALINI, Nathan; MEIRA, Marina. ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais. **Jota**, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 10 jan. 2022.

BIONI, Bruno Ricardo; RIELLI, Mariana Marques. A construção multissetorial da LGPD: história e aprendizados. *In:* FRANCOSKI; Denise de Souza Luiz; TASSO, Fernando Antônio. **A lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Revista dos Tribunais, 2021.

BIONI, Bruno; MARTINS, Pedro. Devido processo informacional: um salto teórico-dogmático necessário? **Jota**, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/devido-processo-informacional-um-salto-teorico-dogmatico-necessario-15072020. Acesso em: 15 jun. 2021.

BIONI, Bruno; RIELLI, Mariana; VICENTE, João Paulo. Memória da LGPD. **Data Privacy**, 2019. Disponível em: https://www.observatorioprivacidade.com.br/memorias/. Acesso em: 14 jan 2022.

BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento válido como processo: em busca do consentimento válido. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.) BIONI, Bruno (Coord. executivo). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo; LUCIANO, Maria. O Princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? *In:* FRAZÃO, Ana; MULHOLLAND (Coord.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. São Paulo: Revista dos Tribunais, 2018.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Forense: Rio de Janeiro, 2019. Livro digital.

BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei geral de proteção de dados pessoais e suas repercussões no Direito Brasileiro**, 2ª ed. São Paulo: Revista dos Tribunais, 2020.

BLUM, Renato Opice; FURTADO, Tiago Neves. Legítimo interesse: nuances e limites para aplicações práticas no âmbito da LGPD. *In:* FRANCOSKI; Denise de

Souza Luiz; TASSO, Fernando Antônio. **A lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Revista dos Tribunais, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 fev. 2022,

BRASIL. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9203.htm. Acesso em: 10 fev. 2022.

BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm. Acesso: 20 fev. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 05 mai. 2020.

BRASIL. **Supremo Tribunal Federal**. Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal. Relatora Min. Rosa Weber, 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 05 jul. 2020.

BRASIL. **Supremo Tribunal Federal**. Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal. Relatora Min. Rosa Weber. Voto Conjunto do Ministro Gilmar Mendes, 2020. Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf. Acesso em: 05 jul. 2020.

BRUNO, Fernanda. Entrevista: Fernanda Bruno. Vigilância hoje. **Revista Dispositiva**, v. 2, n.1, mai. 2013/out.2013b. Disponível em: http://periodicos.pucminas.br/index.php/dispositiva/article/download/6091/5680. Acesso em: 05 mai 2021.

BRUNO, Fernanda. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade**. Porto Alegre: Sulina, 2013.

BRUNO, Fernanda. Tecnopolítica, racionalidade algorítmica e mundo como laboratório. **Instituto Humanitas Unisinos:** entrevista com Fernanda Bruno, 02 de novembro de 2019. Disponível em: http://www.ihu.unisinos.br/78-noticias/594012-tecnopolitica-racionalidade-algoritmica-e-mundo-como-laboratorio-entrevista-com-fernanda-bruno. Acesso em: 19 mai 2021.

BUCAR, Daniel; VIOL, Mario. Tratamento de dados pessoais por “legítimo interesse do controlador”: primeiras questões e apontamentos. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro, 2ª edição**. São Paulo: Revista dos Tribunais, 2020.

BURDICK, Alan. *The A.I, “gaydar” study and the real dangers of big data. **The New Yorker**, September*, 15, 2017. Disponível em: https://www.newyorker.com/news/daily-comment/the-ai-gaydar-study-and-the-real-dangers-of-big-data. Acesso em: 02 jan. 2022.

BURREL, Jenna. *How the machine ‘thinks’: Understanding opacity in machine learning algorithms*. ***Big Data & Society***, January–June 2016: 1–12. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512. Acesso em: 25 mai 2020.

CANABARRO, Diego Rafael; WAGNER, Flávio Rech. A Governança da Internet: definição, desafios e perspectivas. **Trabalho apresentado no 9º Encontro do ABCP XX a XX/07/2014, Brasília/DF**. Disponível em: https://cienciapolitica.org.br/system/files/documentos/eventos/2017/04/governanca-internet-mudanca-tecnologica-redistribuicao-poder.pdf. Acesso em: 05 jul. 2019.

CARUANA, Rich; LOU, Yuin; GEHRKE, Johannes, KOCH, Paul; STURM, Marc; ELHADA, Noémie. *Intelligile models for healthcare: predicting pneumonia risck and hospital 30-day readmission.* **KDD '15:** Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 2015 Pages 1721–1730. Disponível em: https://dl.acm.org/doi/10.1145/2783258.2788613. Acesso em 20 abr. 2020.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.) BIONI, Bruno (Coord. executivo). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

CASSINO, João Francisco. Modulação deleuziana, modulação algorítmica e manipulação midiática. SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu da (ORG.). **A sociedade de controle:** manipulação e modulação nas redes digitais. São Paulo: Hedra, 2018.

CITRON, Danielle, PASQUALE, Frank. *The Scored Society: Due Process for Automated Predictions. **Washington Law Review***, Vol. 89, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 20 mai 2020.

CORTIZ, Diogo. **Inteligência artificial: equidade, justiça e consequências.** Panorama setorial da Internet, número 1, maio, 2020, ano 12. Disponível em: https://www.cetic.br/media/docs/publicacoes/6/20200626161010/panorama_setorial_ano-xii_n_1_inteligencia_artificial_equidade_justi%C3%A7a.pdf. Acesso em: 05 mai 2021.

CRESPO, Marcelo. Desafios de efetivação da LGPD: comentários sobre a fiscalização e a prestação de contas. *In:* FRANCOSKI; Denise de Souza Luiz; TASSO, Fernando Antônio. **A lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Revista dos Tribunais, 2021.

CUMMINGS, Mary. *Automation bias in intelligente time critical decision support sustems*. ***Collection of Technical Papers Aiaa 1st Intelligent Systems Technical Conference***, Vol. 2, p. 557-562, 01 de dezembro de 2004. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.91.2634. Acesso em: 05 abr. 2021.

DANAHER, John; HOGAN, Michael J; NOONE. *Algorithmic governance: Developing a research agenda through the power of collective intelligence.* ***Big Data & Society***, 01 dez. 2017. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951717726554. Acesso em: 20 jun. 2020.

DASTIN, Jeffrey. *Amazon scraps secret AI recruiting tool that showed bias against women*. ***The Reuters***, 10 de outubro de 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. Acesso em: 05 abr. 2020.

DELEUZE, Gilles. **Conversações (1972-1990)**. Tradução de Peter Pál Pelbart. São Paulo: Editora 34, 2013.

DELEUZE, Gilles. O ato de criação. **Retranscrição da conferência filmada, pronunciada na FEMIS** (Fondation Européenne pour les Métiers de l'Image et du Son) no dia 17 de março de 1987, a convite de Jean Narboni e transmitida por FR3/Océaniques no dia 18 de maio de 1989. Disponível em: https://laboratoriodesensibilidades.wordpress.com/2017/11/16/o-que-e-o-ato-de-criacao-gilles-deleuze-abaixo-transcricao-em-portugues-da-filmagem-de-1987/. Acesso em: 25 mai 2021.

DELUA, Julianna. *Supervised vs. Unsupervised Learning: What's the Difference?* ***IBM Analytics, Data Science/Machine Learning***, 12 march 2021. Disponível em: https://www.ibm.com/cloud/blog/supervised-vs-unsupervised-learning. Acesso em: 17 jan. 2022.

DEUTSCHLAND. ***Grundgesetz für die Bundesrepublik Deutschland****. Verkündet am 23. Mai 1949*. Disponível em: https://www.gesetze-im-internet.de/gg/BJNR000010949.html. Acesso em: 14 fev. 2022.

DIAKOPOULOS, Nicholas. *Algorithmic accountability: on the investigation of black boxes*. ***Tow Center for Digital Journalism Publications***, 10 de junho de 2017. Não paginado. Disponível em: https://www.cjr.org/tow_center_reports/algorithmic_accountability_on_the_investigation_of_black_boxes.php#citations. Acesso em: 15 abr. 2020.

DIDER JR, Fredie; ZANETI JR, Hermes. **Curso de direito processual civil:** processo coletivo. Salvador: JusPodvim, 2019.

DOMINGOS, Pedro. **O algoritmo mestre**. São Paulo: Novatec Editora, 2015. [Edição do Kindle].

DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei geral de proteção de dados** (Lei nº 13.709/2018). São Paulo: Revista dos Tribunais, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Revista dos Tribunais, 2019. [Livro eletrônico]

DONEDA, Danilo; ALMEIDA, Virgílio. O que é governança de algoritmos? **Instituto Nupef**, 2016**.** Disponível em: https://politics.org.br/edicoes/o-que-%C3%A9-governan%C3%A7a-de-algoritmos. Acesso em: 10 abr. 2020.

DONEDA, Danilo. Proteção de dados pessoais: contornos da formação de um novo direito. *In:* FRANCOSKI; Denise de Souza Luiz; TASSO, Fernando Antônio. **A lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Revista dos Tribunais, 2021.

EDWARDS, Lilian; VEALE, Michael*. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking **For***. **Duke Law & Technology Review** 18, 2017. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855. DOI: http://dx.doi.org/10.2139/ssrn.2972855. Acesso em: 25 mai 2020.

EUROPEAN COMMISSION. *Article 29 Data Protection Working Party. Advice paper on special categories of data ("sensitive data"), 2011. Disponível em: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. Acesso em: 10 fev. 2022.*

EUROPEAN COMMISSION. *Article 29 Data Protection Working Party. **Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679**, 17/EN, WP251rev.01, Oct. 2017*. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 20 mai 2021.

EUROPEAN COMMISSION. *Article 29 Data Protection Working Party*. ***Guidelines on the Right to Data Portability***, 16/EN, WP242rev.01, Dec. 13, 2016. Disponível em: https://ec.europa.eu/newsroom/article29/items/611233/en. Acesso em: 20 jun. 2021.

*EUROPEAN COMMISSION. Article 29 Data Protection Working Party. **Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation***

2016/679. 17/PT, WP 248 rev.01, April 4, 2017b. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 20 jan. 2022.

EUROPEAN COMMISSION. Article 29 Data Protection Working Party. ***Guidelines on transparency under Regulation 2016/679****. 17/EN, WP260 rev.01, 2017c. Disponível em: https://ec.europa.eu/newsroom/article29/items/622227. Acesso em: 20 dez. 2021.*

EUROPEAN COMMISSION. Article 29 Data Protection Working Party. ***Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC****, 844/14/EN, WP 217, 9 April 2014.* Disponível em: https://www.dataprotection.ro/servlet/ViewDocument?id=1086. Acesso em: 05 dez. 2021,

EUROPEAN COMMISSION. *Article 29 Data Protection Working Party*. ***Statement on the role of a risk-based approach in data protection legal Frameworks***. 14/EN, WP 218, 30 May 2014b. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf. Acesso em: 25 jan. 2022.

EUROPEAN COMISSION. The European Commissions's High-Level Expert Group on Artificial Intelligence, ***Ethic Guidelines For Trustworthy AI***, 2019. Disponível em: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai Acesso em: 28 set. 2019.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de direito civil:** parte geral e LINDB. Salvador: JusPodvim, 2017.

FERRARI, Isabela. *Accountability* de algoritmos: a falácia do acesso ao código e caminhos para uma explicabilidade efetiva. **ITS Rio**, 2018, 3º Grupo de Pesquisa. Disponível em: https://itsrio.org/pt/publicacoes/inteligencia-artificial-gp3/. Acesso em: 10 jul. 2020.

FERRARI, Isabela; BECKER, Daniel. *Ad astra per aspera*: postergação da LGPD e revisitação do art. 20, § 1º. **Jota**, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/ad-astra-per-aspera-postergacao-da-lgpd-e-revisitacao-do-art-20-%C2%A7-1o-09052020. Acesso em 02 jun. 2020.

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. ***Arbitrium ex machina***: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. Revista dos Tribunais. Vol 995/2018. Set/2018. Disponível em: https://www.academia.edu/38199022/ARBITRIUM_EX_MACHINA_PANORAMA_RISCOS_E_A_NECESSIDADE.pdf. Acesso em: 25 mai 2020.

FJELD, Jessica; ACHTEN, Nele; HILLIGOSS, Hannah; NAGY, Adam Christophoer; SRIKUMAR, Madhulika. *Principled artificial intelligence: mapping consensus in ethical and rights-based approaches to principles for AI****. Berkman Klein center for internet & society***, 2020. Disponível em: https://dash.harvard.edu/handle/1/42160420. Acesso em 10 fev. 2022.

FLORIDI, Luciano; PAGALLO, Ugo; COWLS, Josh; BELTRAMETTI, Monica; CHATILA, Raja; CHAZERAND, Patrice; DIGNUM, Virginia; LUETGE, Christoph, MADELIN, Robert; ROSSI, Francesca; SCHAFER, Burkhard; VALCKE, Peggy; VAYENA, Effy. *AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations.* ***Minds & Machines*** 28, 689–707, 2018. Disponível em: https://link.springer.com/article/10.1007/s11023-018-9482-5. Acesso em: 10 jun. 2020.

FLORIDI, Luciano; COWLS, Josh. *A unified framework of five principles for AI in society.* ***Harvard Data Science Review***, 1(1), 01 de julho de 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3831321. DOI: https://doi.org/10.1162/99608f92.8cd550d1. Acesso em: 15 jan. 2022.

FLORIDI, Luciano. *Soft ethics, the governance of the digital and the General Data Protection Regulation*. ***Royal Society***, 15 de outubro de 2018. Disponível em: https://royalsocietypublishing.org/doi/full/10.1098/rsta.2018.0081. DOI: https://doi.org/10.1098/rsta.2018.0081. Acesso em: 10 jun. 2021.

FLORIDI, Luciano; TADDEO, Mariarosaria. *What is data ethics*? Philosophical **Transactions of The Royal Society A Mathematical Physical and Engineering Sciences** December 2016. Disponível em: https://royalsocietypublishing.org/doi/10.1098/rsta.2016.0360. Acesso em: 05 mar. 2020.

FOUCAULT, Michel. **Vigiar e punir:** nascimento da prisão. Tradução de Raquel Ramalhete. Petrópolis, Vozes, 1999.

FRAJHOF, Isabella; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. *In*: MOLHOLLAND, Caitlin**. A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélogo, 2020.

FRAJHOF, Isabella Z. O papel dos mecanismos de *compliance* para a operacionalização do direito à explicação de decisões totalmente automatizadas. *In*: FRAZÃO, Ana, CUEVA, Ricardo Villas Bôas (Coord.). ***Compliance*** **e políticas de proteção de dados**. São Paulo: Revista dos Tribunais, 2022.

FRAZÃO, Ana. Big data, Plataformas digitais e principais impactos sobre o direito da concorrência. *In:* FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de (Coord.). **Empresa, mercado e tecnologia**. Belo Horizonte: Fórum, 2019.

FRAZÃO, Ana. MEDEIROS, Rafaela Martinez. Desafios para a efetividade dos programas de *compliance*. *In:* FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de (Coord.). **Empresa, mercado e tecnologia**. Belo Horizonte: Fórum, 2019.

FRAZÃO, Ana. Controvérsias sobre direito à explicação e à oposição diante de decisões automatizadas. **Jota**, 2018. Disponível em: https://www.jota.info/?pagename=paywall&redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/controversias-sobre-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-automatizadas-12122018. Acesso em: 10 jun. 2020.

FRAZÃO, Ana. Decisões algorítmicas e direito à explicação. **Jota**, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/decisoes-algoritmicas-e-direito-a-explicacao-24112021. Acesso em: 24 jan. 2022.

FRAZÃO, Ana. Discriminação algorítmica: por que algoritmos preocupam quando acertam e erram? **Jota**, 2021b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-por-que-algoritmos-preocupam-quando-acertam-e-erram-04082021. Acesso em: 10 jan. 2022.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – noções introdutórias para a compreensão da importância da lei geral de proteção de dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro, 2ª edição**. São Paulo: Revista dos Tribunais, 2020.

FRAZÃO, Ana. Nova LGPD: ainda sobre a eficácia do direito à explicação e à oposição. **Jota**, 2018b. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-ainda-sobre-a-eficacia-do-direito-a-explicacao-e-a-oposicao-26122018. Acesso em 10 jun. 2020.

FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de compliance e das políticas de proteção de dados. *In*: FRAZÃO, Ana, CUEVA, Ricardo Villas Bôas (Coord.). ***Compliance* e políticas de proteção de dados**. São Paulo: Livraria Revista dos Tribunais, 2022.

FRAZÃO, Ana. Objetivos e alcance da lei geral de proteção de dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019b.

FRAZÃO, Ana. O direito à explicação e à oposição diante de decisões totalmente automatizadas. **Jota**, 2018c. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018. Acesso em: 05 jun. 2020.

FRAZÃO, Ana. Transparência de algoritmos x segredo de empresa. **Jota**, 2021b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/transparencia-de-algoritmos-x-segredo-de-empresa-09062021. Acesso em: 20 fev. 2022.

FRIEDMAN, Batya; NISSENBAUM, Helen. *Bias in Computer Systems.* **ACM Transactions on Information Systems**, Vol. 14, Nº. 3, July 1996, p. 330-347. Disponível em: https://nissenbaum.tech.cornell.edu/papers/Bias%20in%20Computer%20Systems.pdf. Acesso em: 27 jun. 2021.

GADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. ***The Guardian***, 17 de mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 05 de mar. 2021.

GALIMBERTI, Umberto. O ser humano na idade da técnica. **Cadernos IHUideias**, Ano 13, nº 218, vol. 13, 2015. Disponível em: http://www.ihu.unisinos.br/noticias/540793-o-ser-humano-na-idade-da-tecnica. Acesso em: 25 jul. 2020.

GALIMBERTI, Umberto. Psiché y Techné. **Artefato/4**, 2001. Disponível em: https://sociotecnica.files.wordpress.com/2013/09/psichc3a9-y-technc3a9-de-umberto-galimberti.pdf. Acesso em: 05 jan. 2021.

GELLERT, Raphäel. ***We have always managed risks in data protection law****: understanding the similarities and differences between the rights-based and the risk-based approaches to data protection. 2 Eur. Data Prot. L. Rev*. 481 (2016). Disponível em: Heinonline. Acesso em 10 jan. 2022.

GOLDSCHMIDT, Ronaldo Ribeiro. **Uma Introdução à Inteligência Computacional**: fundamentos, ferramentas e aplicações. Rio de Janeiro: IST-Rio, 2010, p. 08.

GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. *In:* LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes (Coord.). **Direito digital:** debates contemporâneos. São Paulo: Thomson Reuters Brasil, 2019, pp 141-153

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In: PALHARES, Felipe (Coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters, 2020.

GUERRA, Sérgio. **Agências reguladoras:** da organização administrativa piramidal à governança em rede. Belo Horizonte: Fórum, 2020.

GUSZCZA, James; LEE, Michelle; AMMANATH, Beena; KUDER, Dave. *Human values in the loop: design principles for ethical AI.* ***Deloitte Review****: Technology and ethics, Issue, January*, 2020. Disponível em: https://www2.deloitte.com/content/dam/insights/us/articles/6452_human-values-in-the-loop/DI_DR26-Human-values-in-the-loop.pdf. Acesso em 10 jan. 2022.

HAN, Byung-Chul. Psicopolítica: o neoliberalismo e as novas técnicas de poder. Belo Horizonte: Âyiné, 2020.

HARDT, Michael; NEGRI, Antônio. **Império**. Tradução de Berilo Vargas, 8ª ed. Rio de Janeiro: Record, 2006.

HILDEBRANDT, Mireille. *Defining profiling. A new type of knowledge. In:* HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling the European Citizen: Cross-Disciplinary Perspectives****, pp. 17-44*. Londres: Springer, 2008. Disponível em: https://www.researchgate.net/publication/226744267_Defining_Profiling_A_New_Type_of_Knowledge. Acesso em: 05 abr. 2021.

HILDEBRANDT, Mireille*. Privacy As Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning.* ***Forthcoming in Theoretical Inquiries of Law***, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081776. DOI: http://dx.doi.org/10.2139/ssrn.3081776. Acesso em: 05 jan. 2021.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital:** transformação digital desafios para o direito. Rio de Janeiro: Forense, 2021.

HOSNI, David Salim Santos; MARTINS, Pedro Bastos Lobo. Tomada de decisão automatizada e a regulamentação da proteção de dados: alternativas coletivas oferecidas pela lei geral de proteção de dados. **Internet&Sociedade**, v.1/n.2/dezembro de 2020, páginas 77 a 101. Disponível em: https://revista.internetlab.org.br/736-2/. Acesso em: 14 fev. 2022.

HUR, Domenico Uhng. Da biopolítica à noopolítica: contribuições de Deleuze. **Lugar comum. nº 40**, p. 201-215, 2013. Disponível em: https://www.researchgate.net/publication/321173904_Da_biopolitica_a_noopolitica_contribuicoes_de_Deleuze. Acesso em: 25 mai 2021.

JIMENE, Camilla do Vale; ZANI, Filipe Hamilton. Frameworks de proteção de dados pessoais e segurança da informação úteis para os setores público e privado. *In:* FRANCOSKI; Denise de Souza Luiz; TASSO, Fernando Antônio. **A lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Revista dos Tribunais, 2021.

INFORMATION COMMISSIONER'S OFFICE (ICO). ***Guide to the General Data Protection Regulation (GDPR)****, 01 January*, 2021. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/. Acesso em: 10 jan. 2022.

INFORMATION COMMISSIONER'S OFFICE (ICO). ***How do we do a DPIA?*** 2021b. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/. Acesso em: 10 fev. 2022.

KAMINSKI, Margot E. *The right to explanation, explained.* ***U of Colorado Law Legal Studies Research*** *Paper nº. 18-24, 19 jun 2018*. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985. Acesso em: 05 jan. 2022.

KAUFMAN, Dora. **A inteligência artificial irá suplantar a inteligência humana?** Barueri: Estão das Letras e Cores, 2019.

KAUFMAN, Dora. Inteligência Artificial e os desafios éticos: a restrita aplicabilidade dos princípios gerais para nortear o ecossistema de IA. **PAULUS**: Revista de Comunicação da FAPCOM, São Paulo, v. 5, n. 9, p. 73-84, jan./jul. 2021.

KELLER, Clara Iglesias. **Regulação nacional de serviços na internet:** exceção, legitimidade e o papel do Estado. Rio de janeiro: Lumen Juris, 2019.

KITCHIN, Rob. *Thinking critically about and researching algorithm*s. ***Information, Communication & Societ***, 2017, Vol. 20, nº 1, p. 14-29. Disponível em: http://futuredata.stanford.edu/classes/cs345s/handouts/kitchin.pdf. Acesso em: 15 mai. 2020.

KOENE, Ansgar; CLIFTON, Chris; HATADA, Yohko; WEBB, Helena, PATEL, Menisha, MACHADO, Caio; LAVIOLETTE, Jack; RICHARDSON, Raschida; REISMAN, Dillon. *A governance framework for algorithmic accountability and transparency. **European Parliamentary Research Service***, abr. 2019*. Disponível em:* https://op.europa.eu/en/publication-detail/-/publication/8ed84cfe-8e62-11e9-9369-01aa75ed71a1/language-en/format-PDF/source-120507593. Acesso em: 15 jul. 2020.

KOENE, Ansgar. *A survey of artificial intelligence risk assessment methodologies: the global state of play and leading practices identified. **Trilateral Research***, 2022. Disponível em: https://www.trilateralresearch.com/wp-content/uploads/2022/01/A-survey-of-AI-Risk-Assessment-Methodologies-full-report.pdf. Acesso em: 05 de jan. 2022.

KROLL, Joshua A. *The fallacy of inscrutability*. ***Philosophical transactions of the royal society***, 2018. Disponível em: https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0084. Acesso em: 28 mai 2020

KURBALIJA, Jovan. **Uma introdução à governança da Internet.** São Paulo: Comitê Gestor da Internet no Brasil, 2016. Disponível em: https://cgi.br/media/docs/publicacoes/1/CadernoCGIbr_Uma_Introducao_a_Governanca_da_Internet.pdf. Acesso em: 10 out. 2019.

LAMONT, Tom. *The student and the algorithm: how the exam results fiasco threatened one pupil's future. **The Guardian***, 18 de fevereiro de 2021. Disponível em: https://www.theguardian.com/education/2021/feb/18/the-student-and-the-algorithm-how-the-exam-results-fiasco-threatened-one-pupils-future. Acesso em: 02 jul. 2021.

LAPOUJADE, David. **Deleuze, os movimentos aberrantes**. São Paulo: n-1 edições, 2015.

LATZER, Michael; JUST, Natascha. *Governance by and of algorithms on the internet: impact and consequence*s. ***Oxford University Press USA***, fevereiro de

2020. Disponível em: https://www.researchgate.net/publication/339675115_Governance_by_and_of_algorithms_on_the_internet_impact_and_consequences. DOI: 10.1093/acrefore/9780190228613.013.904. Acesso em: 18 abr. 2020.

LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren; ANGWIN, Julia. *How We Analyzed the COMPAS Recidivism Algorithm***. ProPublica,** 23 de maio de 2016. Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. Acesso em: 10 jun. 2021.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2012.

LEWIS, Paul. *I was shocked it was so easy': meet the professor who says facial recognition can tell if you're gay. **The Guardian**,* 07 jul. 2018. Disponível em: https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis. Acesso em: 25 set. 2019.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e efetividade da lei geral de proteção de dados:** de acordo com a lei geral de proteção de dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.583/2019), o marco civil da internet (Lei n. 12.965/2014) e as sugestões de alteração do CPC (PL 3.514/2015). São Paulo: Almedina, 2020.

LIMA, Taisa Maria Macena de; DE SÁ, Maria de Fátima Freire. Inteligência artificial e lei geral de proteção de dados pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil – RBDCivil** – Belo Horizonte, v. 26, p. 227-246, out./dez. 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584. Acesso em: 10 dez. 2021.

LINDOSO, Maria Cristine Branco. **Discriminação de gênero no tratamento automatizado de dados pessoais:** como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021.

LINDOSO, Maria Cristine. O uso do *compliance* e das políticas de proteção de dados como formas de coibir a discriminação algorítmica: como essas ferramentas podem resguardar as empresas, proteger os usuários e ainda ajudar na diminuição da discriminação de minorias. *In*: FRAZÃO, Ana, CUEVA, Ricardo Villas Bôas (Coord.). ***Compliance* e políticas de proteção de dados**. São Paulo: Revista dos Tribunais, 2022.

LÓPEZ, Núria. Decisões automatizadas: o futuro regulatório de inteligência artificial. *In:* FRANCOSKI; Denise de Souza Luiz; TASSO, Fernando Antônio. **A lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Revista dos Tribunais, 2021.

LUDWING, 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**, v. 19, Março/2001. Disponível em: https://seer.ufrgs.br/revfacdir/article/view/71531/40592. Acesso em: 14 fev. 2022.

MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélago Editoral Ltda, 2019.

MAGRANI, Eduardo. *Governance of internet of things and ethics of artificial intelligence*. **Revista Direitos Culturais.** Santo Ângelo, v. 13, n. 31, p. 153-190, set./dez. 2018. Disponível em: http://eduardomagrani.com/governance-of-internet-of-things-and-ethics-of-artificial-intelligence/. Acesso em: 10 abr. 2020.

MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de; CAMPELLO, Tatiana. Guia de boas práticas em inteligência artificial. **DEMAREST**, novembro 2021. Disponível em: https://www.demarest.com.br/lancamento-guia-de-boas-praticas-em-inteligencia-artificial/. Acesso em: 20 jan. 2022.

MAGRANI, Eduardo. Hackeando o eleitorado: sobre o uso de dados pessoais em campanhas eleitorais. **Berlim: Konrad-Adenauer-Stifung**, 2020. Disponível em: https://www.kas.de/documents/252038/7995358/Hackeando+o+Eleitorado+-+Sobre+o+uso+de+dados+pessoais+em+campanhas+eleitorais.pdf/e99e38c1-dbfc-66db-ec14-aac88b4316ff. Acesso em: 15 jan. 2021.

MAGRANI, Eduardo; GUEDES, Paula. Inteligência artificial: desafios éticos e jurídicos. *In*: FRAZÃO, Ana, CUEVA, Ricardo Villas Bôas (Coord.). ***Compliance* e políticas de proteção de dados**. São Paulo: Revista dos Tribunais, 2022.

MALGIERI, Gianclaudio; COMANDÉ, Giovanni. *Why a right to legibility of automated decision-making exists in the general data protection regulation*. ***International Data Privacy Law***, 2017, Vol. 7, nº. 4. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3088976. Acesso em: 10 jan. 2022.

MARCHANT, Gary. *The growing gap between emerging technologies and the law. Published as Chapter* 2, pp. 19-32. *In*: MARCHANT, Gary; ALLENBY, Braden; HERKERT, Joseph (Eds.). ***The growing gap between emerging technologies and legal ethical oversight: the pacing problem***. Dordrecht, Germany: Springer, 2011. Disponível em: https://www.researchgate.net/publication/226523376_The_Growing_Gap_Between_Emerging_Technologies_and_the_Law. Acesso em: 02 jun. 2021.

MATTIUZZO, Marcela. Discriminação algorítmica: reflexões no contexto da lei geral de proteção de dados pessoais. *In:* DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). **Lei geral de proteção de dados (Lei nº 13709/2018):** a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters, 2020.

MATTIUZZO, Marcela. *"Let the algorithm decide": is human dignity at stake?* **Revista Brasileira de Políticas Públicas**, Brasília, v. 11, n. 1. p. 342-369, 2021. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/6784. DOI: https://doi.org/10.5102/rbpp.v11i1.6784. Acesso em: 25 jun. 2021.

MAYNTZ, Renate. *From government to governance: political steering in modern societies.* ***Summer Academy on IPP:*** *Wuerzburg, September* 7-11, 2003.

Disponível em: https://www.ioew.de/fileadmin/user_upload/DOKUMENTE/Veranstaltungen/2003/SuA2Mayntz.pdf. Acesso em: 05 out. 2020.

MCCARTHY, John. What is artificial intelligence? Computer Science Departmente, Stanfor University, 12 de novembro de 2007. Disponível em: http://jmc.stanford.edu/articles/whatisai.html. Acesso em: 24 set. 2019.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. 2ª ed. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. A lei geral de proteção de dados pessoais: um modelo de aplicação em três níveis. **Caderno Especial LGPD**, p. 35-56. São Paulo: Revista dos Tribunais, 2019.

MENDES, Laura Schertel. Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord). **Lei geral de proteção de dados (Lei nº 13.709/2018). A caminho da efetividade:** contribuições para implementação da LGPD. São Paulo: Revista dos Tribunais, 2020b.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **Jota**, 2020. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 10 jun. 2020.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da lei geral de proteção de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.); BIONI, Bruno (Coord. executivo). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez/ 2018. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 15 nov. 2021.

MENDES, Laura Schertel; JÚNIOR, Otavio Luiz Rodrigues; FONSECA, Gabriel Campos Soares. O supremo tribunal federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.) BIONI, Bruno (Coord. executivo). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. [Livro eletrônico].

MEJIAS, Ulises; COULDRY, Nick. *Datafication**. Internet Policy Review***, 29 nov 2019. Disponível em: https://policyreview.info/concepts/datafication. DOI: 10.14763/2019.4.1428. Acesso em: 27 abri. 2020.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfagang; COELHO, Alexandre Zavaglia P. (Coord.). **Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2014. Livro eletrônico.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. *The ethics of algorithms: Mapping the debate*. ***Big Data & Society***, July-December, 2016: 1–21. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951716679679. Acesso em: 22 abr. 2020.

MODENESI, Pedro. *Privacy by design* e código digital: a tecnologia a favor de direitos e valores fundamentais. In: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (Coord.). **Proteção de dados pessoais na sociedade da informação: entre dados e danos**. Indaiatuba: Foco, 2021.

MOKANDER, Jacob; FLORIDI, Luciano. *Ethics – Based Auditing to Develop Trustworthy AI.* ***Minds and Machines*** (2021) 31:323–327. Disponível em: https://link.springer.com/article/10.1007%2Fs11023-021-09557-8. DOI: https://doi.org/10.1007/s11023-021-09557-8. Acesso em: 05 fev. 2022.

MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Apontamentos sobre direito, ciência e tecnologia na perspectiva de políticas públicas sobre regulação em ciência e tecnologia. In: MENDES, Gilmar Mendes; SARLET, Ingo Wolfang, e; COELHO, Alexandre Zavaglia P. (Coord.). **Direito, tecnologia e inovação**. São Paulo: Saraiva, 2015. Livro eletrônico.

MONTEIRO, Renato Leite. CRUZ, Sinuhe. Direitos dos titulares: fundamentos, limites e aspectos práticos. *In:* FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (Coord.). **A lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo, Revista dos Tribunais, 2021.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**, dez/2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 26 set. 2019.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. **Jota**, 2018a. Disponível em: https://www.jota.info/opiniao-e-analise/ colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 10 jan. 2022.

MONTEIRO FILHO, Carlos Edison do Rêgo; ROSENVALD, Nelson. Riscos e responsabilidades na inteligência artificial e noutras tecnologias digitais emergentes. *In:* TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coord.). **O direito civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020. [versão eletrônica]

MORASSUTTI, Bruno Schimitt. **Regulação de tecnologias e arquitetura de sistemas:** um estudo sobre o *privacy by design* e a transparência aplicada a algoritmos computacionais. Orientador: Juarez Freitas. 2019. 182 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, PUC, RS, Porto Alegre, 2019.

MOROZOV, Evgeny. *The rise of data and the death of politics.* ***The Guardian***, 20 de julho de 2014. Disponível em: https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation. Acesso em: 04 abri. 2021.

MULHOLLAND, Caitlin. GOMES, Rodrigo Dias de Pinho. Inteligência artificial e seus principais desafios para os programas de *compliance* e as políticas de proteção de dados. *In*: FRAZÃO, Ana, CUEVA, Ricardo Villas Bôas (Coord.). ***Compliance*** **e políticas de proteção de dados**. São Paulo: Livraria Revista dos Tribunais, 2022.

MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

NETO, Cláudio Pereira de Souza; SARMENTO, Daniel. **Direito Constitucional:** teoria, história e métodos de trabalho. Belo Horizonte: Fórum, 2016.

NISSENBAUM, Helen. *Accountability in a computerized society.* ***Science and Engineering Ethics*** *(1996) 2, 25-42.* Disponível em: https://nissenbaum.tech.cornell.edu/papers/AccountabilityinaComputerizedSociety.pdf. DOI: https://doi.org/10.1007/BF02639315. Acesso em: 15 fev. 2022.

O'NEIL, Cathy. **Algoritmos de destruição em massa:** como a big data aumenta a desigualdade e ameaça a democracia. Tradução Rafael Abraham. Santo André: Rua do Sabão, 2020.

PAGALLO, Ugo; CASANOVAS, Pompeu; MADELIN, Robert. *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data.* ***The Theory and Practice of Legislation***, 7:1, 1-25, 2019. Disponível em: https://doi.org/10.1080/20508840.2019.1664543. Acesso em: 08 out. 2020.

PALMEIRA, Mariana de Moraes. A segurança e as boas práticas no tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

PASQUALE, Frank. *The Automated Public Sphere*. ***Brooklyn Law School***, 10 de novembro de 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067552. Acesso em: 15 fev. 2021.

PÉREZ LUÑO, Antonio-Enrique. *Internet y los derechos humanos*. *In:* **Anuario de Derechos Humanos**. Nueva Época. Vol. 12. 2011, pp. 288-289. Disponível em: https://revistas.ucm.es/index.php/ANDH/article/view/38107/36859. Acesso em: 02 jun. 2020.

PIERRO, Bruno de. O mundo mediado por algoritmos: sistemas lógicos que sustentam os programas de computador têm impacto crescente no cotidiano. **Pesquisa FAPESP**, Edição 266, abr. 2018, pp. 18-25. Disponível em: https://revistapesquisa.fapesp.br/o-mundo-mediado-por-algoritmos/. Acesso em: 10 abr. 2020.

POLIDO, Fabrício Bertini Pasquot. Novas perspectivas para regulação da inteligência artificial: diálogos entre as políticas domésticas e os processos legais transnacionais. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito:** ética, regulação e responsabilidade. São Paulo, Revista dos Tribunais, 2020.

QUELLE, Claudia. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability – and Risk-based Approach. **European Journal of Risk Regulation**, 9(3), 2018, p. 502-526.

RAGAZZO, Carlos Emmanuel Joppert. **Regulação jurídica, racionalidade econômica e saneamento básico**. Rio de Janeiro: Renovar, 2011.

RODAS, Sérgio. Constitucionalização da proteção de dados é marco e aumenta segurança jurídica. **Consultor jurídico**, 11 de fevereiro de 2022. Disponível em: https://www.conjur.com.br/2022-fev-11/constitucionalizacao-protecao-dados-marco-aumenta-seguranca. Acesso em: 14 fev. 2022.

RODOTÀ, Stefano**. A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. *Accountability* e mitigação da responsabilidade civil na lei geral de proteção de dados pessoais. *In*: FRAZÃO, Ana, CUEVA, Ricardo Villas Bôas (Coord.). ***Compliance* e políticas de proteção de dados**. São Paulo: Livraria Revista dos Tribunais, 2022.

ROUVROY, Antoinette. Entrevista com Antoinette Rouvroy: Governamentalidade Algorítmica e a Morte da Política. **Revista de Filosofia Moderna e Contemporânea**, Brasília, v.8, n.3, dez. 2020, p. 15-28. ISSN: 2317-9570. Disponível em: https://periodicos.unb.br/index.php/fmc/article/view/36223. DOI: https://doi.org/10.26512/rfmc.v8i3.36223. Acesso em: 20 mai. 2021.

ROUVROY, Antoinette; BERNS, Thomas. Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? **Revista Eco Pós.** Tecnopolíticas e vigilância, v. 18, n. 2, 2015. ISSN 2175-8689. Disponível em: https://revistaecopos.eco.ufrj.br/eco_pos/article/view/2662. DOI: https://doi.org/10.29146/eco-pos.v18i2.2662. Acesso em: 22 mai. 2021.

ROUVROY, Antoinette. *"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data. **Council of Europe**, Strasbourg*, 11 *janauary* 2016. Disponível em: https://www.semanticscholar.org/paper/%22Of-Data-and-Men%22.-Fundamental-Rights-and-Freedoms-Rouvroy/13830dd9e5e6d78603e06965ef69932bd2e82e6c#related-papers. Acesso em: 10 fev. 2022.

RUARO, Regina Linden (2015). Privacidade e autodeterminação informativa obstáculos ao estado de vigilância? **Arquivo Jurídico**. V. 2, nº 1, p. 41-60, jan./jun. de 2015. Disponível em: https://revistas.ufpi.br/index.php/raj/article/view/4505/2647. Acesso em: 25 mai. 2020.

SAAVEDRA,Giovani Agostini. Compliance de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.); BIONI, Bruno (Coord. executivo). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

SADIN, Éric. ***Critica della ragione artificiale:** Una difesa dell'umanità*. Roma: LUISS University Press, 2019.

SADOWSKI, Jathan. *When data is capital: datafication, accumulation, and extraction. **Big Data & Society**, January-June*, 2019, p. 1-12. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951718820549. DOI: 10.1177/2053951718820549. Acesso em: 15 mar. 2020.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 7ª ed. Porto Alegre: Livraria do Advogado, 2007.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coord.) BIONI, Bruno (Coord. executivo). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

SARLET, Ingo Wolfgang. Notas acerca do direito fundamental à proteção de dados pessoais na constituição federal brasileira de 1988. *In:* GOMES, Ana Cláudia Nascimento; ALBERGARIA, Bruno; CANOTILHO, Mariana Rodrigues (Coord.). **Direito constitucional:** diálogos em homenagem ao 80ª aniversário de J. J. Gomes Canotilho. Belo Horizonte: Fórum, 2021b.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas**. 2ª ed. Rio de Janeiro: Lumen Juris, 2008.

SAURWEIN, Florian; LATZER, Michel; JUST, Natascha. *Governance of algorithms: options and limitations. **Emerald Group Publishing Limited***, Vol. 17, nº 6, 2015, pp. 35-49. ISSN 1463-6697. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2710400. DOI: 10.1108/info-05-2015-0025. Acesso em: 20 abr. 2020.

SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2013.

SELBST, Andrew; BAROCAS, Solon. *The Intuitive Appeal of Explainable Machines*. ***Fordham Law Review***, Vol 87, p. 1085-1139, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126971. Acesso em: 12 mai 2020.

SELBST, Andrew; POWLES, Julia. *Meaningful information and the right to explanation.* ***International Data Privacy Law***, Volume 7, Issue 4, November 2017, Pages 233–242. Disponível em: https://academic.oup.com/idpl/article/7/4/233/4762325. DOI: https://doi.org/10.1093/idpl/ipx022. Acesso em: 20 jun. 2021.

SCHERMER, Bart. *The limits of privacy in automated profiling and data mining.* ***Computer law & security review*** 27 (2011) 45-52. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364910001767. Acesso em: 15 fev. 2022.

SILES, Emile Loza de. *Artificial intelligence bias and discrimination: will we pull the arc of the moral universe towards justice? Journal of internacional and comparative law (dec. 2021), Vol. 8, nº 2, 2021. Duquesne University School of Law Research Paper* nº 2022-02. Disponível em: https://ssrn.com/abstract=4002486. Acesso em 17 fev. 2022.

SILVA, Priscilla Regina. Os direitos dos titulares de dados. *In*: MULHOLLAND, Caitlin (Org.) **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

SILVA; Ricardo Barretto Ferreira da Silva; DA SILVA, Camila Taliberti Ribeiro; IKEDA, Juliana Sene; SERRAGLIO, Lorena Pretti. *Accountability* e responsabilização sobre proteção de dados. In: BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia (Coord.) **Proteção de dados pessoais no Brasil:** uma nova visão a partir da Lei nº 13.709/2018. Belo Horizonte: Fórum, 2019.

SILVA, Rosane Leal da. **Cultura ciberlibertária X regulação da internet**: a co-regulação como modelo capaz de harmonizar este conflito. Revista Brasileira de Estudos Constitucionais, v. 21, p. 308, 2012.

SILVEIRA, Sérgio Amadeu da. A noção de modulação e os sistemas algorítmicos. *In*: SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu da (Org.). **A sociedade de controle: manipulação e modulação nas redes digitais.** São Paulo: Hedra, 2018.

SINGER, Natasha. *Amazon is pushing facial technology that a study says could be biased.* ***The New York Times***, 24 junho 2019. Disponível em: https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html?auth=login-google. Acesso em: 05 mai. 2020.

SNOW, Jacob*. Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. **ACLU**, 26 julho 2018. Disponível em: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28. Acesso em: 15 jun. 2020.

SOUZA, Carlos Affonso; MAGRANI, Eduardo; CARNEIRO, Giovana. Lei geral de proteção de dados pessoais: uma transformação na tutela dos dados pessoais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo do Brasil**. Porto Alegre: Arquipélago, 2020.

SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. *In*: DONEDA, Danilo, *et al*. (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro, Forense, 2021.

STATT, Nick. *Amazon bans police from using its facial recognition technology for the next year.* ***Theverge*****,** 10 junho de 2020. Disponível em: https://www.theverge.com/2020/6/10/21287101/amazon-rekognition-facial-recognition-police-ban-one-year-ai-racial-bias. Acesso em: 05 mai. 2020.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. São Paulo: RT, 2005.

TAYLOR, Diane. *Black boy in stop and search '30 times' accuses Met police of racist profiling,* ***The Guardian***, 15 de novembro de 2021. Disponível em: https://www.theguardian.com/uk-news/2021/nov/15/black-boy-in-stop-and-search-30-times-accuses-met-police-of-racist-profiling. Acesso em: 10 fev. 2022.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais. **Instituto de Tecnologia & Sociedade do Rio (ItsRio)**, 2018. Disponível em: https://itsrio.org/pt/publicacoes/proposta-anpd/. Acesso em: 21 fev. 2022.

TENE, Omer. POLONETSKY, Jules. *Big Data for All: Privacy and User Control in the Age of Analytics.* ***Northwestern Journal of Technology and Intellectual Property***, 2013. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 25 mai 2021.

TEPEDINO, Gustavo. A tutela da personalidade no Ordenamento Civil-Constitucional Brasileiro. *In*: TEPEDINO, Gustavo. **Temas de direito civil.** Rio de Janeiro: Renovar, 1999. Disponível em: https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil_constitucional_brasileiro. Acesso em: 05 jan. 2022.

TIKU, Nitasha. *Get Ready for the Next Big Privacy Backlash Against Facebook.* ***Wired*****,** 21 de maio de 2017. Disponível em: https://www.wired.com/2017/05/welcome-next-phase-facebook-backlash/. Acesso em: 15 mar. 2021.

UNIÃO EUROPEIA. Parlamento e Conselho. Regulamento (EU) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral de sobre Proteção de Dados). **Jornal Oficial**

da União Europeia, [s. l.], L 119/1, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. Acesso em: 05 jun. 2021.

UNIÃO EUROPEIA. Cara dos direitos fundamentais da União Europeia. Jornal Oficial das Comunidades Europeias (2000/C 364/01). Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 10 fev. 2022.

UNITED NATIONS. ***Universal Declaration of Human Rights (UDHR)****. Enacted on December 10, 1984.* Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 15 fev. 2022.

VAINZOF, Rony; MORAES, Henrique Fabretti. As qualificações e os desafios do encarregado pelo tratamento de dados pessoais no setor privado. *In:* FRANCOSKI; Denise de Souza Luiz; TASSO, Fernando Antônio. **A lei geral de proteção de dados pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paulo: Revista dos Tribunais, 2021.

VIEIRA; James Batista; BARRETO, Rodrigo Tavares de. Governança, gestão de riscos e integridade. Brasília: Enap, 2019. Disponível em: https://repositorio.enap.gov.br/bitstream/1/4281/1/5_Livro_Governan%C3%A7a%20Gest%C3%A3o%20de%20Riscos%20e%20Integridade.pdf. Acesso em: 05 jan. 2021.

WACHTER, Sandra. *Affinity profiling and discrimination by association in online behavioural advertising.* ***Berkeley Technology Law Journal****, Vol. 35, No. 2, 2020, Forthcoming* (*May* 15, 2019). Disponível em: https://ssrn.com/abstract=3388639 or http://dx.doi.org/10.2139/ssrn.3388639. Acesso em: 10 jan. 2022.

WACHTER, Sandra; MITTELSTADT, Brent. *A right to reasonable inferences: re-thinking data protection law in the age of big data and IA****. Columbia Business Law Review***, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Acesso em: 05 jan. 2021.

WALLACH, Wendell, *Control and Responsilbe Innovation in the Developmente of AI and Robotics.* ***The hastings center****,* 2020. Disponível em: https://www.thehastingscenter.org/who-we-are/our-research/current-projects/control-and-responsible-innovation-in-the-development-of-autonomous-machines/. Acesso em: 02 nov. 2020.

WIMMER, Miriam; PIERANTI, Octavio Penna. Programas de *compliance* e a LGPD: a interação entre autorregulação e a regulação estatal. *In*: FRAZÃO, Ana, CUEVA, Ricardo Villas Bôas (Coord.). ***Compliance*** **e políticas de proteção de dados**. São Paulo: Livraria Revista dos Tribunais, 2022.

YEUNG, Karen. Algorithmic regulation: a critical interrogation. **King's College London Dickson Poon School of Law Legal Studies Research Paper Series:** Paper nº. 2017-27, Disponível em:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972505. Acesso em: 04 de abr. 2021.

ZANATTA, Rafael; ABRAMOVAY, Ricardo. Dados, vícios e concorrência: representando o jogo das economias digitais. **Estudos Avançados 33** (96), p. 421-446, 2019. Disponível em: https://www.revistas.usp.br/eav/article/view/161303. DOIS: https://doi.org/10.1590/s0103-4014.2019.3396.0021. Acesso em: 10 mar. 2021.

ZANATTA, Rafael. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? **REDE 2017**. I Encontro da Rede de Pesquisa em Governança da Internet, 14 de nov. 2017. Disponível em: http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em: 07 jun. 2020.

ZUBOFF, Shoshana. *Big Brother*: capitalismo de vigilância e perspectivas para uma civilização de informação. BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; HUILHON, Luciana e MELGAÇO, Lucas (Orgs.). **Tecnopolíticas da vigilância:** perspectivas da margem. São Paulo: Boi Tempo, 2018. [Versão Eletrônica]