

**REVISTA SEMESTRAL DE
DIREITO EMPRESARIAL**

Nº 28

Publicação do Departamento de Direito Comercial e do Trabalho
da Faculdade de Direito da Universidade do Estado do Rio de Janeiro

Rio de Janeiro
Janeiro / Junho de 2021

Publicação do Departamento de Direito Comercial e do Trabalho da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (Prof. Alexandre Ferreira de Assumpção Alves, Prof. Eduardo Henrique Raymundo Von Adamovich, Prof. Enzo Baiocchi, Prof. Ivan Garcia, Prof. João Batista Berthier Leite Soares, Prof. José Carlos Vaz e Dias, Prof. José Gabriel Assis de Almeida, Prof. Leonardo da Silva Sant'Anna, Prof. Marcelo Leonardo Tavares, Prof. Mauricio Moreira Menezes, Prof. Rodrigo Lychowski e Prof. Sérgio Campinho).

EDITORES: Sérgio Campinho e Mauricio Moreira Menezes.

CONSELHO EDITORIAL: Alexandre Ferreira de Assumpção Alves (UERJ), Ana Frazão (UNB), António José Avelãs Nunes (Universidade de Coimbra), Carmen Tiburcio (UERJ), Fábio Ulhoa Coelho (PUC-SP), Jean E. Kalicki (Georgetown University Law School), John H. Rooney Jr. (University of Miami Law School), Jorge Manuel Coutinho de Abreu (Universidade de Coimbra), José de Oliveira Ascensão (Universidade Clássica de Lisboa), Luiz Edson Fachin (UFPR), Marie-Hélène Monsérié-Bon (Université des Sciences Sociales de Toulouse), Paulo Fernando Campos Salles de Toledo (USP), Peter-Christian Müller-Graff (Ruprecht-Karls-Universität Heidelberg) e Werner Ebke (Ruprecht-Karls-Universität Heidelberg).

CONSELHO EXECUTIVO: Carlos Martins Neto e Mariana Pinto (coordenadores). Guilherme Vinseiro Martins, Leonardo da Silva Sant'Anna, Livia Ximenes Damasceno, Mariana Campinho, Mariana Pereira, Mauro Teixeira de Faria, Nicholas Furlan Di Biase e Rodrigo Cavalcante Moreira.

PARECERISTAS DESTE NÚMERO: Bruno Valladão Guimarães Ferreira (PUC-Rio), Caroline da Rosa Pinheiro (UFJF), Fabrício de Souza Oliveira (UFJF), Fernanda Valle Versiani (UFMG), Gerson Luiz Carlos Branco (UFRGS), José Gabriel Lopes Pires Assis de Almeida (UERJ), Maíra Fajardo Linhares Pereira (UFJF), Marcelo Féres (UFMG), Marcelo Lauar Leite (UFERSA), Pedro Wehrs do Vale Fernandes (UERJ), Rafael Vieira de Andrade de Sá (FGV-SP), Raphaela Mag-nino Rosa Portilho (UERJ) e Sergio Marcos Carvalho de Ávila Negri (UFJF).

PATROCINADORES:



ISSN 1983-5264

CIP-Brasil. Catalogação-na-fonte
Sindicato Nacional dos Editores de Livros, RJ.

Revista semestral de direito empresarial. — n° 28 (janeiro/junho 2021)
. — Rio de Janeiro: Renovar, 2007-.

v.

UERJ
Campinho Advogados
Moreira Menezes, Martins Advogados

Semestral

1. Direito — Periódicos brasileiros e estrangeiros.

94-1416.

CDU — 236(104)

INTELIGÊNCIA ARTIFICIAL E *COMPLIANCE* - A (IN)SUFICIÊNCIA DOS MARCOS DE PROTEÇÃO DE DADOS¹

ARTIFICIAL INTELLIGENCE AND COMPLIANCE – THE (IN)SUFFICIENCY OF DATA PROTECTION FRAMEWORKS

*Caroline Rosa Pinheiro**
*Gabriel Ribeiro Brega***

Resumo: O presente estudo busca analisar o tratamento a ser dispensado aos algoritmos e à inteligência artificial no *compliance* realizado por sociedades empresárias. Nesse sentido, almeja perquirir a resposta aos seguintes questionamentos: o cumprimento às atuais normas relativas à proteção de dados é capaz de lidar, também, com os riscos relacionados à inteligência artificial, em particular, aos algoritmos? São necessárias medidas adicionais para esse desiderato? Com objetivo de responder a essas perguntas, realizou-se uma revisão bibliográfica sobre o tema, baseada na análise dos riscos inerentes à adoção dos algoritmos, sobretudo quando utilizados para a tomada de decisões para e sobre seres humanos. A conclusão a que se chegou é a de que o uso de algoritmos gera riscos cujo devido enfrentamento não é resolvido apenas pelo seguimento dos comandos dispostos na legislação de proteção de dados.

¹ Artigo recebido em 27.11.2021 e aceito em 06.03.2022.

* Professora Adjunta do curso de Direito da Universidade Federal de Juiz de Fora – UFJF. Doutora em Direito pela Universidade do Estado do Rio de Janeiro – UERJ. Mestre pela Fundação Getúlio Vargas – FGV-Rio. Coordenadora do Grupo de Pesquisa Empresa, Desenvolvimento e Responsabilidade (EDRESP) da Faculdade de Direito da UFJF. Advogada. E-mail: caroline.ufjf@gmail.com

** Graduando em Direito na Universidade Federal de Juiz de Fora – UFJF. Pesquisador do Grupo de Pesquisa Empresa, Desenvolvimento e Responsabilidade (EDRESP) da Faculdade de Direito da UFJF. E-mail: gabrielbrega37@gmail.com

Palavras-chave: Algoritmos. Inteligência Artificial. Compliance. Direito Digital. Direito Empresarial.

Abstract: The present study seeks to analyze the treatment to be given to algorithms and artificial intelligence in the compliance performed by companies. In this scope, it aims to investigate the answer to the following questions: does the compliance with the current rules concerning data protection exhaust the risks related to artificial intelligence, in particular, to algorithms? Are additional measures necessary for that purpose? In order to answer these questions, a literature review was conducted on the subject, based on the analysis of the risks inherent to the adoption of algorithms, especially when used to make decisions for and about human beings. The conclusion reached is that the use of algorithms generates risks whose proper response is not solved only by following the commands set out in data protection legislation.

Keywords: Algorithms. Artificial Intelligence. Compliance. Digital Law. Business Law.

Sumário: Introdução. 1. Algoritmos e Inteligência Artificial. 2. Regulação do Tema. 3. As Legislações de Dados e os Algoritmos. Conclusão.

Introdução.

No mundo hodierno, o ser humano se vê cada vez mais inserido em uma realidade hiperconectada, em que a esfera digital assume um caráter quase ubíquo. Progressivamente, as pessoas se deparam com conceitos como dados pessoais, inteligência artificial, algoritmos e internet das coisas, elementos estes que possuem um impacto cada vez maior em suas vidas. Cientistas sustentam² que, hoje,

² Dentre eles, Tim Berners-Lee, o criador da *world wide web*, e Nigel Shadbolt, pesquisador

vive-se em uma terceira geração da internet (*Web 3.0*), marcada pela interação não só entre pessoas, mas entre estas e coisas. Referida interação levaria à chamada *web* semântica, na qual as coisas passam a obter, processar e interpretar um volume expressivo de dados dos usuários, a fim de lhes fornecer serviços da maneira mais personalizada possível.³

Nesse cenário, os dados pessoais⁴ assumem uma importância cada vez mais expressiva, manifestada, sobretudo, no fenômeno do *Big Data*, termo que designa grandes volumes de dados, estruturados ou não, oriundos de variadas fontes, e coletados, armazenados e analisados em alta velocidade.⁵ Essas estruturas de dados, por sua vez,

em inteligência artificial na Universidade de Oxford. SHANNON, Victoria. *A 'more revolutionary' Web*. 2006. Disponível em: <https://www.nytimes.com/2006/05/23/technology/23iht-web.html>. Acesso em: 30 dez. 2020.

3 MAGRANI, E. *Entre dados e robôs*. Porto Alegre: Arquipélago Editorial, 2019.

4 De acordo com o artigo 5º, I da LGPD, dado pessoal consiste numa “informação relacionada a pessoa natural identificada ou identificável”. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União, Brasília, DF, 14 ago. 2018. Embora a maior parte da doutrina trate “dados” e “informações” de maneira indistinta, alguns autores fazem uma diferenciação, dando aos dados uma conotação mais primitiva e fragmentada, no sentido de ser uma informação em potencial. A informação, por sua vez, aludiria a algo além da representação contida no dado, após sua interpretação e elaboração. Nesse sentido, ver DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJLL]*, Chapecó, v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 16 fev. 2021. Todavia, neste trabalho, os termos serão trabalhados de maneira indistinta.

5 CAVALCANTI, J. The New “ABC” of ICTs (Analytics + Big Data + Cloud Computing): A Complex Trade-Off between IT and CT Costs. In: MARTINS, J. T.; MOLNAR, A. (Eds.). *Handbook of Research on Innovations in Information Retrieval, Analysis, and Management*. Hershey: IGI Global, 2016. p. 152–186. Disponível em: <https://www.igi-global.com/gateway/chapter/137478>. Acesso em: 30 dez. 2020. Esse conceito ilustra as 3 principais características do *Big Data*, conhecidas como “3 V’s”, quais sejam: volume, velocidade e variedade. Alude-se ainda a uma quarta característica, um quarto “V”, que seria a veracidade, utilizada, por exemplo, por Ana Frazão em FRAZÃO, A. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (Eds.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia LTDA., p. 23–52, 2019.

servem de alimento para o desenvolvimento e funcionamento dos mais diferentes algoritmos. Assim, depara-se hoje com uma realidade em que, mais do que nunca, o ser humano é submetido a processos decisórios realizados não por outras pessoas, mas por algoritmos, muitos dos quais já dotados de inteligência artificial.

Esses recursos, entretanto, não se restringem apenas àquilo que tradicionalmente se atribui ao meio digital (como redes sociais e mecanismos de busca), sendo amplamente utilizados por sociedades empresárias dos mais diversos ramos e tipos. Contudo, o recurso a algoritmos – sobretudo os de maior complexidade – é uma medida envolta em uma série de riscos, dada a imprevisibilidade intrínseca a essas tecnologias, conforme se constatará. Nessa perspectiva, no âmbito do Direito Empresarial, o *compliance* apresenta importante função, visto que se constitui como medida capaz de auxiliar os agentes econômicos em sua tarefa de mitigar riscos e se adequar às mudanças normativas que acompanham as rápidas transformações tecnológicas do mundo atual, além de amparar a definição de estratégias de longo prazo para a atividade empresarial.

Portanto, este trabalho tem o escopo de escrutinar se a elaboração de programas de integridade que atendam às novas exigências de proteção de dados no Brasil – notadamente após a publicação da Lei Geral de Proteção de Dados (LGPD) – encerra os riscos ligados à utilização de algoritmos, ou se medidas adicionais são necessárias. Aliás, esses dois processos – o tratamento de dados pessoais e a automatização de decisões – são intimamente ligados, e a estruturação das companhias de modo a atender aos requisitos normativos do primeiro pode gerar a impressão (falsa ou verdadeira, a se verificar) de que os perigos do segundo estão sendo devidamente administrados.

A hipótese ante o questionamento colocado é de que os algoritmos são elementos de tamanha importância que hoje devem merecer, nos programas de integridade das corporações, um tratamento que ultrapassa aquele destinado à proteção dos dados pessoais. Além disso, acredita-se que o mero seguimento da LGPD não seja capaz de resolver todos os riscos que são colocados por essas tecnologias.

A perquirição do problema *sub examine*, feita a partir de revisão bibliográfica sobre o tema, terá como referencial teórico as ideias desenvolvidas por Michael Latzer *et al.*⁶ Acerca dos problemas provenientes da ampla utilização dos algoritmos. Segundo os autores, essas tecnologias assumem um poder cada vez maior e seu uso, para a tomada de decisões que afetam diretamente os seres humanos, traz diversos riscos, em diferentes ordens, o que torna necessária uma maior gerência sobre esse processo.

O trabalho se dividirá, então, em três partes. Em um primeiro momento, busca-se definir os conceitos de algoritmos e inteligência artificial, ressaltando os desafios a eles atrelados. Em seguida, é feita uma breve descrição do atual regime normativo desses fenômenos, bem como da proteção de dados, destacando o papel do *compliance* nesse cenário. Ato contínuo, a terceira seção trata dos riscos gerados pela utilização de algoritmos por sociedades empresárias, contrastando-os com o regime de proteção de dados, a fim de constatar se este é suficiente para dirimi-los. Por fim, chegar-se à conclusão acerca das perguntas colocadas, à luz da problemática apresentada.

1. Algoritmos e Inteligência Artificial.

Algoritmos são um conjunto de instruções (códigos), destinados à realização de uma tarefa, produzindo um *output* (um resultado) a partir de um *input* (aquilo com que são “alimentados”, como dados).⁷ Em outras palavras, são:

6 LATZER, M; SAURWEIN, F.; JUST, N. Governance of Algorithms: Options and Limitations. Info, Cambridge, v. 17, n. 6, p. 35–49, 2015. Disponível em: https://www.researchgate.net/publication/281862395_Governance_of_algorithms_Options_and_limitations. Acesso em: 30 dez. 2020.

7 DONEDA, D.; ALMEIDA, V. What Is Algorithm Governance? *IEEE Internet Computing*, [s. l.], v. 20, n. 4, p. 60-63, jul./ago. 2016. Disponível em: <https://www.computer.org/csdl/magazine/ic/2016/04/mic2016040060/13rRUYekJ2d>. Acesso em: 30 dez. 2020.

conjuntos de **regras** que os computadores *seguem para resolver problemas e tomar decisões sobre um determinado curso de ação*. Em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa, ou seja, uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa.⁸ – grifos nossos

Contudo, sem material sobre o qual atuar, os algoritmos possuem limitada funcionalidade. Conforme destacam Doneda e Almeida,⁹ a razão de hoje se verificar um acelerado crescimento na utilização dos códigos é a massiva disponibilidade de dados. A propósito, referidos recursos são a base sobre a qual os algoritmos operam, de modo que sua presença em maior volume tem permitido o desenvolvimento de algoritmos mais complexos, capazes, inclusive, de tomar decisões sobre e para seres humanos. Com isso, constata-se a emergência de uma realidade em que um número cada vez maior de decisões é delegada às máquinas.

Esse processo de automatização se intensifica nos casos em que os códigos são dotados de inteligência artificial (IA). A inteligência artificial¹⁰ foi um termo cunhado em 1956, por John McCarthy,

8 MAGRANI, E., *Op. Cit.*, p. 19.

9 DONEDA, D.; ALMEIDA, V., *Op. Cit.*

10 Tecnicamente, quando se fala em inteligência artificial, é necessário ter em mente que existem três tipos dessa tecnologia: (1) a IA fraca, ou estreita (*weak AI* ou *narrow AI*) uma máquina não ciente, consistente em programas que desempenham tarefas específicas, ainda que complexas, o que envolve desde jogar xadrez, até dirigir carros; (2) a IA forte (*strong AI*), que possui a capacidade de aplicar a inteligência a qualquer problema, e não somente a domínios específicos, sendo capazes de resolver problemas a respeito dos quais não tinham conhecimento quando foram desenvolvidos; (3) a super inteligência (*super intelligence*), que seriam máquinas capazes de ultrapassar a semântica, a percepção e a cognição humanas. Vale destacar que, até hoje, foram desenvolvidos algoritmos situados tão somente no primeiro grupo, sendo os outros dois ainda hipotéticos. BUTLER, T.; BRIEN, L. O. Artificial Intelligence for

pesquisador de Stanford, durante a Conferência de Dartmouth, referindo-se à situação em que um programa de computador seria capaz de fazer algo que normalmente é atribuído à inteligência¹¹ de seres humanos.¹² Não obstante, conforme destacado pela *Society for the Study of Artificial Intelligence and Simulation of Behavior*,¹³ em referência a esse conceito, a inteligência artificial não necessariamente seria feita pela reprodução de mecanismos da inteligência humana, podendo tal resultado ser atingido por outros meios.

De qualquer forma, essa capacidade de realizar aquilo que, tradicionalmente, é considerado como fruto da inteligência humana é possibilitada, sobretudo, a partir do processo de *machine learning*, pelo qual os algoritmos aprendem e se desenvolvem com base em suas experiências anteriores, de modo que os próprios códigos estariam em constante mutação. A forma de *machine learning* de maior eminência hoje é o *deep learning*, que consiste na alimentação da máquina com vasta quantidade de dados, que serão por ela classificados sucessivamente, através de redes neurais não lineares, com base nos *outputs* de camadas antecedentes.¹⁴

Regulatory Compliance: are we there yet? *Journal of Financial Compliance*, [s.l.], v. 3, n. 1, p. 44–59, 2019.

11 Segundo definição adotada pela OCDE, no documento *Recommendation of the Council on Artificial Intelligence*, em tradução livre, a inteligência artificial é um sistema baseado em máquinas que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões, recomendações ou decisões, influenciando ambientes reais ou virtuais. Ver em OECD. *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449. 2019. Disponível em: <https://www.oecd.org/going-digital/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm>. Acesso em: 26 dez. 2020. O mesmo conceito foi adotado pela Estratégia Brasileira de Inteligência Artificial. Conforme BRASIL. Portaria GM nº 4.617, de 6 de abril de 2021. *Institui a Estratégia Brasileira de Inteligência Artificial e seus eixos temáticos*. Ministério da Ciência, Tecnologia e Inovações/Gabinete do Ministro. Diário Oficial da União, Brasília, DF, 6 de abril de 2021B.

12 MAGRANI, E., *Op. Cit.*

13 THE SOCIETY FOR THE STUDY OF ARTIFICIAL INTELLIGENCE AND SIMULATION OF BEHAVIOUR. *What is AI?* 2014. Disponível em: <https://aisb.org.uk/what-is-ai/>. Acesso em: 26 dez. 2020.

14 MARR, B. What Is The Difference Between Deep Learning, Machine Learning and AI? *For-*

Embora possa parecer que o debate acerca dos algoritmos e da inteligência artificial se limita às sociedades empresárias com atuação no espaço digital, como *fintechs* ou provedoras de aplicações (como redes sociais), tal suposição se trata de grande engano. Os algoritmos, inclusive aqueles dotados de inteligência artificial, vêm sendo, cada vez mais, empregados por agentes econômicos dos mais diversos ramos, deixando de se restringir apenas às sociedades empresárias que possuem seu objeto social alinhado à tecnologia. Sua crescente utilização visa à obtenção de maior objetividade na tomada de decisões, que passariam a se basear em critérios estatísticos e estariam, pretensamente, imunes a vieses (*bias*) típicos das decisões tomadas pelos seres humanos.¹⁵ Além disso, sua aplicação possibilita a redução de custos de transação, bem como a mitigação de assimetrias informacionais, notadamente no campo empresarial.¹⁶

É possível dividir a utilização de inteligência artificial no âmbito empresarial em duas grandes áreas: a externa, relativa à interface com terceiros, e a interna, referente aos processos decisórios no interior da sociedade.¹⁷ A doutrina elenca, ainda, como possíveis formas de utilização dessa tecnologia no âmbito corporativa as seguintes:

[...] (i) melhoria na infraestrutura, soluções e serviços; (ii) aperfeiçoamento dos sistemas de defe-

bes, 8 dez. 2016. Disponível em: <https://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference-between-deep-learning-machine-learning-and-ai/?sh=38e77cf426cf>. Acesso em: 22 dez. 2020.

15 DONEDA, D. *et al.* Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar – Revista de Ciências Jurídicas*, Fortaleza, v. 23, n. 04, p. 1–17, 2018. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8257>. Acesso em: 30 dez. 2020.

16 LATZER, M. *et al.* *The Economics of Algorithmic Selection on the Internet*. Zurich: IPMZ – Institute of Mass Communication and Media Research, 2014. Disponível em: https://www.mediachange.ch/media/pdf/publications/Economics_of_algorithmic_selection_WP.pdf. Acesso em: 30 dez. 2020.

17 TEFFÉ, C. S.; MEDON, F. Responsabilidade Civil e Regulação De Novas Tecnologias: Questões Acerca da Utilização de Inteligência Artificial na Tomada de Decisões Empresariais. *Revista Estudos Institucionais*, Rio de Janeiro, v. 6, n. 1, p. 301–333, 2020. Disponível em: <https://estudosinstitucionais.com/REI/article/view/383>. Acesso em: 30 dez. 2020.

sa em cibersegurança; (iii) maiores benefícios em cuidados de saúde das pessoas; (iv) automação no processo de recrutamento de novos empregados; (v) interfaces de conversação inteligentes; (vi) redução no uso de energia e de custos; (vii) previsão de exploração de vulnerabilidades; (viii) melhoria na análise das respostas de consumidores a pesquisas de satisfação; (ix) previsão de mercado; (x) aceleração do processo de leitura, em comparação com seres humanos; (xi) melhoria na contabilidade e análise financeira; (xii) melhoria nas regras de cobrança dos consumidores; (xiii) melhor compreensão de intenções e comportamentos; e (xiv) revisão de propostas.¹⁸

Assim, verifica-se a amplitude do campo de aplicação desses recursos, que tende apenas a se diversificar. Destaque-se que esse processo ocorre não só pelo desenvolvimento de algoritmos pelas próprias sociedades empresárias que vão deles se valer internamente (como é o caso do famoso algoritmo responsável pela formação do *feed* no *Facebook*, o *EdgeRank*), mas também pela aquisição de tecnologias ofertadas por companhias nisso especializadas, que fornecem um mesmo *software* a diferentes agentes. Fato é que, progressivamente, as sociedades empresárias têm obtido acesso a *softwares* capazes de orientar a tomada de decisões no âmbito corporativo. Estudos existem, por exemplo, sobre a viabilidade de sua aplicação para a identificação de cláusulas penais em textos legais, para fins de adequação a exigências normativas.¹⁹ Destaque-se, nesse sentido, o *ROSS*, inteligência artificial desenvolvida pelo computador *Watson*, da *IBM*, e destinado a atuar como consultor jurídico, sendo capaz de

18 *Ibidem*, p. 314.

19 GOLTZ, N.; MAYO, M. *Enhancing Regulatory Compliance by Using Artificial Intelligence Text Mining to Identify Penalty Clauses in Legislation*. MIREL 2017 – Workshop on ‘Mining and REasoning with Legal texts’. London, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977570. Acesso em: 22 dez. 2020.

ler mais de um bilhão de documentos por segundo.²⁰ Na mesma seara encontra-se a *Lex Machina*, *software* dotado de tecnologia de *machine learning*, desenvolvido pela *LexisNexis*, e que promete reduzir o risco de litigância, aumentar a efetividade, prever custos legais e identificar o melhor conselho legal para contratar. Este, vale dizer, conforme informado na própria página inicial do produto, é utilizado por diversas companhias, como *FedEx*, *GM*, *hp*, *Huawei* e *Johnson e Johnson*.²¹

Há, também, a *Neota Logic*, plataforma de inteligência artificial destinada à criação, por parte das sociedades empresárias (consumidoras do sistema), de aplicativos inteligentes para a solução automatizada de problemas. Nesse último caso, há, inclusive, a expressa promessa de que a plataforma contribui para garantir o *compliance* da sociedade, como anunciado em sua página: “*Ensure Compliance. Help your business remain compliant with expert RegTech advice at their fingertips*”.²² Outro exemplo que vale destacar é o *Kira Systems*, *software* dotado de *machine learning*, destinado à análise de contratos, e que promete possibilitar às sociedades empresárias a tomada de decisões, com base em dados, a nível de toda a corporação, a revelação de *insights* críticos e a redução de custos com auditorias.²³ No Brasil, cabe destaque à plataforma Dados Legais, que garante a adequação das companhias às exigências da LGPD.²⁴

Não obstante, tal processo é acompanhado de enormes preocupações. Isso, porque, a tomada de decisões por algoritmos

20 IBM. *Watson Assistant*. Disponível em: <https://www.ibm.com/blogs/watson/2016/01/ross-and-watson-tackle-the-law/>. Acesso em: 22 dez. 2020.

21 LEX MACHINA. *Lex Machina Company*. Disponível em: <https://lexmachina.com/company/>. Acesso em: 26 dez. 2020.

22 NEOTALOGIC. *Risk and Compliance*. Disponível em: <https://www.neotalogic.com/department/ai-automation-for-risk-compliance-departments>. Acesso em: 22 dez. 2020. Tradução livre: Ajude o seu negócio a manter-se em compliance, com os conselhos especialistas de RegTech na ponta dos seus dedos.

23 KIRA SYSTEMS. [s. l.]. Disponível em: <https://kirasystems.com/>. Acesso em: 23 dez. 2020.

24 Disponível em: <https://dadoslegais.com.br/>. Acesso em: 16 fev. 2021.

pode trazer uma série de riscos, na medida em que, em diversas das vezes, os resultados não podem ser explicados, e tampouco antecipados, pelos próprios desenvolvedores dos códigos.²⁵

Nessa toada, Introna²⁶ destaca dois principais motivos pelos quais os algoritmos merecem cautela: sua inescrutabilidade (*inscrutability*) e sua executabilidade (*executability*). O primeiro aspecto diz respeito ao fato de que eles atuam sob a superfície daquilo que se utiliza, de modo que não podem ser inspecionados. Já o segundo se refere à questão de que os algoritmos operam automaticamente, sem a necessidade de intervenção humana após o seu início.

A fortiori, com a aplicação de algoritmos dotados de inteligência artificial, os algoritmos deixariam de representar uma mudança tão somente quantitativa em relação à atividade humana (por exemplo, sendo capazes de fazer cálculos de maneira mais rápida), mas representariam uma verdadeira mudança de paradigma:

Mais recentemente, o desenvolvimento e a implementação de tecnologias de inteligência artificial (IA) proporcionou efeitos que, muitas vezes, não podem mais ser compreendidos em termos meramente quantitativos, e que implicam uma mudança na subjetividade das relações entre as pessoas e a tecnologia. Essas novas tecnologias possibilitam a automatização da tomada de decisão em diversas situações complexas, executando tarefas que estávamos habituados a considerar como prerrogativas humanas, derivadas da inteligência – a ponto de que diversas manifestações dessas tecnologias foram denominadas como realizações de uma “inteligência artificial”.

25 DONEDA, D.; ALMEIDA, V., *Op. Cit.*

26 INTRONA, L. D. Algorithms, Governance and Governmentality: on governing academic writing. *Science, Technology, & Human Values*, [s.l.], v. 41, n. 1, p. 17-49, 2016.

Assim, os computadores passaram a não ser vistos somente como dispositivos destinados a fazer cálculos, sistematizações ou classificações, porém a deter, em algum grau, algo passível de ser comparado às ações humanas autônomas.²⁷

Nesse sentido, agravar-se-iam os riscos em relação aos algoritmos tradicionais. Conforme ressaltado em documento²⁸ da *Information Commissioner's Office*, a autoridade de dados do Reino Unido, a incorporação dessas tecnologias à análise de dados leva a uma opacidade do processo decisório dos algoritmos, uma vez que o motivo pelo qual tomaram determinada decisão não é compreensível para os seres humanos. Com isso, a possibilidade de auditoria e controle sobre seus *inputs* e *outputs* estaria ainda mais prejudicada, e esses sistemas, ainda menos transparentes.²⁹ Aliás, tornam-se verdadeiras caixas-pretas (*black boxes*), materializadas em milhões de linhas de códigos que, após uma série de mutações autorrealizadas, mostram-se incompreensíveis e inescrutáveis inclusive por seus desenvolvedores.³⁰

Latzer *et al.*³¹ identificam nove principais riscos decorrentes da

27 DONEDA, D. *et al.* *Op. Cit.*, p. 2.

28 INFORMATION COMMISSIONER'S OFFICE. *Big data, artificial intelligence, machine learning and data protection*. 2017. Disponível em: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Acesso em: 20 dez. 2020.

29 FRAZÃO, A. *Algoritmos e Inteligência Artificial*. 2020. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018. Acesso em: 330 dez. 2020.

30 INTRONA, L. D. *Op. Cit.*.

31 LATZER *et al.*, *Op. Cit.*, p. 37. Tradução livre a partir do original, que dispõe: “1. manipulation; 2. diminishing variety, the creation of echo chambers and filter bubbles, biases and distortions of reality; 3. constraints on the freedom of communication and expression, for example, censorship by intelligent filtering [...]; 4. surveillance and threats to data protection and privacy [...]; 5. social discrimination [...]; 6. violation of intellectual property rights [...]; 7. abuse of market power [...]; 8. effects on cognitive capabilities and the human brain [...]; and 9. growing heteronomy and loss of human sovereignty and controllability of technology.”

tomada de decisões por algoritmos, quais sejam: (i) a manipulação; (ii) a diminuição da variedade, com a criação de “bolhas de filtros” e com o enviesamento; (iii) a restrição à liberdade de expressão e comunicação; (iv) o monitoramento e as ameaças à privacidade e à proteção de dados; (v) a discriminação; (vi) a violação de direitos de propriedade intelectual; (vii) abuso de poder de mercado; (viii) efeitos sobre as capacidades cognitivas e o cérebro humano; (ix) o crescimento da heteronomia e a perda do controle humano sobre a tecnologia.

Por conseguinte, referidas tecnologias devem ser adotadas com cautela. Tendo em mente esses riscos, buscar-se-á discutir se seu enquadramento é devidamente realizado pelo *compliance* à luz das atuais normativas referentes à proteção de dados, ou se diligências adicionais são exigidas das sociedades empresárias para que se protejam de suas potencialidades. Para tanto, na próxima seção, serão brevemente apresentadas as normas relativas aos algoritmos e proteção de dados, bem como explicitadas as principais noções vinculadas ao *compliance*.

2. Regulação do Tema.

Os fenômenos aqui trabalhados, como o *Big Data* e a utilização de algoritmos, evoluíram, por muito tempo, em um ambiente praticamente desprovido de efetiva regulação normativa por parte do Estado, o que fez com que esse vácuo fosse preenchido por instrumentos autorregulatórios, executados pelos próprios agentes econômicos envolvidos.³² Em que pese a existência, até 2017, de mais de 40 normas regulando, ainda que indiretamente, a proteção de dados no Brasil,³³ estas tinham um caráter eminentemente setorial, não sendo ca-

32 FRAZÃO, A. *Op. Cit.*, p. 31.

33 Conforme tabela elaborada por Monteiro. MONTEIRO, R. L. *Proteção de dados e a legislação vigente no Brasil*. 2017. Disponível em: <http://baptistaluz.com.br/wp-con>

pazes de abranger toda a complexidade intrínseca a esses temas. Nesse sentido, destacam-se o Código de Defesa do Consumidor (Lei 8.078/1990), que, em seus artigos 43 e 46, trata do acesso a cadastros e a bancos de dados no âmbito das relações de consumo, a Lei do Cadastro Positivo (Lei 12.414/2011), que disciplina a questão dos bancos de dados para a formação de históricos de créditos e o Marco Civil da Internet (Lei 12.965/2014), que garante, ainda que de forma tímida, uma proteção de dados pessoais no ambiente *online*.

Contudo, foi somente com aprovação da Lei Geral de Proteção de Dados (Lei 13.709/2018, LGPD) que o tema passou a contar com uma efetiva regulação, de caráter geral, e não mais setorial.³⁴ Ademais, a LGPD não só unificou e harmonizou o ordenamento jurídico no que tange a esse ponto, como também o complementou, reconhecendo outros direitos.

Embora o escopo do presente trabalho seja a questão da utilização dos algoritmos, e não especificamente a proteção de dados pessoais, a menção a esses diplomas se faz de central importância tendo em vista que os dois temas possuem diversos pontos em comum; aliás, o tratamento de dados,³⁵ a que se refere a LGPD, é, muitas das vezes, feito por algoritmos. Assim, diversas provisões previstas nessas normativas se aplicam também aos algoritmos, de modo geral, e à inteligência artificial, particularmente. Nesse aspecto, de especial relevância se mostra a questão do direito à explicação previsto nesses diplomas, e que será trabalhado em tópico posterior.

tent/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf. Acesso em: 26 dez. 2020.

34 MONTEIRO, R. L. *Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?* 2018. Instituto Igarapé, Artigo Estratégico 39. 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 dez. 2020.

35 De acordo com o artigo 5º, X da Lei, tratamento de dados consiste em “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.

Não obstante, não há, ainda, no ordenamento pátrio, norma que trate especificamente de algoritmos e da inteligência artificial, mas tão somente documentos que apontam para intenções. Em maio de 2019, o Brasil aderiu³⁶ aos princípios da Organização para a Cooperação e Desenvolvimento Econômico para a administração responsável de inteligência artificial,³⁷ documento não vinculante que elencou cinco princípios para o desenvolvimento responsável dessa tecnologia, quais sejam: *inclusive growth, sustainable development and well-being; human-centred values and fairness; transparency and explainability; robustness, security and safety*; e *accountability*.³⁸ Além disso, estabeleceu cinco recomendações com base nesses princípios: *investing in AI research and development; fostering a digital ecosystem for AI; shaping an enabling policy environment for AI; building human capacity and preparing for labour market transformation*; e *international co-operation for trustworthy AI*.³⁹

Posteriormente, no dia 12 de dezembro de 2019, o Ministério da Ciência, Tecnologia, Inovações e Comunicações lançou consulta pública para a Estratégia Brasileira de Inteligência Artificial, que ficou disponível para discussão até o dia 2 de março de 2020.⁴⁰ A consulta foi organizada em seis eixos verticais (qualificações para um futuro

36 ÉPOCA NEGÓCIOS ONLINE. *OCDE cria princípios para desenvolvimento de IA; Brasil é um dos 42 signatários*. 2019. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2019/05/ocde-cria-principios-para-desenvolvimento-de-ia-brasil-e-um-dos-42-signatarios.html>. Acesso em: 26 dez. 2020.

37 OECD, *Op. Cit.*, 2019.

38 Tradução livre: crescimento inclusivo, desenvolvimento sustentável e bem-estar; valores centrados no ser humano e equidade; transparência e explicabilidade; robustez e segurança; e responsabilização.

39 Tradução livre: investir em pesquisa e desenvolvimento de IA; promover um ecossistema digital para IA; moldar um ambiente de políticas favorável à IA; desenvolver a capacidade humana e preparar-se para a transformação do mercado de trabalho; e cooperação internacional para uma IA confiável.

40 PORTAL DO GOVERNO BRASILEIRO. *Estratégia brasileira de inteligência artificial*. Disponível em: <http://participa.br/profile/estrategia-brasileira-de-inteligencia-artificial>. Acesso em: 26 dez. 2020.

digital; força de trabalho; pesquisa, desenvolvimento, inovação e empreendedorismo; aplicação no setor público; aplicação nos setores produtivos; segurança pública) e três eixos transversais (legislação, regulação e uso ético; aspectos internacionais; governança de IA), além da seção “prioridades e objetivos”.⁴¹ Ao fim, a estratégia contou com 908 contribuições; os eixos com os quais mais se contribuiu foram os de “legislação, regulação e uso ético” (256 contribuições) e “governança de IA” (108 contribuições), sendo a maior parte dos comentários advindos de indivíduos, conforme estudo realizado pelo Instituto de Tecnologia e Sociedade.⁴²

Após longo processo de elaboração, no dia 6 de abril de 2021, foi lançada a Estratégia Brasileira de Inteligência Artificial, veiculada pela Portaria GM nº 4.617. Além da consulta pública, o documento foi elaborado a partir de consultoria especializada em IA, contratada para tal fim, e de um *benchmarking* nacional e internacional, tendo como finalidade: “contribuir para a elaboração de princípios éticos para o desenvolvimento e uso de IA responsáveis”, “promover investimentos sustentados em pesquisa e desenvolvimento em IA”, “remover barreiras à inovação em IA”, “capacitar e formar profissionais para o ecossistema da IA”, “estimular a inovação e o desenvolvimento da IA brasileira em ambiente internacional” e “promover ambiente de cooperação entre os entes públicos e privados, a indústria e os centros de pesquisas para o desenvolvimento da Inteligência Artificial”.⁴³

Além de explicitar a metodologia na qual se baseou, a Estratégia promoveu interessante diagnóstico da realidade brasileira em

41 ITS – INSTITUTO TECNOLOGIA E SOCIEDADE. *Contribuições para a Estratégia Brasileira de Inteligência Artificial*. 2020. Consulta Pública – MCTIC. Disponível em: <https://itsrio.org/wp-content/uploads/2020/04/Contribui%C3%A7%C3%B5es-ITS-Consulta-P%C3%BAblica-IA.pdf>. Acesso em: 26 dez. 2020.

42 ITS – INSTITUTO TECNOLOGIA E SOCIEDADE. *Estratégia Brasileira de Inteligência Artificial*: perfil da participação da sociedade na consulta pública. 2020B. Disponível em: <https://itsrio.org/pt/comunicados/estrategia-brasileira-de-inteligencia-artificial/>. Acesso em: 26 dez. 2020.

43 ITS – INSTITUTO TECNOLOGIA E SOCIEDADE, 2021B. *Op. Cit.*

relação à sua capacidade inovativa. Ainda, teceu uma série de considerações a respeito nos nove eixos supramencionados, propondo uma série de ações estratégicas para cada um deles. Cabe ressaltar que, assim como na consulta, a questão relativa à regulação e governança da IA recebeu significativo destaque no trabalho do governo federal, embora ainda, como o restante do documento, em caráter propositivo.

Destarte, percebe-se que a temática da regulação da IA tem sido ponto nevrálgico na discussão, motivo pelo qual cabe agora realizar breve explicitação a respeito da própria noção de regulação.

Para fins do presente trabalho, considerar-se-á a regulação como gênero, cujas espécies são a heterorregulação, que é proveniente do Estado, e a autorregulação, desenvolvida pelos próprios agentes regulados,⁴⁴ embora não se ignore as divergências acerca desses termos.⁴⁵

Ressalte-se, ainda, que não se tem a pretensão de discutir sobre qual a melhor forma de regulação da inteligência artificial – se a partir do Estado ou a partir dos próprios agentes econômicos –, e, tampouco, de propor instrumentos regulatórios. O escopo desta perquirição é discutir se o *compliance* de dados pessoais realizado pelas

44 DIAS, L. A. R.; BECUE, S. M. F. Regulação e Autorregulação do Mercado de Valores Mobiliários Brasileiro: Limites da Autorregulação. *Revista Direito Empresarial*, Curitiba, v. 1, n. 12, p. 13–35, 2012.

45 A discussão sobre as divergências acerca das concepções de autorregulação foge ao escopo do presente trabalho. Contudo, em sua tese, Angela Donaggio desenvolve amplo debate a esse respeito, no que vale transcrever: “Em geral, atribui-se três significados ao termo autorregulação. O primeiro se refere à ausência de regulação no sentido da capacidade de funcionamento ‘equilibrado’ da economia, isto é, quando – ao menos teoricamente – não seria necessária a imposição de normas por ator externo aos agentes. O segundo significado trata da regulação de um determinado grupo por meio de normas voluntárias e autovinculação voluntária, nomeada como ‘autorregulação pura ou privada’. Por último, a autorregulação pode ser entendida como ‘a capacidade de determinado grupo de se regular mediante reconhecimento oficial e com meios de direito público’”. DONAGGIO, A. R. F. *Regulação e Auto-Regulação no Mercado de Valores Mobiliários: o caso dos segmentos especiais de listagem da BM&FBovespa*. Dissertação (Doutorado), Universidade de São Paulo, São Paulo, 2016. p. 187.

sociedades empresárias é capaz de abarcar os riscos gerados pela utilização de algoritmos.

No âmbito empresarial, compreende-se o *compliance*⁴⁶ (termo que, literalmente, designa o ato de cumprir), como “conjunto de procedimentos adotados por uma determinada sociedade, objetivando otimizar o cumprimento de normas legais, regulamentos e políticas estabelecidas pela organização, com o intuito de mitigar riscos e responsabilidades.”⁴⁷

Assim, diz respeito à adequação não só a normas legais, estipuladas pelo Estado, como também a parâmetros regulatórios estipulados por atores não-governamentais. Aliás, não se afigura como mera postura de seguimento de regras, moldando-se, na realidade, como “linha mestra de orientação da sociedade empresária”, ligada à ideia de contenção de riscos e de garantia de segurança jurídica.⁴⁸ Nessa toada, tais programas são utilizados pelas companhias como instrumentos que determinam os parâmetros que serão seguidos, considerando uma série de variáveis, regulatórias e não regulatórias, mas que impactam no desenvolvimento de sua política institucional para persecução do objeto social, de forma juridicamente eficiente e economicamente viável.

O *compliance*, vale ressaltar, vem sendo muito associado ao tema do ESG (*Environmental, Social, and Governance*), índice que avalia a atividade das sociedades empresárias conforme os seus impactos em três eixos da sustentabilidade – o Meio Ambiente, o Social e a Governança.⁴⁹ Esse índice, formulado por agências avaliadoras (as chamadas *ESG rating agencies*), tem sido progressivamente con-

46 Aqui, utilizado como sinônimo de programa de integridade.

47 PINHEIRO, C. da R. *Os Impactos dos Programas de Integridade (Compliance) sobre os Deveres e Responsabilidades dos Acionistas Controladores e Administradores de Companhia*. Rio de Janeiro: Universidade do Estado do Rio de Janeiro, Faculdade de Direito, 2017. p. 18.

48 *Ibidem*, p. 20.

49 De acordo com o conceito adotado pelo Pacto Global. PACTO GLOBAL. *Gigante no mercado financeiro adere ao investimento sustentável*. Disponível em: <https://www.pactoglobal.org.br/noticia/42>. Acesso em: 24 nov. 2021.

siderado por investidores no momento da alocação de seus recursos, seja por acreditarem que companhias com melhores índices possibilitarão maior retorno financeiro, seja por desejarem efetivamente contribuir para as mudanças em questão.⁵⁰

O ESG busca aferir a sustentabilidade corporativa de uma dada companhia, sendo esta entendida enquanto as atividades nela desempenhadas que proativamente procuram contribuir para a sustentabilidade, em suas dimensões econômica, ambiental e social, considerando os sistemas da sociedade empresária, ou seja, suas operações, sua gestão, sua estratégia, dentre outros fatores.⁵¹ Nesse cenário, o *compliance* é visto não só como parte de um dos pilares do ESG (a Governança), mas também como um instrumento para a garantia do bom desempenho nos demais (o Social e o Meio Ambiente).

Todavia, parte-se aqui de uma concepção pela qual os programas de integridade elaborados pelas sociedades empresárias possuem – ou, ao menos, deveriam possuir – caráter vinculante para elas, de modo a apresentar natureza de *hard law*. Acredita-se que, uma vez divulgado o programa de integridade, seu cumprimento passa a ser exigível das companhias, que podem ser penalizadas por órgãos de controle (inclusive judiciais) no caso de seu descumprimento – afastando-se o argumento normalmente veiculado de que teriam caráter meramente voluntarista.⁵² Nesse sentido:

Juridification by the courts, with which the legal qualification of the corporate codes enters into newfound land, runs in two opposing directions. On the one side, the courts exert strict control of

50 GIESE, G. *et al.* Foundations of ESG Investing: How ESG Affects Equity Valuation, Risk, and Performance. *The Journal of Portfolio Management*, [s.l.], v. 45, n. 5, p. 69-83, jul. 2019.

51 LOZANO, R. A Holistic Perspective on Corporate Sustainability Drivers. *Corporate Social Responsibility and Environmental Management*, [s.l.], v. 22, n.1, p. 32-44, 2013.

52 TEUBNER, G. Politics, Governance, and the Law: Transnational Economic Constitutionalism in the Varieties of Capitalism. *Global Perspectives*, [s. l.], v. 1, Issue 1, p. 1-12, 2020. Disponível em: <https://online.ucpress.edu/gp/article/1/1/13412/110924/Transnational-Economic-Constitutionalism-in-the>. Acesso em: 17 fev. 2021.

the contents of the codes, insofar as the codes burden employees or consumers; on the other side, the courts transform the codes into binding state law, insofar as they contain obligations in the public interest.⁵³

A propósito, caso não se reconheça ao programa de integridade um caráter vinculante, corre-se o risco de que tal instrumento constitua mero meio de publicidade para as companhias, apto a impactar positivamente suas relações públicas, inclusive por captação de recursos, sem que assumam compromisso efetivo com as medidas que propõem.⁵⁴ Assim, embora entendido como mecanismo autorregulatório, o *compliance* constitui instrumento de autorregulação regulada, tendo em vista que, apesar de ser elaborado pelas próprias sociedades empresárias, seu cumprimento é delas exigível.⁵⁵ Essa tem sido, inclusive, a tônica empregada pela legislação mais recente, como a Lei Anticorrupção (Lei 12.846/2013) e a própria LGPD.

Desde a aprovação da LGPD, fala-se cada vez mais da necessidade da adoção de um *compliance* orientado ao seguimento do novel diploma. Esse programa de conformidade seria necessário não só para garantir a adequação da estrutura corporativa à LGPD e às decisões da Agência Nacional de Proteção de Dados, como também para conferir maior concretude e aplicabilidade a diversos conceitos e

53 *Ibidem*, p. 9. Tradução livre: a “juridificação” pelos tribunais, com a qual a qualificação legal dos códigos empresariais entra em terras novas, corre em duas direções opostas. Por um lado, os tribunais exercem rígido controle sobre o conteúdo dos códigos, desde que os códigos sobrecarreguem funcionários ou consumidores; por outro lado, os tribunais transformam os códigos em leis vinculantes do Estado, contanto que contenham obrigações de interesse público.

54 REVAK, Haley. Corporate Codes of Conduct: Binding Contract or Ideal Publicity? *Hastings Law Journal*, São Francisco, v. 63, Issue 6, p.1646-1669, 2012. Disponível em: https://repository.uclahastings.edu/hastings_law_journal/vol63/iss6/9/. Acesso em: 17 fev. 2021.

55 AGUILAR, A. *O Compliance de Dados Pessoais das Sociedades do “Novo Mercado”*. Trabalho de Conclusão de Curso apresentado à Universidade Federal de Juiz de Fora. Juiz de Fora, 2020.

determinações deixados em aberto no texto legal.⁵⁷ Nesse sentido, a Lei estimula explicitamente a realização do *compliance*, contando o diploma com uma seção denominada “Das Boas Práticas e da Governança”, na qual há não só o estabelecimento de diretrizes para a realização do programa de integridade, como também a estipulação – artigo 50, §2º – de um conteúdo mínimo que ele deve conter.⁵⁸

Apesar da concentração nessa seção, essa lógica de estímulo à governança se espraia por todo o documento legal. Está presente, por exemplo, na imposição de sanções administrativas, tendo em vista que estas devem ser cominadas considerando a adoção de boas práticas e governança pelo agente (artigo 52, §1º, IX, LGPD). Além disso, reflete-se em outros instrumentos de cuja elaboração a Lei trata, e que também se destinam à proteção de dados, como o Relatório de Impacto em Proteção de Dados (artigo 38, LGPD) e os avisos de privacidade (artigo 9, LGPD).⁵⁹

Também o Regimento Interno da Autoridade Nacional de Proteção de Dados (ANPD), veiculado na Portaria nº 1 de 8 de março de 2021,⁶⁰ reforça essa perspectiva da Lei. Aliás, o documento estabelece que a ANPD será responsável por “reconhecer regras de boas práticas e de governança relacionadas ao tratamento de dados pessoais” (artigo 5º, VII), “solicitar a agentes públicos a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Públi-

57 FRAZÃO, A.; OLIVA, M. D.; ABRIL, V. DA S. Compliance de Dados Pessoais. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (Eds.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson reuters Brasil Conteúdo e Tecnologia LTDA., 2019. p. 677–715.

58 AGUILAR, A., *Op. Cit.*

59 O aviso de privacidade, ou *privacy notes*, “seria o documento direcionado ao titular de dados para que ele tenha ciência de seus direitos”. AGUILAR, A., *Op. Cit.*, p. 20.

60 BRASIL. Portaria nº 1, de 8 de março de 2021. *Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados – ANPD*. Presidência da República/Autoridade Nacional de Proteção de Dados/Conselho Diretor. Diário Oficial da União, Brasília, DF, 8 de março de 2021A.

co” (artigo 5º, XXIV) e divulgar, ao público em geral, “regras de boas práticas e de governança relacionadas ao tratamento de dados pessoais, reconhecidas pelo Conselho Diretor” (artigo 18, XVI, alínea “b”).

Ainda, tendo em vista o entendimento da proteção de dados pessoais enquanto um direito fundamental,⁶¹ diversos estudos têm apontado que sua efetivação é importante medida para a concreção do pilar Social do ESG. Dessa forma, uma atuação corporativa pautada no cumprimento das legislações de proteção de dados (no caso brasileiro, a LGPD) tende a ser levada em consideração nos índices elaborados pelas agências de avaliação ESG, na medida em que reflete o comprometimento empresarial com um direito fundamental do cidadão.⁶²

Portanto, constata-se que, hoje, há a exigência de adequação, em relação a padrões legais e éticos, das mais diversas organizações, dentre elas, as sociedades empresárias, o que, notadamente desde a LGPD – e, em menor medida, desde o Marco Civil da Internet –, direcionou-se também ao meio digital. Entretanto, questiona-se se o atual tratamento dado à proteção de dados é capaz de dirimir também os riscos criados pela utilização de algoritmos, principalmente aqueles dotados de inteligência artificial.

3. As Legislações de Dados e os Algoritmos.

Conforme até aqui já discutido, as sociedades empresárias têm

61 No Brasil, tramita no Congresso Nacional, atualmente, a Proposta de Emenda à Constituição 17/2019, que visa a incluir a proteção de dados pessoais no rol dos direitos fundamentais constitucionalmente protegidos. AGÊNCIA SENADO. *Senado inclui proteção de dados pessoais como direito fundamental na Constituição*. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protacao-de-dados-pessoais-como-direito-fundamental-na-constituicao>. Acesso em: 24 nov. 2021.

62 CUNTO, R. *A LGPD é ESG? Pensar a LGPD aplicada é pensar o conceito base da ESG com o indivíduo no centro da relação sociedade-corporação*. 2021. Lex Latin. Disponível em: <https://br.lexlatin.com/opiniao/lgpd-e-esg>. Acesso em: 24 nov. 2021.

cada vez mais se utilizado de algoritmos para a tomada de decisões nos mais diferentes aspectos e setores. Contudo, a adoção dessas tecnologias traz uma série de riscos para a atividade, ligados, sobretudo, a sua inescrutabilidade e imprevisibilidade.⁶³ Ademais, não há até hoje uma lei que regule a questão dos algoritmos específica e expressamente, salvo diretrizes gerais e não-vinculantes ratificadas pelo Estado brasileiro no âmbito internacional – a exemplo dos princípios da Organização para a Cooperação e Desenvolvimento Econômico para a administração responsável de inteligência artificial. Nesse cenário, assume especial relevância, então, para a gestão dos riscos criados pelos algoritmos, os programas de integridade adotados pelas companhias, os quais, ressalte-se mais uma vez, não se limitam ao seguimento de regras existentes, devendo constituir verdadeira “linha mestra” de orientação das ações da sociedade empresária.⁶⁴

Não obstante, poder-se-ia alegar que a mitigação dos riscos gerados pela utilização de algoritmos já seria realizada por meio da adequação das sociedades empresárias às exigências relativas à proteção de dados; a propósito, a utilização de algoritmos e o tratamento de dados pessoais (sobretudo considerando a conceituação ampla deste adotada pela LGPD) são processos intimamente conectados. Conforme afirma Monteiro:

Regular o uso e o tratamento de dados pessoais é o principal objetivo das leis de proteção de dados. Estas visam não somente proteger a privacidade, mas também outros direitos fundamentais e liberdades individuais, que somente podem ser

63 Vale, neste ponto, lembrar que, consoante elencado por Latzer *et al.*, a utilização de algoritmos traz como principais riscos: (i) a manipulação; (ii) a diminuição da variedade, com a criação de “bolhas de filtros” e com o enviesamento; (iii) a restrição à liberdade de expressão e comunicação; (iv) o monitoramento e as ameaças à privacidade e à proteção de dados; (v) a discriminação; (vi) a violação de direitos de propriedade intelectual; (vii) abuso de poder de mercado; (viii) efeitos sobre as capacidades cognitivas e o cérebro humano; (ix) o crescimento da heteronomia e a perda do controle humano sobre a tecnologia. LATZER *et al* (2015), *Op. Cit.*, p. 37.

64 PINHEIRO, C. da R. *Op. Cit.*

exercidos na sua completude caso seja garantido o uso adequado dos dados pessoais que, muitas vezes, funcionam como representação do indivíduo. Desta forma, as leis de proteção de dados são como “guarda-chuvas” regulatórios que protegem outros direitos.⁶⁵

De fato, a questão dos dados pessoais e dos algoritmos estão intrinsecamente ligadas; aliás, aqueles são o combustível destes. Desse modo, sobretudo no caso de algoritmos inteligentes, que necessitam de um maior volume de dados, é quase impossível falar de um deles sem se referir aos outros.⁶⁶ Não obstante, não há uma perfeita sobreposição de uma questão em relação à outra, de maneira que, em certos casos, embora o código do algoritmo esteja em plena conformidade com o ordenamento jurídico, os dados que o alimentam foram coletados de modo ilegal, ou destinados para uma finalidade distinta da inicial; por outro lado, certamente há situações em que, embora os dados tenham sido coletados de forma diligente, e estejam sendo processados de acordo com critérios legais, o código, em si, fere, de alguma maneira, o ordenamento jurídico.

Nessa toada, a atual regulação relativa à proteção de dados, e o *compliance* empresarial realizado à sua luz, mostram-se aptos a lidar com as primeiras situações (em que a falha está nos dados); cabe, porém, questionar, se são capazes de lidar com casos em que a violação ao ordenamento advém do próprio algoritmo. Em relação aos nove riscos, Latzer et al.⁶⁷ *acreditam que as recentes iniciativas legislativas dos Estados em relação à questão dos dados pessoais resolveram somente os riscos trazidos pelos algoritmos no que concerne à privacidade, mas não os demais. Igualmente, Doneda e Almeida*⁶⁸ *expressam a opinião de que as legislações de proteção de dados resolvem*

65 MONTEIRO, R. L., *Op. Cit.*, p. 2.

66 Cf. DONEDA, D. *et al*, *Op. Cit.*

67 LATZER, M. *et al.*, *Op. Cit.*

68 DONEDA, D.; ALMEIDA, V., *Op. Cit.*

muitos, mas não todos os problemas relacionados à utilização desses códigos.

Por outro lado, pode-se argumentar que, especificamente no caso brasileiro, a LGPD, por possuir um escopo amplo e abrangente, encerraria também a questão dos algoritmos, na medida em que trata de algumas questões atinentes a eles em si. A propósito, o artigo 20⁶⁹ da Lei consagra o direito à explicação, que “diz respeito ao direito de receber informações suficientes e inteligíveis que permita ao titular dos dados entender a lógica e os critérios utilizados para tratar seus dados pessoais para uma ou várias finalidades”.⁷⁰ Assim, garante ao indivíduo a revisão e a explicação de decisões tomadas com base unicamente no tratamento automatizado de seus dados, como se verifica:

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.

§ 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.

§ 2º Em caso de não oferecimento de informações

69 Vale ressaltar que este dispositivo possuía um terceiro parágrafo, garantindo ao titular de dados o direito de ter a decisão revisada por pessoa natural. Tratar-se-ia do direito à revisão, que “compreende o direito do titular de requisitar a revisão, por um humano, de uma decisão totalmente automatizada que possa ter um impacto nos seus interesses, principalmente os relacionados à definição do seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade”. MONTEIRO, R. L., *Op. Cit.*, p. 4. No entanto, o trecho foi vetado (Lei nº 13.853/2019).

70 MONTEIRO, R. L., *Op. Cit.*, p. 4.

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.⁷¹

Essa prerrogativa, decorrente do princípio da transparência (Art. 6º, IV, LGPD), assegura aos titulares dos dados o direito de saber que tipos de dados pessoais seus são utilizados pelos algoritmos em suas decisões automatizadas, bem como os critérios utilizados no processo. Ainda, caso o processo automatizado vise a formar perfis comportamentais, ou se valha de um perfil comportamental para tomar uma decisão subsequente, esse direito também inclui os dados anonimizados.⁷² Vale ressaltar, porém, que esse direito se restringe às decisões que afetem os interesses dos titulares, conforme previsto no *caput*, e há, ainda, uma ressalva expressa em relação a “segredos comercial e industrial”, o que pode prejudicar seriamente o escrutínio desses processos decisórios automatizados. Ainda assim, o direito à explicação na LGPD é mais amplo do que aquele previsto no *General Data Protection Regulation* – normativa europeia sobre proteção de dados pessoais.⁷³

Ademais, a LGPD também busca prevenir a discriminação que possivelmente possa ser causada pela automatização. Aliás, consagra o artigo 6º, IX o princípio da não discriminação, pelo qual os dados colhidos não podem ser manuseados de forma discriminatória nem para fins discriminatórios.⁷⁴ A referência à “forma discriminatória” do manuseio de dados contempla a sua utilização por algoritmos, de modo que tal previsão abarca situações decorrentes de falhas presentes unicamente nos algoritmos. *A fortiori*, permite dirimir questões

71 BRASIL (2018), *Op. Cit.*

72 MONTEIRO, R. L., *Op. Cit.*

73 *Ibidem*, p. 14.

74 MAGRANI, E., *Op. Cit.*

que resultam não só de falhas no algoritmo, mas de uma confluência entre sua utilização e a disposição de um banco de dados enviesado,⁷⁵ à exemplo do que ocorreu com a robô *Tay*, inteligência artificial da *Microsoft* criada para interagir autonomamente com pessoas no ambiente virtual (*chatbot*), e que, após algumas horas, passou a emitir comentários machistas, homofóbicos, racistas e antisemitas.⁷⁶

Portanto, constata-se que, de fato, a Lei Geral de Proteção de Dados brasileira se preocupa com riscos da utilização de algoritmos que ultrapassam a proteção de dados, abarcando a proteção contra a discriminação e, em certa parcela, contra a heteronomia. Contudo, ante os diversos riscos mencionados por Latzer *et al.*,⁷⁷ o atual marco regulatório mostra-se ainda insuficiente, sendo necessária sua complementação por outras formas de governança.

Consideração semelhante, inclusive, é consignada na Estratégia Brasileira de Inteligência Artificial, a qual sustenta que, de fato, a LGPD responde a algumas das questões que são colocadas pelo uso da Inteligência Artificial, mas que é necessário ir além, e analisar os demais impactos dessa tecnologia.⁷⁸

A propósito, tome-se como exemplo o risco, mencionado por Frazão,⁷⁹ de que os algoritmos de diversas sociedades empresárias, responsáveis pela fixação dos preços e produtos ofertados, passassem a adotar, automaticamente, práticas de cartelização em determinado mercado. Referida prática não poderia ser evitada pelas tradi-

75 Isso porque, conforme destacado pela própria Estratégia Brasileira de Inteligência Artificial, o viés, nesses casos, pode decorrer tanto dos próprios algoritmos utilizados, quanto das bases de dados usadas para o seu treinamento. BRASIL, 2021B, *Op. Cit.*

76 MÜLLER, Léo. *Tay*: Twitter conseguiu corromper a IA da Microsoft em menos de 24 horas. 2016. Disponível em: <https://www.tecmundo.com.br/inteligencia-artificial/102782-tay-twitter-conseguiu-corromper-ia-microsoft-24-horas.htm>. Acesso em: 15 dez. 2020.

77 LATZER *et al.*, 2015.

78 BRASIL (2021B), *Op. Cit.*

79 FRAZÃO, A. *Op. Cit.*

cionais formas de combate a cartéis (seja pelo Estado, seja pelas próprias sociedades), e tampouco constitui situação abarcada pela LGPD, na medida em que não necessariamente lida com dados pessoais. Nesse âmbito, vale destacar o estudo conduzido por Ezechiel e Stucke,⁸⁰ especificamente sobre o tema:

[...] we are shifting from the world where executives expressly collude in smoke-filled rooms to a world where pricing algorithms continually monitor and adjust to each other's prices and market data. In this new world, there is not necessarily any collusive agreement among executives. Each firm may unilaterally adopt its own pricing algorithm, which sets its own price. In this new world, there is not necessarily anticompetitive intent. The executives cannot predict if, when, and for how long the industry-wide use of pricing algorithms will lead to inflated prices. The danger here is not express collusion, but more elusive forms of collusion. Computers may limit competition not only through agreement or concerted practice, but also through more subtle means. For example, this may be the case when similar computer algorithms reduce or remove the degree of strategic uncertainty in the marketplace and promote a stable market environment in which they predict each other's reaction and dominant strategy. Such a digitalized environment may be more predictable and controllable.⁸¹

80 EZRACHI, A.; STUCKE, M. E. Artificial Intelligence & Collusion: when Computers Inhibit Competition. *University of Illinois Law Review*, Champaign, v. 2017, n. 5, p. 1775–1810, 2018.

81 EZRACHI, A.; STUCKE, M. E., *Op. Cit.*, p. 1782. Tradução livre: “[...] estamos migrando do mundo onde os executivos conspiram expressamente em salas cheias de fumaça para um mundo onde os algoritmos de preços continuamente monitoram e se ajustam aos preços e dados de mercado uns dos outros. Neste novo mundo, não há necessariamente nenhum acordo de colusão entre os executivos. Cada empresa pode adotar unilateralmente seu próprio algo-

Os autores destacam, em seguida, que existem 4 formas de a inteligência artificial ser utilizada de modo a levar a práticas anticompetitivas. A primeira categoria (*Messenger*) diz respeito ao uso da tecnologia meramente para a execução da vontade humana, já existente, de realizar o cartel, de modo a atuar tão somente na implementação e no monitoramento do arranjo. A segunda (*Hub and Spoke*) se refere ao emprego de um mesmo algoritmo de fixação de preço de mercado por diversas sociedades empresárias, que podem ou não ter o intuito de realizar o conluio – ainda que tácito. Já a terceira (*Predictable Agent*) representa a situação em que cada um dos atores econômicos unilateralmente desenvolve máquinas capazes de reagir no mercado de maneira a mudar suas condições e trazer-lhe maior previsibilidade, de modo que a adoção de programas semelhantes por todo o setor pode levar à cartelização, ainda que não haja qualquer acordo nesse sentido. Por fim, a quarta forma (*Digital Eye*), de maior relevância para o presente artigo, concerne também à situação em que as sociedades empresárias desenvolvem e usam algoritmos unilateralmente, mas a estes são dadas tarefas específicas, como maximizar lucros, de modo que passam a executar qualquer estratégia tida como capaz de atingir o objetivo, com base no que aprendem no próprio mercado. Essas duas últimas situações, destaque-se, não poderiam ser evitadas por tradicionais técnicas regulatórias (sejam auto, sejam heterorregulatórias).

No mesmo sentido, encontram-se, por exemplo, os exaustivamente mencionados veículos autônomos. Nos últimos anos, foram noticiados acontecimentos como a ultrapassagem de um sinal verme-

ritmo de fixação de preços, que estabelece seu próprio preço. Neste novo mundo, não há necessariamente uma intenção anticompetitiva. Os executivos não podem prever se, quando e por quanto tempo o uso de algoritmos de precificação em toda a indústria levará a preços inflados. O perigo aqui não é a colusão expressa, mas formas mais elusivas de conluio. Os computadores podem limitar a concorrência não só através de acordos ou práticas combinadas, mas também através de meios mais sutis. Por exemplo, esse pode ser o caso quando algoritmos de computador similares reduzem ou removem o grau de incerteza estratégica no mercado e promovem um ambiente de mercado estável no qual eles preveem a reação e a estratégia dominante um do outro. Tal ambiente digitalizado pode ser mais previsível e controlável.”

lho por um carro autônomo da *Uber*,⁸² e, inclusive, o atropelamento de uma mulher por este nos Estados Unidos.⁸³ Referidas falhas dizem respeito ao algoritmo, ao código em si, e não à coleta dos dados que o alimentam, de modo que o mero seguimento de disposições relativas à proteção de dados não seria capaz de evitar referidos acidentes. Em que pese, neste caso, a tecnologia ser de uso extremamente restrito, esses questionamentos são relevantes para uma provável disseminação dessas formas de inteligência artificial num cenário futuro.

Ainda, conforme mencionado no primeiro tópico deste trabalho, torna-se cada dia mais comum a utilização de *softwares* baseados em inteligência artificial para a realização do próprio *compliance* nas sociedades empresárias. Isto é, utiliza-se de um instrumento intrinsecamente dotado de riscos para a realização de um processo de análise e mitigação de riscos. A título de exemplo, cite-se o programa *clickCompliance*, desenvolvido pela sociedade Ímpeto, o qual é apresentado como um *compliance bot*, e cuja página anuncia:

Com a criação da Lei Anticorrupção, as sanções se tornaram mais severas contra empresas que são beneficiados por condutas ilícitas. Empresas agora são passíveis de responsabilização objetiva. Ou seja, basta ter ligação com alguém envolvido em atividades ilegais para que a empresa sofra punição, mesmo que alegue desconhecimento. Em casos de uma auditoria ou investigação, a empresa pode utilizar os dados do *clickCompliance* para provar que possui procedimentos de Compliance e Integridade. Assim, ela responsabiliza o indivíduo que venha a cometer um crime ou infração e evita punições na Pessoa Jurídica.⁸⁴

82 EXTRA. *Vídeo flagra carro autônomo do Uber furando sinal vermelho*. 2016. Disponível em: <https://extra.globo.com/noticias/celular-e-tecnologia/video-flagra-carro-autonomo-do-uber-furando-sinal-vermelho-20650783.html>. Acesso em: 30 dez. 2020.

83 G1. *Carro autônomo da Uber atropela e mata mulher nos EUA*. 2019. Disponível em: <https://g1.globo.com/carros/noticia/carro-autonomo-da-uber-atropela-e-mata-mulher-nos-eua.ghtml>. Acesso em: 30 dez. 2020.

84 CLICK COMPLIANCE. *O que é clickCompliance?* Disponível em: <https://clickcompliance.com/sobre-nos/>. Acesso em: 04 jun. 2021.

Nesse ínterim, questiona-se se um *compliance* realizado por um *software* seria idôneo e suficiente para eximir uma sociedade empresária da responsabilidade por eventual dano provocado por sua atividade.⁸⁵ Também neste caso, o simples seguimento das disposições relativas à proteção de dados não exaure os inúmeros questionamentos legais que essa prática levanta.

Destarte, percebe-se que há um vácuo regulatório atinente aos algoritmos, no qual mostra-se possível – e provável – o surgimento de riscos para as sociedades empresárias, os quais, porém, não são capazes de dirimir, seja utilizando os tradicionais mecanismos de *compliance*, seja recorrendo aos recentes instrumentos de adequação à proteção de dados.

Latzer *et al.*⁸⁶ propõem, como forma de controlar o enorme poderio dessas tecnologias, e dirimir os riscos por elas criados, uma “governança dos algoritmos” (*governance of algorithms*), em contraposição à atualmente existente “governança pelos algoritmos” (*governance by algorithms*).⁸⁷ Esta governança seria realizada, sob uma perspectiva institucional, pelos agentes econômicos situados num

85 Na página deste mesmo programa há referência, ainda, à utilização da inteligência artificial no mercado financeiro, no qual essa tecnologia teria quatro principais aplicações: em investimentos, em instituições bancárias, na garantia da segurança digital e em softwares de *compliance*. CLICK COMPLIANCE. *4 Usos da Inteligência Artificial no Mercado Financeiro*. Disponível em: <https://clickcompliance.com/inteligencia-artificial-mercado-financeiro/>. Acesso em: 04 jun. 2021.

86 LATZER, M. *et al.*, *Op. Cit.*

87 A governança à qual ora se refere deve ser entendida como mera regulação, não se confundindo com o conceito de “governança corporativa”, com significados e implicações próprias. De acordo o Instituto Brasileiro de Governança Corporativa, “[g]overnança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas”. Disponível em: <https://www.ibgc.org.br/quemsomos>. Acesso em: 30 dez. 2020. Assim, é um instituto que, embora em muitos pontos coincida com o *compliance*, deste se difere: enquanto a governança corporativa se destina mais à resolução de conflitos internos nas sociedades empresárias, o programa de integridade visa a garantir a adequação destas à legalidade e ao interesse público, tendo escopo mais amplo PINHEIRO, (2017). C. DA R., *Op. Cit.*

continuum de centralização, a saber: (1) a regulação por mecanismos de mercado (seja na perspectiva da demanda, seja na perspectiva da oferta); (2) a auto-organização por sociedades empresárias; (3) a autorregulação coletiva por companhias de um setor industrial; (4) a correção, partilhada pelo Estado e as sociedades empresárias; (5) e a regulação pelo Estado por meio da lógica de comando-controle.

Em seguida, os autores desenvolvem uma sistematização na qual associam quais atores nessa estrutura de governança estariam aptos a solucionar quais dos nove riscos elencados, decorrentes da utilização de algoritmos. No que diz respeito à auto-organização por sociedades empresárias, objeto deste trabalho, é destacada sua capacidade de lidar com as questões da manipulação, da censura, da violação do direito à privacidade, da discriminação social, da violação à propriedade intelectual e do abuso do poder de mercado. Estariam, assim, fora do âmbito corporativo interno o risco do enviesamento (*bias*), da heteronomia e do acarretamento de danos sobre as capacidades cognitivas humanas.

Referida auto-organização, que almejasse a redução dos danos associados à utilização de algoritmos, poderia, na visão dos autores, ser realizada por medidas como a adoção de princípios que reflitam o interesse público, a realização de avaliações internas e a implementação de sistemas de ouvidoria. Há, inclusive, menção à implementação, pelo *Google*, de um conselho de ética (*ethics board*) destinado à resolução de questões ligadas à inteligência artificial.⁸⁸ Certamente, uma medida ideal nessa perspectiva de auto-organização apontada pelos pesquisadores seria a expansão das medidas de *compliance* que já são realizadas pelas sociedades empresárias, a fim de lidar também com problemas afetos especificamente ao paradigma dos algoritmos.

Paralelamente, Doneda e Almeida⁸⁹ sugerem que uma governança sobre os algoritmos deve ser centrada em três principais obje-

88 LATZER, M. *et al.*, *Op. Cit.*, p. 39.

89 DONEDA, D.; ALMEIDA, *Op. Cit.*

tivos: transparência, responsabilização – que abarcaria responsabilidade, justiça e devido processo no uso dessas tecnologias – e garantia técnica. Conforme ressaltam os autores, a persecução desses objetivos poderia ser feita, dentre outras formas, pela própria estruturação interna corporativa, com a implementação de órgãos internos destinados a garantir a integridade dos códigos, bem como que estes estejam em *compliance* com o interesse público.

No âmbito nacional, a Estratégia Brasileira de Inteligência Artificial resalta também a importância da implementação de estruturas de governança sobre IA na estrutura empresarial, propondo mecanismos como: a designação de indivíduos ou grupos específicos dentro da empresa para promover a conformidade com princípios ligados a tal tecnologia; a adoção de medidas para aumentar a conscientização interna sobre a necessidade dessa conformidade, inclusive por treinamentos; a implementação de um processo de escalação por meio do qual os membros da organização possam levantar preocupações de conformidade e resolver essas preocupações; a criação de selos, certificações e códigos de conduta corporativos ou governamentais.⁹⁰

Portanto, constata-se que, enquanto não houver uma regulação estatal específica acerca dos diversos dilemas criados a partir da utilização de algoritmos e da inteligência artificial – dispensando o juízo sobre se tal regulação deve ou não ser realizada –, impende-se que as sociedades empresárias adequem seus programas de integridades aos riscos gerados por essas tecnologias, a fim de permitir sua devida mitigação. A propósito, constatou-se que o seguimento das disposições trazidas nas regulações brasileiras até hoje existentes a esse respeito – notadamente, da LGPD – não se mostra como suficiente para dirimir os efeitos perniciosos que a automatização pode gerar. Assim, se, de fato, uma sociedade empresária tem a pretensão de ter um *compliance* efetivo, necessário se faz que se adeque a essas novas exigências.

⁹⁰ BRASIL (2021B), *Op. Cit.*

Todavia, não se ignora que esse processo de submissão dos algoritmos a um maior escrutínio, por parte das próprias sociedades que os utilizam, enfrenta grandes limitações, sobretudo quando centrado numa exigência de maior transparência. Aliás, a opacidade dos algoritmos resulta não só de aspectos técnicos (como a complexidade que, notadamente naqueles munidos de *machine learning*, torna-os incompreensíveis inclusive para seus desenvolvedores), como também de aspectos não técnicos, relacionados à concorrência. Isso, porque, os códigos são propriedades intelectuais, de modo que sua exposição poderia levar a desvantagens competitivas em relação a outras sociedades.⁹¹ Tome-se como exemplo, para ilustrar os limites desse processo, o fato de que, o supramencionado conselho de ética centrado em IA do *Google*, o *Advanced Technology External Advisory Council (ATEAC)*, foi fechado pouco após sua criação, por conta de conflitos internos.⁹²

Conclusão.

Os algoritmos são códigos que se destinam à realização de uma tarefa, produzindo um resultado a partir de dados que lhes são fornecidos. Apesar de divergências no que diz respeito à conceituação técnica, considera-se que são dotados de inteligência artificial quando são capazes de desempenhar uma atividade normalmente atribuída à inteligência humana. Tais recursos têm sido cada vez mais utilizados pelas sociedades empresárias, a fim de facilitar o processo de tomada de decisões.

Entretanto, o recurso a essas tecnologias está associado a uma série de riscos, decorrentes, sobretudo, de sua inescrutabilidade e sua imprevisibilidade, que aumentam de maneira proporcional à comple-

91 DONEDA, D.; ALMEIDA, *Op. Cit.*

92 WAKEFIELD, Jane. *Google's ethics board shut down*. 2019. Disponível em: <https://www.bbc.com/news/technology-47825833>. Acesso em: 25 dez. 2020.

xidade do código utilizado. Conforme destacado, dentre os principais riscos gerados pelos algoritmos estão: a manipulação; a diminuição da variedade de informações; a restrição à liberdade de expressão; o monitoramento e as ameaças à privacidade e à proteção de dados; a discriminação; a violação de direitos de propriedade intelectual; abuso de poder de mercado; efeitos sobre as capacidades cognitivas e o cérebro humano; o crescimento da heteronomia e a perda do controle humano sobre a tecnologia.

Ocorre que não há, ainda, no ordenamento brasileiro, regulação atinente aos algoritmos de forma específica, em que pese a existência de diretrizes de teor voluntarista. Com isso, assume especial importância o *compliance* realizado pelas sociedades empresárias, como forma de mitigar os riscos criados por essas tecnologias, cujo devido tratamento não é feito pelo Estado. Contudo, dada a similaridade da tomada de decisões por algoritmos com a questão do tratamento de dados prevista na LGPD, é possível questionar se a adequação dos programas de integridade a esta Lei seria suficiente para dirimir os problemas supracitados.

De fato, a LGPD abrange considerável parte da problemática atinente à utilização dos algoritmos (como o direito à explicação e a vedação à decisões discriminatórias). Aliás, fornece às sociedades empresárias balizas sólidas para o processo regulatório na proteção de dados, o que acaba por abarcar parte significativa da atuação dos algoritmos sobre seu substrato.

Não obstante, essa legislação não exaure o tratamento que deve ser dado a essas tecnologias, uma vez que existem diversos riscos que não são por ela abarcados. Os algoritmos ainda representam um desafio regulatório, sobretudo porque a questão revela a dificuldade de um adequado encaminhamento normativo sobre a responsabilidade pelos impactos negativos que podem advir da utilização de máquinas para a tomada de decisões. A propósito, o simples seguimento das disposições atinentes à proteção de dados não é capaz de dirimir toda a complexidade – de riscos e desafios legais – levantadas

pela utilização de algoritmos como instrumentos de *compliance*, ferramentas de fixação de preços, objetos de delegação de escolhas (como no caso da *Uber*), entre outros.

Portanto, mostra-se necessário que as sociedades empresárias adotem um *compliance* efetivamente direcionado à mitigação dos riscos associados à utilização de algoritmos, ainda que não haja regulação estatal expressa determinando que assim o façam. Todavia, não se ignoram os desafios atrelados à submissão dessas tecnologias a um maior controle, tendo em vista os diversos interesses conflitantes que envolvem a sua utilização.