MILTON YASUO FUJIMOTO

SEGREDOS DE NEGÓCIOS, PROTEÇÃO DE DADOS PESSOAIS E INTELIGÊNCIA ARTIFICIAL – OS DESAFIOS DO DIÁLOGO

Dissertação de Mestrado

Orientador **Prof. Dr. Balmes Vega Garcia**.

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2023

MILTON YASUO FUJIMOTO

SEGREDOS DE NEGÓCIOS, PROTEÇÃO DE DADOS PESSOAIS E INTELIGÊNCIA ARTIFICIAL – OS DESAFIOS DO DIÁLOGO

Dissertação de Mestrado apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo, na área de concentração de Direito Comercial, sob orientação do Prof. Dr. Balmes Vega Garcia.

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2023

Catalogação da Publicação

Serviço de Biblioteca e Documentação

Faculdade de Direito da Universidade de São Paulo

Fujimoto, Milton Yasuo

Segredo de negócios, Proteção de Dados Pessoais e Inteligência Artificial – Os Desafios do Diálogo; Milton Yasuo Fujimoto; orientador: Balmes Vega Garcia - São Paulo, 2023.

229

Dissertação (Mestrado — Programa de Pós-Graduação em Direito Comercial) — Faculdade de Direito, Universidade de São Paulo, 2023.

1. Decisões automatizadas. 2. Proteção de Dados pessoais. 3. Inteligência Artificial. 4. Segredo de Negócios. I. Garcia, Balmes Vega, orient. II. Título.

Segredos de negócios, proteção de dados pessoais e inteligência artificial – os desafios do diálogo

Dissertação de Mestrado apresentada à Banca Examinadora do programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, na área de concentração do Direito Comercial, sob a orientação do Prof. Dr. Balmes Vega Garcia.

Aprovado em:

BANCA EXAMINADORA

Prof(a). Dr(a). _____

Instituição

Julgamento _____

Assinatura _____

Prof(a). Dr(a). _____

Instituição

Julgamento _____

Assinatura _____

Prof(a). Dr(a). _____

Instituição

Julgamento _____

Assinatura _____

Esta Dissertação é dedicada *in memorian*

para *Hiroe e Masanobou*,

mãe e pai queridos.

Aos filhos amados,

Gustavo e *Mônica*,

razão e inspiração desta viagem.

À parte metade, *Clarice*,

parceira de caminhada.

Aos colegas estudantes,

caminhantes

neste sofrido e querido País.

AGRADECIMENTOS

A Deus, Origem e destino,

pela viagem, minha gratidão.

Ao Professor Balmes,

amigo, que além de lecionar,

orienta e acolhe.

Aos funcionários, com apreço,

também aos demais professores,

pelos cinco anos passados

nestas Arcadas sagradas,

profundamente agradeço!

Aos revisores,

seus olhos afiados

aprimoraram esta Dissertação,

os acertos lhes atribuo,

dos erros me responsabilizo.

Gustavo, Sunahara, Mônica,

Clarice, Edivado e Sebastião,

minha eterna gratidão!

RESUMO

FUJIMOTO, Milton Yasuo. **Segredo de negócios, proteção de dados pessoais e inteligência artificial – os desafios do diálogo**. Dissertação (Mestrado). Faculdade de Direito, Universidade de São Paulo, São Paulo, 2023.

Esta dissertação tem como objetivo avaliar a interação entre a proteção dos segredos comerciais, a privacidade dos dados pessoais e o direito de explicação e revisão das decisões automatizadas, considerando a Lei Geral de Proteção de Dados (LGPD) e o debate em torno da regulação do uso e desenvolvimento da inteligência artificial (IA). O objetivo é apresentar uma perspectiva holística que concilie potenciais conflitos, com foco na explicabilidade das decisões automatizadas. A pesquisa é exploratória e visa sedimentar estudos posteriores sobre a relação entre o direito e as novas tecnologias de informação e comunicação, especialmente a IA. Começa com uma visão geral da transformação digital, aborda as noções básicas sobre a IA e analisa os regimes jurídicos aplicáveis aos temas estudados, culminando no mapeamento do debate em torno do direito à informação, transparência e explicação das decisões automatizadas no tratamento de dados pessoais. Prossegue com uma análise interdisciplinar para identificar os pontos comuns entre esses direitos e interesses em potencial conflito. Para isso, discute as perspectivas internacionais sobre o equilíbrio entre a proteção dos segredos comerciais e a proteção dos dados pessoais, com foco na perspectiva europeia. Também examina a harmonização da estratégia brasileira com os parâmetros internacionais de desenvolvimento de uma IA robusta, transparente e confiável. Em seguida, explora o debate público em torno do marco legal da IA no Brasil. No final, apresenta uma percepção geral sobre a possibilidade de conciliação entre a tutela dos segredos comerciais e a proteção dos dados pessoais. O argumento é que a conciliação passa pela observância do devido processo, o que inclui o contínuo aperfeiçoamento dos mecanismos procedimentais de escrutínio individual e social das decisões automatizadas, em sincronia com os desenvolvimentos das aplicações da IA. Em resumo, esta dissertação oferece uma análise interdisciplinar da relação entre a proteção dos segredos comerciais, dados pessoais e decisões automatizadas no contexto do debate em torno da regulação e regulamentação da IA no Brasil. Sugere que é necessário avançar nas pesquisas sobre os mecanismos de correção da assimetria informacional na tomada de decisões automatizadas, atendendo-se às expectativas plurais da sociedade na definição dos parâmetros normativos aplicáveis no desenvolvimento de uma IA robusta, segura e confiável no País.

Palavras-chave: inteligência artificial, decisão automatizada, segredo de negócios e proteção de dados pessoais.

ABSTRACT

FUJIMOTO, Milton Yasuo. **Trade secrets, personal data protection, and artificial intelligence - the challenges of dialogue**. Dissertation (Master's). Faculty of Law, University of São Paulo, São Paulo, 2023.

This dissertation examines the interaction between the protection of trade secrets, privacy of personal data, and the right to explanation and review of automated decisions, considering the Brazilian Data Protection Law (LGPD) and the debate surrounding the regulation of the use and development of artificial intelligence (AI). The objective is to present a holistic perspective that reconciles these potential conflicts, with a focus on the explicability of automated decisions. The research is exploratory and aims to lay the groundwork for further studies on the relationship between law and new information and communication technologies, especially AI. It begins with an overview of digital transformation, discusses the basic concepts of AI, and analyzes the legal regimes applicable to the topics studied, culminating in mapping the debate surrounding the right to information, transparency, and explanation of automated decisions in the processing of personal data. It then proceeds with an interdisciplinary analysis to identify the common points between these potentially conflicting rights and interests. To do so, it discusses international perspectives on the balance between protecting trade secrets and protecting personal data, with a focus on the European perspective. It also examines the harmonization of the Brazilian strategy with international parameters for the development of robust, transparent, and reliable AI. Next, it explores the public debate surrounding the legal framework for AI in Brazil. Finally, it presents a general perception of the possibility of reconciling the protection of trade secrets and the protection of personal data. The argument is that reconciliation involves the observance of due process, which includes the continuous improvement of procedural mechanisms for individual and social scrutiny of automated decisions, in sync with developments in AI applications. In summary, this dissertation offers an interdisciplinary analysis of the relationship between the protection of trade secrets, personal data, and automated decisions in the context of the debate surrounding the regulation and regulation of AI in Brazil. It suggests that further research is needed on mechanisms for correcting informational asymmetry in automated decision-making, meeting the plural expectations of society in defining the normative parameters applicable to the development of robust, secure, and reliable AI in the country.

Keywords: artificial intelligence, automated decision, trade secrets, personal data protection.

SUMÁRIO

INTRODUÇÃO

Diante dos avanços da Inteligência Artificial (IA), a proteção de dados pessoais tornou-se uma questão crucial que desafia a sociedade contemporânea. Torna-se mais evidente que a opacidade da IA e a preservação do segredo tecnológico colide diretamente com a necessidade de proteger as informações pessoais dos indivíduos. A problemática nos remete a dois clichês que também impulsionaram o estudo: "informação é poder" e "o segredo é a alma do negócio".

Predomina na sociedade digital, o discurso de que a informação é o valor que mais importa. Termos como "mineração de dados" e "novo petróleo"[1] emergem para expressar que, com os avanços tecnológicos, qualquer informação sobre uma pessoa, devidamente processada, adquire significado e valor monetário em um mercado digital. Os agentes econômicos se baseiam no comportamento predominante das pessoas, que muitas vezes estão dispostas a fornecer seus dados em troca de comodidades oferecidas pelos serviços digitais "gratuitos". O crescimento desses negócios leva ao aumento exponencial da demanda por grandes quantidades de dados sobre os clientes e seus padrões de comportamento (visam coletá-los, tratá-los e monetizá-los). Grande parte dessas informações são dados pessoais relacionados a indivíduos identificáveis, reclamando a incidência das leis de proteção de dados pessoais.

Dado o cenário ilustrativo, é importante ressaltar a opinião de estudiosos de que, tanto o segredo de negócios como a proteção de dados derivam originalmente da problemática da privacidade. Estudos realizados por Doneda (2021) revelam que a evolução dessa disciplina enfrentou desafios práticos e conceituais consideráveis, dada a tradição patrimonialista do direito civil. Contemporaneamente, essa área — assim como outras especialidades jurídicas — são desafiadas a lidar com a necessidade de proteger direitos fundamentais diante das novas tecnologias de inteligência artificial e suas implicações sociotécnicas.

Nesse contexto se coloca o desenvolvimento desta pesquisa.

---

[1] SCHOLZ (2018) vê com reservas a analogia que se faz com tanta frequência entre dados pessoais e o "novo" petróleo, alertando que "(...) *É certo que os dados, como o petróleo, são valiosos e ambos impulsionam a economia moderna. Mas para estender qualquer analogia como uma questão de lei e política é imprudente. (...) (1) Dados como o óleo da economia da informação é uma analogia ruim por uma questão de lógica, e (2) dados como o petróleo são enganosos e analogia perigosa aplicada à lei e à política, porque obscurece as principais características do recurso subjacente e sua função na economia. Ao contrário do petróleo, a fonte de dados pode ser rastreada até pessoas individuais, um fato que exige consideração moral e legal*".

Os “desafios do diálogo” entre segredo de negócios e proteção de dados pessoais — tema de fundo deste estudo — não parece dizer muito, tampouco identifica de forma óbvia ou evidente a problemática envolvida em interface com a inteligência artificial (IA). De um lado, a proteção de dados pessoais demanda a ampliação da esfera de proteção dos direitos de personalidade dos titulares e o controle sobre os seus dados; de outro, os segredos de negócio representam o direito legítimo das entidades à tutela da confidencialidade dos conhecimentos por elas considerados valiosos e/ou estratégicos para os seus negócios. Em meio a essa tensão, a transparência emerge como vetor necessário na promoção da confiança no desenvolvimento dessas novas tecnologias.

Assim, pretende-se apresentar uma perspectiva integrada – holística, portanto, – que concilie esses interesses e direitos em potencial conflito, com foco na explicabilidade das decisões automatizadas.

Como ponto de partida, o trabalho aborda panoramicamente o fenômeno da transformação digital. Segue na abordagem das noções básicas sobre a inteligência artificial e analisa os regimes jurídicos aplicáveis aos fenômenos estudados, desaguando no mapeamento do debate em torno do direito de informação, transparência e de explicação das decisões automatizadas, no âmbito do tratamento de dados pessoais, disciplinado na Lei 13.709/2018 (LGPD).

Em seguida, realiza uma análise interdisciplinar, com base na qual busca-se

identificar os “lugares comuns” entre esses direitos e interesses em potencial conflito. Nesse sentido, as discussões internacionais sobre o equilíbrio entre a proteção dos segredos comerciais e a privacidade dos dados pessoais são abordadas a partir da perspectiva europeia.

Examina também a harmonização da estratégia brasileira a determinados parâmetros internacionais de desenvolvimento de uma IA idealmente robusta, transparente e confiável. Na sequência, adentra na análise das “perspectivas regulatórias” para explorar o debate público em torno do marco legal da IA no País.

Nesse ponto de chegada o trabalho apresenta uma percepção geral sobre a possibilidade de conciliação entre a tutela dos segredos comerciais e a proteção dos dados pessoais, com base no aprimoramento dos mecanismos procedimentais de escrutínio individual e social aplicáveis na tomada de decisões automatizadas com apoio da inteligência artificial.

O estudo sugere que é necessário prosseguir nas pesquisas focadas na melhoria dos mecanismos de correção da assimetria informacional na tomada de decisões automatizadas, que - com base nas expectativas plurais da sociedade - definam parâmetros normativos aplicáveis no desenvolvimento de uma IA responsável, ética e explicável no País.

Dentre as hipóteses aventadas a pesquisa se apoia nas sinalizações doutrinárias no sentido de que o diálogo entre o segredo de negócios e proteção de dados pessoais se apoiaria em princípio no tripé confiabilidade-integridade-accountability das novas tecnologias utilizadas no tratamento de dados e que assim deverá a técnica se conformar ao Estado de Direito, e não o contrário[2].

Em perspectivas mais amplas, imbuído de pretensa imparcialidade e neutralidade, busca-se afastar tanto quanto possível, das posições extremadas do determinismo tecnológico e das denominadas posturas solipsistas[3]. Na busca do ideal de equilíbrio — a partir da doutrina referenciada — quer-se enfatizar que na perspectiva jurídica a conciliação há que se dar no âmbito do próprio (devido) processo informacional/comunicativo/dialógico, mediante participação dos respectivos atores envolvidos.

Nesse ponto situa-se o escopo exploratório desta pesquisa de — ao fim — sedimentar percepções em relação à natureza "sociotécnica" das tecnologias em geral e dos "imaginários sociotécnicos"[4] por hipótese alvitrados na construção do marco regulatório da IA. Assume-se que as constatações a serem buscadas na presente dissertação poderiam subsidiar os estudos futuros que desde já se aventa, a partir da ideia de "interações cognitivas" ora pressuposta com base na Teoria dos Sistemas desenvolvida por Luhmann (1998), *apud* Vilas Boas Filho (2009, pp.24-25; 34)[5]. Como se sabe, aludida teoria concebe o Direito como um "subsistema" do

---

[2] "*While the labels remain the same, however, the conceptual foundations for their legitimation and justification are shifting as a greater emphasis on accountability; risk; ethics and the social/political value of privacy have gained purchase in the policy community*". (BENNETT, RAAB, 2017). [Em tradução livre: "Embora os rótulos permaneçam os mesmos, no entanto, os fundamentos conceituais para sua legitimação e justificação estão mudando à medida que uma maior ênfase na responsabilidade; risco; ética e o valor social/político da privacidade ganharam força na comunidade política"]

[3] O termo parece se relacionar com a ideia de um hermetismo sistêmico, aqui infirmada. Para Dhenis Cruz Madeira (2020): "O solipsismo judicial é uma forma de sacralização da atividade judicante. A sacralização ocorre no sentido agambeniano (AGAMBEN, 1995), ou seja, há um obscurecimento da atividade de julgar, tornando-a sagrada e, portanto, inacessível à crítica. Estabelece-se, assim, uma crença de que o julgador, por características que lhes são subjetivas e imanentes, seja capaz de dizer o que é bom, justo, certo e verdadeiro para o restante da sociedade, em especial, para aqueles que sofrerão os efeitos de suas decisões, notadamente, as partes".

[4]

[5] No bojo do estudo acerca da aplicabilidade da teoria dos sistemas, preconizado por Niklas Luhmann, no Direito brasileiro, Vilas Bôas Filho (2009) destaca a importância da compreensão enquanto elemento do processo

sistema social, vocacionado a mediar o processo comunicacional entre os demais subsistemas, com “natural” aptidão para produzir (e reproduzir) soluções normativas frente à problemática decorrente da possível “insinceridade” e “incomunicabilidade”, latentes nas relações “intersistêmicas” e por hipótese reveladas nos diversos atributos qualificativos que se conferem às novas tecnologias de IA, no contexto da sua utilização no tratamento de dados pessoais (v.g., opacidade, invisibilidade, inexplicabilidade, incompreensibilidade etc.)

Essa ideia, que será desenvolvida mais detalhadamente em pesquisas futuras, é corroborada pela possibilidade virtual de traduzir regras lógicas (incluindo regras legais) em regras "técnicas", por meio de comandos binários de sim/não ("01" e "00"), equivalentes à estrutura "bipolar" do Direito (lícito/ilícito), como discutido na doutrina de Tércio Sampaio Ferraz Jr (1980, p. 100). Sua teoria considera o sistema jurídico não apenas como um conjunto de normas ou instituições, mas como um fenômeno de "partes em comunicação", no qual os seres humanos interagem comunicativamente seguindo as regras estabelecidas nesse sistema, constantemente retroalimentado em suas interações comunicativas com outros sistemas.

Embora bom número de pensadores desenvolvam a mesma ideia sob diferentes prismas, a maioria parece desaguar na ideia de promoção do equilíbrio entre a pluralidade de valores consagrados no Ordenamento com os efeitos da utilização da tecnologia para processamento de dados pessoais, seja tal utilização destinada a fins humanitários, mercadológicos ou a qualquer outra utilidade considerada relevante (DONEDA, 2021). Em linha semelhante, HOFFMANN-RIEM (2021, p. 151-152) assevera — ao se discorrer sobre o conceito de Legal Tech e ao relacioná-lo às tomadas de decisão automatizadas com apoio na IA — que há uma imbricação entre regras sociais, regras legais e regras algorítmicas em relação aos quais o Direito sozinho poderá não dar conta de disciplinar.

Segundo o autor em referência, é necessário desmitificar a possível autonomia da IA, uma vez que "mesmo os algoritmos de aprendizagem altamente desenvolvidos devem ser programados por seres humanos antes de poderem se programar independentemente". Com base nessa ideia preliminar, especula-se que, se os "planos de negócios" devem se conformar aos comandos legais aplicáveis ao tratamento de dados pessoais, surge a responsabilidade do detentor/proprietário/desenvolvedor da tecnologia em adotar medidas técnicas e

---

comunicacional normativamente mediado: “(...) a comunicação será concebida por Luhmann como síntese de três seleções: mensagem (*Mitteilung*), informação (*Information*) e compreensão (*Verstehen*). Luhmann enfatiza a necessidade de inclusão da compreensão da compreensão na unidade da comunicação, uma vez que, segundo ele, somente assim a comunicação pode ser concebida como autorreferencial”.

administrativas que garantam a regularidade da atividade. Isso inclui tanto a inserção das prescrições regulatórias (como a explicabilidade algorítmica) no código de máquina, como também a adoção das precauções técnicas consideradas necessárias e suficientes para preservar a confidencialidade dos conhecimentos tecnológicos, se assim for de seu interesse para proteger os segredos comerciais envolvidos.

Em suma, reafirma-se o objetivo principal desta pesquisa, que é apresentar uma perspectiva integrada capaz de conciliar os interesses e direitos em potencial conflito, com foco na explicabilidade das decisões automatizadas. Entre os objetivos específicos, está a análise interdisciplinar da relação entre a proteção de segredos comerciais, dados pessoais e decisões automatizadas no contexto do debate público sobre a regulação e possível regulamentação da inteligência artificial no Brasil.

.

CAPÍTULO 1 - A PASSAGEM DO ANALÓGICO AO DIGITAL: AS TRANSFORMAÇÕES SÓCIOTÉCNICAS E O DIREITO

Transformações sociais e reformulação dos paradigmas no direito parecem caminhar juntos. A economia baseada em dados (ou economia digital) tem sido apontada como decorrência natural da evolução tecnológica e da oferta de soluções inovadoras que surgem a partir do incremento da inteligência artificial, da internet das coisas e do acúmulo sem precedentes de dados e informações. Isso ocorre devido à velocidade e acurácia do processamento proporcionada pela tecnologia da big data. As mudanças alcançam todos os setores da vida e naturalmente desafiam todo o Sistema Jurídico a fornecer respostas consentâneas com o Estado Democrático de Direito (LIMA, 2019) [6].

Trabalhos interessantes nas ciências sociais abordam o tema da evolução tecnológica/transformação digital sob a perspectiva da "opacidade algorítmica". Ao explicar esse fenômeno, oferecem subsídios para a análise na perspectiva jurídica, embora nem sempre se deem conta da conexão direta desses temas com os institutos incorporados no Sistema Jurídico que são objetos da pesquisa aqui empreendida. Essas circunstâncias por si só são suficientes para nos instigar ao estudo.

Por outro lado, a pesquisa preliminar indica que, no âmbito da Academia, o estudo transversal da temática (segredo de negócios/proteção de dados pessoais/tecnologia) navega em um cenário tão profuso quanto disperso. Assim, há que se reconhecer e aproveitar os esforços já empreendidos, notadamente porque a compreensão do fenômeno de imbricação da realidade física-virtual com o mundo digital deve preceder a compreensão do seu exame sobre sua dimensão dialógica com os diversos microssistemas jurídicos, direta ou indiretamente implicados.

No contexto da sociedade da informação, caracterizada principalmente pela intensa utilização e disseminação de Tecnologias de Informação e Comunicação (TICs), o caráter

[6] “O modelo informacional alterou a gramática cultural da Sociedade, encetando novos conflitos ainda isentos de adequada regulamentação jurídica e impelindo uma análise a partir do princípio da dignidade da pessoa humana, dos direitos humanos e fundamentais previstos na maioria das constituições, sobretudo na brasileira, que, nessa medida, forjaram os alicerces éticos e jurídicos para uma investigação da sociedade informacional, enfatizando, portanto, a relevância pela busca por instrumentos adequados para assegurar, em uma perspectiva multinível, a integralidade dos direitos e das garantias à pessoa humana, dentro e fora do ambiente digital”. (LIMA, 2019, [n.p.])

absoluto da autonomia individual parece gradativamente ceder espaço para os interesses difusos da coletividade. A partir da "popularização" dos artefatos tecnológicos de comunicação, verifica-se um ligeiro deslocamento da atenção centrada no bem-estar individual para o bem-estar coletivo. Esse fenômeno potencializa uma crescente demanda pela concretização da função social da propriedade, conforme atribuída na maioria das constituições democráticas, e transforma a informação em bem essencial para a conexão e consequente sustentação do novo modo de ser e de viver na sociedade moderna[7].

A necessidade de adequação da norma à realidade tecnológica é apontada na doutrina jurídica, não sendo possível ignorar a facilidade e rapidez da circulação dos conhecimentos como vetor de ressignificação das antigas concepções de privacidade e confidencialidade[8]. Diante da complexidade do cenário em si, a ideia inicial deste trabalho é voltada ao desvendamento do contexto tecnológico de forma gradativa, pressupondo que sua apresentação em níveis de complexidade crescente facilitará não só a demonstração da conexão temática, mas também a compreensão das nuances da convivência dialógica dos regimes jurídicos no contexto dos objetivos implicitamente enunciados no artigo 20 da LGPD.

Por um lado, existe a necessidade de assegurar, em tese, ao titular de dados acesso às informações a ele relacionadas, por meio da instituição dos requisitos de transparência e de explicabilidade das decisões automatizadas afetas aos seus direitos e liberdades. Por outro lado, é preciso garantir o secretismo dos conhecimentos tecnológicos, reforçando, em benefício do agente controlador, o sentido finalístico da Lei nº 9.279, de 14 de maio de 1996 (Lei de Propriedade Industrial – "LPI"), como estímulo ao desenvolvimento socioeconômico lastreado na inovação tecnológica.

Vale destacar as recomendações da Unesco e da OCDE, que contaram com a adesão do Brasil[9], sobre a Inteligência Artificial ("IA"). Essas recomendações abordam princípios voltados ao desenvolvimento responsável da IA, além de outras menções específicas às políticas públicas e à cooperação internacional. Nenhuma delas parece concordar com a possível "despersonalização" da técnica ou sua desvinculação com a ação humana em suposta sobreposição ao Estado de Direito.

---

[7] Para Castells (2000), a sociedade da informação cria demandas sociais, como a necessidade de participação cidadã, de acesso ao conhecimento e à informação, de conexão e comunicação em tempo real.
[8] FEKETE, 2003, p. 430; e DONEDA, 2021, p. 135.
[9] Portaria MCTI 4.979, de 13 de agosto de 2021 (BRASIL, 2021).

Dentre os princípios e recomendações estabelecidos, destacam-se aqueles que dialogam com os argumentos desenvolvidos neste trabalho:

> - A IA deve beneficiar as pessoas e o planeta, impulsionando o crescimento inclusivo, o desenvolvimento sustentável e o bem-estar.
>
> - Os sistemas de IA devem ser projetados de maneira a respeitar o Estado de Direito, os direitos humanos, os valores democráticos e a diversidade e devem incluir salvaguardas apropriadas - possibilitando a intervenção humana sempre que necessário - para garantir uma sociedade justa.
>
> - Organizações e indivíduos que desempenham um papel ativo no ciclo de vida de IA devem se comprometer com a transparência e com a divulgação responsável em relação a sistemas de IA, fornecendo informações relevantes e condizentes com o estado da arte que permitam: (i) promover a compreensão geral sobre sistemas de IA; (ii) tornar as pessoas cientes quanto às suas interações com sistemas de IA; (ii) permitir que aqueles afetados por um sistema de IA compreendam os resultados produzidos; e (iv) permitir que aqueles adversamente afetados por um sistema de IA possam contestar seu resultado.
>
> - Os sistemas de IA devem funcionar de maneira robusta, segura e protegida ao longo de seus ciclos de vida. Os riscos em potencial devem ser avaliados e gerenciados continuamente.

A ideia desta seção preliminar é apresentar panoramicamente o contexto que informa as questões envolvidas no estudo transversal do segredo de negócios e da proteção de dados. Assim, são brevemente apresentadas as linhas gerais da denominada sociedade da informação em sua imbricação com o *conceito da técnica* contextualizando-o no processo de *transformação digital*.

1.1 SOCIEDADE DA INFORMAÇÃO E DETERMINISMO TECNOLÓGICO

Segundo Werthein (2000), a expressão "sociedade da informação" surgiu no campo das ciências sociais para substituir o conceito complexo de "sociedade pós-industrial" e descrever o novo paradigma técnico-econômico. De acordo com o autor, essa concepção refere-se às transformações técnicas, organizacionais e administrativas que têm como "fator-chave" os insumos baratos de informação, viabilizados pela evolução da microeletrônica e das telecomunicações, ao invés dos insumos baratos de energia presentes na sociedade industrial.

A sociedade pós-industrial, também chamada de "informacional" por Castells (2000), está relacionada à expansão e reestruturação do capitalismo que teve início nos anos 80. Nesse novo modelo, o capitalismo industrial dá lugar a um capitalismo apoiado em novas tecnologias,

que prioriza a flexibilidade e a eficiência, desregulamentando, privatizando e rompendo com o modelo de contrato social entre capital e trabalho. As transformações rumo à sociedade da informação estão mais avançadas nos países industrializados em comparação com os menos desenvolvidos. A tecnologia da informação, como novo paradigma, medeia novas relações entre a economia e a sociedade.

Podemos resumir o cenário conforme Castells (2000), que aponta as seguintes características fundamentais do novo paradigma:

> - **A informação como matéria-prima**: ao contrário do que ocorria no passado, quando a informação era usada para "agir sobre as tecnologias", o desenvolvimento das tecnologias visa permitir que o homem atue sobre a informação, crie implementos novos ou os adapte a novos usos.
>
> - **As novas tecnologias passam a ter grandes impactos na medida em que** a informação passa a integrar todas as atividades humanas, individual ou coletiva, e, nessa esteira, todas essas atividades tendem a ser afetadas diretamente pela nova tecnologia.
>
> - **Predominância da lógica de redes** em todo tipo de relação complexa, cuja implementação material passa a ser viabilizada em qualquer tipo de processo, graças às novas tecnologias.
>
> - **Flexibilidade**: a tecnologia é altamente reconfigurável, possibilitando processos reversíveis e viabilizando modificação por reorganização de componentes.
>
> - **Convergência de tecnologias contínua**, notadamente na microeletrônica, nas telecomunicações, na optoeletrônica, nos componentes computacionais, e, de forma crescente, na biologia. Uma nova trajetória de desenvolvimento tecnológico se abre a partir da nova forma de pensar os processos, cuja aplicação é estendida às distintas categorias, as quais se interligam diversas áreas do conhecimento.

Dado o caráter interdisciplinar deste trabalho, acredita-se que a compreensão de tais características ficaria mais clara se examinada a relação da tecnologia, técnica e ciência.

Segundo Tomasevicius (2018) [10], desde a revolução industrial houve conscientização no sentido de que "nem sempre a humanidade evolui em termos de relacionamentos interpessoais, sociais e políticos", e que "a partir da década de 1950 inaugurou-se uma nova era: a pós-

[10] Essas transformações podem ter sido afetadas pela evolução da eletrônica e da informática. Tomasevicius (2018) menciona a invenção do transístor na década de 1950, seguida anos depois, dos circuitos integrados, dos televisores e dos computadores; a internet, criada igualmente na década de 1950, inicialmente usada com fins militares, depois pela comunidade científica, até a sua transformação, em 1994, em rede aberta irrestritamente, cuja expansão resultou na sua incorporação na vida de grande parte dos seres humanos, alterando rapidamente as telecomunicações, a imprensa e o comércio, e assim contribuindo para que as relações humanas passassem do "analógico" para o ambiente virtual, como se constata, hoje, na verificação do tempo de conexão e "engajamento" de grande parte da população nas redes sociais.

modernidade". Portanto, a compreensão das implicações da tecnologia na sociedade tornou-se um tema central de reflexão das ciências sociais, especialmente do direito, que utiliza a "metalinguagem" especializada da tecnologia como parte de seu discurso, conforme apontado por Doneda (2021, p. 50). Essa visão é compartilhada por Feenberg (2012, p.3), que destaca o papel das novas tecnologias digitais não apenas na condicionamento direto da sociedade, mas também como instrumentos e mecanismos de controle, afetando a privacidade individual. Confira-se:

> Tecnologia não é nem um campo de consenso racional nem uma mera ferramenta na mão de proprietários e gestores. Temos aprendido dos estudos sociais de ciência e tecnologia (STS) que a tecnologia reúne trabalhadores, usuários, até mesmo vítimas, que compartilham o mundo que ela cria. Essa participação nesses mundos tecnológicos moldam a concepção de suas preocupações e canaliza suas atividades. Ainda assim isso não é uma tese determinista. Tecnologia não é uma variável independente, mas é ‘co-construída’ pelas forças sociais que ela organiza e libera.

Seja como ajuste ou como aceleração da rota, nos últimos anos, a humanidade foi desafiada a testar os limites das potencialidades das tecnologias digitais de rede devido ao distanciamento e recolhimento social impostos no contexto da Covid-19. Essas medidas foram adotadas devido à letalidade de um inimigo invisível.

É notório que houve uma repentina (e aparentemente momentânea) migração do mundo físico para o virtual. Esse fenômeno foi viabilizado pela disponibilidade de recursos tecnológicos invisíveis oferecidos pelas plataformas digitais desenvolvidas por grandes intermediadores da internet, que são responsáveis pelo fluxo de dados e informações.

Pode-se arriscar a dizer que a confiança na segurança desses recursos prevaleceu, já que, caso fossem contestados, a manutenção das atividades econômicas e a conexão social necessária à sobrevivência da humanidade seriam impossibilitadas. Em suma, sob esse novo "normal", a vida no planeta seguiu e ainda segue para bilhões de indivíduos, exceto para os milhões que sucumbiram ao novo vírus.

A tragédia humana vivenciada globalmente pode ter aprofundado a percepção geral sobre a interdependência das interações do mundo físico da sociedade com o espaço virtual (HOFFMAN-RIEM, 2021). Ao superar resistências, certamente contribuiu ou contribuirá decisivamente para acelerar a transformação digital em larga escala.

Com efeito, é intuitivo afirmar que mudanças mais profundas ocorrerão em novos

estágios da transformação digital e que maiores serão as inquietações sociais e econômicas já suscitadas em razão do atual estado de opacidade e nível de "digitalização da vida", em razão dos usos[11] - e eventuais abusos – ancorados nessas tecnologias (ditas emergentes) de tratamento de dados pessoais[12] (em especial, *big data*[13], algoritmo[14] e inteligência artificial[15]).

Visões que reputamos realista foram em nossa pesquisa preliminar constatadas em avaliações como as oferecidas por Hoffman-Riem[16], em cuja opinião o uso dos algoritmos digitais pode mudar a "percepção dos eventos reais, pode ser usado para influenciar atitudes, valores e comportamentos, e pode influenciar processos de tomada de decisão sociopolíticos".

---

[11] "A inovação baseada em dados constitui um pilar fundamental nas fontes de crescimento do século XXI. A confluência de diversas tendências, incluindo a crescente migração de atividades socioeconômicas para a Internet e o declínio do custo de coleta, armazenamento e processamento de dados, estão levando à geração e ao uso de grandes volumes de dados – comumente chamados de '*big data*'. Esses grandes conjuntos de dados estão se tornando um ativo central na economia, fomentando novas indústrias, processos e produtos e criando vantagens competitivas significativas. Por exemplo: Nos negócios, a exploração de dados promete criar valor em uma variedade de operações, a partir da otimização das cadeias de valor na manufatura global e serviços de uso mais eficiente do trabalho e relacionamento com os clientes sob medida; A adoção de tecnologias de '*smart-grid*' está gerando grandes volumes de dados sobre padrões de consumo de energia e recursos que podem ser explorados para melhorar a eficiência energética e de recursos. O setor público também é um importante usuário de dados, mas também uma fonte chave de dados. Um maior acesso e uso mais eficaz das informações do setor público (PSI), como solicitado pela Recomendação do Conselho da OCDE sobre PSI, pode gerar benefícios em toda a economia. Um maior acesso e uso de dados cria uma ampla gama de questões políticas, como privacidade e proteção ao consumidor, acesso aberto a dados, habilidades e emprego e medição para citar alguns". (OCDE, 2021).

[12] O conceito de "tratamento de dados pessoais" é aquele atribuído no art. 5º, X, da Lei nº 13.709, de 2018 (LGPD): "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".

[13] O termo *big data* é de definição imprecisa e não taxativa. Em linhas gerais, os autores referem-se ao *big data* como técnicas de captação, armazenamento e processamento de dados em larga escala para extrair novos *insights* ou criar formas de valor, alterando sensivelmente mercados, organizações, as relações entre Governo e seus cidadãos. (MAYER-SCHÕNBERGER; CUKIER, 2014. p. 6)

[14] "Um algoritmo é comumente descrito como um conjunto de instruções, organizadas de forma sequencial, que determina como algo deve ser feito. De maneira alguma é um conceito dependente do uso do poder do computador moderno, pois é possível que alguém crie um algoritmo para auxiliá-lo a se vestir, um algoritmo para pegar o ônibus para o trabalho, para fazer uma receita de bolo, ou para inúmeras outras atividades, já que um algoritmo é nada mais do que uma fórmula na qual tarefas são colocadas em uma ordem específica para atingir determinado objetivo". Thomas Cormen (2013, p. 1) indica que há uma diferença entre um algoritmo qualquer e aqueles que operam em computadores. Computadores, diferentemente de seres humanos, não compreendem o significado de termos como "suficiente", "quase", "ruim" ou qualquer outra palavra que implique uma avaliação subjetiva do mundo ao seu redor. Por essa razão, um algoritmo que determine que um celular reduza a luz de sua tela sempre que "quase não haja mais bateria" é inútil. Um computador é capaz de interpretar porcentagens, mas não de determinar o que "quase sem bateria" significa, a não ser que alguém explicite como fazê-lo. (DONEDA *et al*, 2021, p. 422.)

[15] Nas palavras do prof. Tomasevicius (2018), "A inteligência artificial surgiu concomitantemente com a eletrônica e a ciência da computação na década de 1950. Tem sido aplicada cada vez mais em diversas áreas e potencializou-se com a maior capacidade de armazenamento e tráfego de dados pela Internet. Todavia, especialmente em 2018, ampliou-se a percepção da sociedade para os efeitos positivos e negativos do emprego dessa tecnologia, do ponto de vista não apenas político, mas também dos direitos da personalidade, sobretudo o direito à privacidade".

[16] HOFFMAN-RIEM, 2021, p. 99.

Seja como for, não é possível negar a realidade desnudada pelo neologismo "*on-life*"[17], agora em voga para designar a ideia de que para além da conexão "*off line*" com o "*on line*", a partir da digitalização, a vida parece se deslocar para um mundo "*on-life*", retratando uma nova realidade em que as tecnologias digitais emergentes libertariam as pessoas de tomar decisões, porque os códigos inseridos nos computadores e robôs passariam a substituir as decisões humanas[18].

Do complexo debate, emerge a disputa entre cientistas e engenheiros em relação ao papel da ciência de base, também conhecida como "ciência pura", na inovação técnica. Essas duas correntes extremas discutem a autonomia ou dependência dos especialistas em relação à ciência pura. No entanto, uma "terceira via" mais central inclui opiniões não apenas dos cientistas, engenheiros e indústria, mas também de responsáveis pela política científica, sociólogos, filósofos e historiadores (KLINE, 2011; ALEXANDER, 2012; BUD, 2012, apud SAITO, FUMIKAZU e BELTRAN, 2014).

Nesse contexto de uma quantidade cada vez maior de dados capturados diariamente, com geração e análise automáticas cada vez mais rápidas e precisas, surge o interesse em expandir a pesquisa para entender minimamente o contexto dos desafios regulatórios. Esses desafios envolvem equilibrar o avanço da economia e dos negócios baseados em tecnologia digital de tratamento de dados pessoais com a promessa de proteção dos direitos existenciais básicos[19], garantindo a intimidade e privacidade das pessoas.

A centralidade da tecnologia intensifica a visão simplista do determinismo tecnológico, que afirma que as transformações em direção à sociedade da informação são resultado exclusivo da tecnologia, seguindo uma lógica técnica, neutra e fora da interferência de fatores sociais e políticos. No entanto, ao analisar esse processo dialético presente na evolução das tecnologias em geral e das tecnologias da informação em particular, Castells (2000) destaca que o equívoco está em ignorar a interação complexa entre fatores sociais pré-existentes, criatividade, espírito empreendedor e as condições da pesquisa científica. Confira-se na transcrição:

---

[17] *Idem*.

[18] O contexto é mencionado por Mireille Hildebrandt (2016 *apud* HOFFMAN-RIEM, 2021, p. 25)

[19] Daniel Bucar e Mário Viola argumentam: "Nos conflitos entre um interesse que resguarde uma situação existencial e outro patrimonial parece não haver lugar para a ponderação. A regra, aqui, é da prevalência das situações existenciais, não havendo interesse legítimo para tratamento de dados sem consentimento do seu titular ou sem a existência de outra base legal autorizativa do tratamento que não o interesse legítimo. (...) necessidade de atribuir à atividade econômica suporte ao livre desenvolvimento da personalidade e incessante busca do ordenamento constitucionalizado de colocar *o ser* sobre *o ter*...".

> É provável que o fato da constituição desse paradigma ter ocorrido nos EUA e, em certa medida, na Califórnia e nos anos 70, tenha tido grandes consequências para as formas e a evolução das novas tecnologias da informação. Por exemplo, apesar do papel decisivo do financiamento militar e dos mercados nos primeiros estágios da indústria eletrônica, da década de 40 à de 60, o grande progresso tecnológico que se deu no início dos anos 70 pode, de certa forma, ser relacionado à cultura da liberdade, inovação individual e iniciativa empreendedora oriunda da cultura dos *campi* norte-americanos da década de 60 (...) Meio inconscientemente, a revolução da tecnologia da informação difundiu pela cultura mais significativa de nossas sociedades o espírito libertário dos movimentos dos anos 60. (CASTELLS, 2000, pp.25)

Entende-se, de acordo com Castels (2000), que é inadequada a visão evolucionista do novo paradigma tecnológico presente na "sociedade da informação". Será preciso expandir o olhar para além de um determinismo ingênuo. O autor explica que o determinismo e o evolucionismo simplificam a análise do processo de mudança social, sugerindo uma atitude passiva e contemplativa em relação a esse processo, sem considerar o papel histórico desempenhado pela sociedade no sentido de sufocar ou promover o desenvolvimento tecnológico e suas aplicações sociais, especialmente através da atuação do Estado.

Além disso, acrescenta-se que nada foi diferente em relação às novas tecnologias, cujo avanço foi amplamente resultado da ação estatal. Isso pode ser observado tanto no processo evolutivo das nações industrializadas, que já estão inseridas no nível de desenvolvimento da "sociedade da informação", quanto naquelas que ainda estão inseridas no antigo paradigma industrial mecanicista, cujas potencialidades ainda não foram totalmente exploradas.

No contexto contemporâneo, Morozov (2018, 2020) e Tavares (2021) alertam sobre a ideologia determinística promovida pelo Vale do Silício, que atribui ao solucionismo tecnológico a única e grande alternativa disponível para os formuladores de políticas, ignorando outros modelos tradicionais de solução. Esses autores também ressaltam que mesmo que houvesse disponibilidade de tais modelos, não haveria meios economicamente viáveis para controlar determinadas situações sociais, exceto pelo uso da tecnologia e dos dados dos cidadãos.

Portanto, fica claro que os efeitos da ciência em algum ponto se tornam imprevisíveis, e o Direito não pode permanecer inerte, embora caminhe um passo atrás da evolução científica. Nesse contexto, é necessário lembrar as lições de Niklas Luhmann (2005, p. 41) sobre a confiança sistêmica na sociologia, a partir das quais se infere que a sociedade deposita (ou deve depositar) suas expectativas no funcionamento das instituições jurídicas. Se necessário, o

sistema jurídico deve buscar novos mecanismos de estabilização das expectativas normativas para restaurar a unidade e a confiança (ALMEIDA, 2017).

No entanto, antes de abordar as expectativas da sociedade em relação à ciência e ao Direito, é fundamental compreender a interação entre a linguagem técnica e a jurídica. É nesse sentido que no próximo tópico se pretende examinar especificamente o novo paradigma tecnológico atribuído, no senso comum, à evolução da internet e de suas estruturas.

1.2 O PARADIGMA TECNOLÓGICO: ENTRE O DIREITO E A SOCIOLOGIA

Neste tópico, exploramos aspectos básicos relacionados ao conceito do paradigma tecnológico[20]. É essencial refletir sobre as profundas transformações digitais e o intenso fluxo de informações em redes de computadores interconectados, conhecidos como internet. Essas transformações trazem consigo riscos e benefícios significativos para os direitos e liberdades conquistados pela sociedade.

Dentre as diversas abordagens relacionadas ao termo "paradigma", destaca-se aquela que considera o fluxo do conhecimento e das informações. A invenção da prensa de tipos móveis, atribuída a Johannes Gutenberg (HOFFMANN-RIEM, 2021, p. 1) é considerada um marco tecnológico fundamental nesse contexto. A prensa de tipos móveis teve um impacto cultural transformador na sociedade, promovendo a transição da oralidade para a escrita e influenciando a formação dos direitos de propriedade intelectual (FREITAS, 2021, seção 2.2, pp. 161 passim.).

A literatura demonstra que esse evento foi capaz de libertar os indivíduos de uma forma de dominação ligada a limitações de espaço e tempo. Freitas (2021), com base em diversos pensadores, destaca o papel da prensa na elevação da credibilidade das cópias, estabilizando assim "determinados conhecimentos a partir de unidades autônomas". Esse processo de estabilização contribuiu para o desenvolvimento de uma nova estrutura social e fabril, impulsionada por uma perspectiva tecnológica inovadora.

[20] Inspira-nos pensar no conceito desenvolvido por Thomas Kuhn no tocante aos períodos de normalidade e de crise que acompanham e desafiam as revoluções científicas.

Além da invenção da impressão tipográfica, a digitalização contemporânea, apoiada no avanço da Tecnologia da Informação e Comunicação (TIC), tem sido um importante catalisador de transformações na economia, cultura, política e comunicação, abrangendo praticamente todas as áreas da vida. A digitalização de dados e informações abre caminho para mudanças profundas, como a exaustão dos direitos e a distribuição de conhecimento como serviço, conectando-se a palavras-chave como algoritmos, big data e Inteligência Artificial (IA).

No entanto, antes de prosseguirmos, é importante compreender melhor o processo de transformação tecnológica que ocorreu da passagem do paradigma tecnológico analógico para o digital, da antiga para a realidade contemporânea. Essa compreensão é fundamental para o estudo da proteção de dados pessoais e segredos comerciais no contexto da evolução dos sistemas computacionais de IA[21]

Com o intuito de aprofundar essa compreensão conceitual, exploraremos brevemente os seguintes "paradigmas tecnológicos" específicos: a internet, entendida como uma tecnologia estrutural; a "rede" de suporte da internet, conhecida como infraestrutura física e lógica por onde os dados e informações transitam; e as tecnologias emergentes, em especial *big data*, algoritmos e inteligência artificial[22].

Assim, para além da simples ideia de um somatório de tecnologias, a rede internet – em conjunto com as TICs – passa a ser considerada um “sistema sociotécnico"[23]. Nesse sistema, estão presentes relações de poder ancoradas em dispositivos técnicos e uma arquitetura física peculiar, integrada por protocolos, normas técnicas e estruturas de governança. Essa arquitetura é organizada em camadas, conforme Benkler (2006, 392). A primeira camada é a "camada física", que envolve infraestruturas; a segunda é a "camada lógica", composta por protocolos, algoritmos, padrões e outros procedimentos que traduzem conhecimento humano para que as máquinas possam transmitir, armazenar, computar e processar informações com significado para os seres humanos. Acima dessas camadas, há o que Benkler (2006, p. 392) chama de "camada de aplicações" ou "conteúdo", relacionada ao esquema TCP/IP. Por meio dessas três

[21] RODOTÀ, 2002, p. 564 *apud* DONEDA, 2021, p. 135: “As velhas tecnologias tinham essa vantagem. Eram visíveis, volumosas, rumorosas. Impunham-se com tal materialidade que todos eram constritos a sentir seu peso e, quando pareciam intoleráveis, bastava pedir a alguém para que as suprimisse”.
[22] Essa classificação é baseada no enquadramento analítico do paradigma tecnológico da tecnologia da informação e comunicação (TICs) realizado por Louçã e Freeman (2004), tendo por base o capitalismo contemporâneo. Em grande parte, o desenvolvimento deste tópico apoia-se no estudo de Valente (2018).
[23] *Ibidem*.

camadas, ocorre o fluxo de dados, ainda seguindo os padrões técnicos estabelecidos na década de 1960[24].

Nesse contexto, diversos atores com papéis distintos integram essas camadas e refletem a diversidade de interesses, o que potencializa a disputa em torno da definição das regras de interação no ambiente online. Isso contrasta com a ideia de um "espaço sem lei" atribuído às grandes instituições privadas de tecnologia, que, devido à sua dominância, autoproclamam-se responsáveis por ditar as regras do jogo (ZUBOFF, 2020, p. 122).

Lessig (2006, p. 04) afirma que a construção da arquitetura de rede idealmente seria impulsionada pelo governo e pelo mercado, permitindo uma regulação eficiente para o aperfeiçoamento do controle da rede e dos usuários. Ou seja, garantida a liberdade, o ciberespaço poderia se tornar uma ferramenta de controle eficiente, mas isso dependeria da arquitetura construída". Segundo Lessig, ao invés do Estado, um pequeno grupo de empresários fortes acaba controlando o funcionamento da rede, resultando na necessidade de lutar não pelo governo, mas para garantir a preservação das liberdades essenciais nesse ambiente de controle perfeito (LEMOS, J. G. DE; MENEZES COELHO, 2022).

Atualmente, a internet está novamente no centro dos debates regulatórios, inclusive no Brasil, com discussões sobre a garantia dos direitos humanos e a necessidade de arranjos sociais, culturais e políticos no ciberespaço[25].

Pierre Lévy e Melvin Kranzberg destacam que a tecnologia não é boa nem má, nem neutra[26] A percepção do conteúdo ideológico da tecnologia depende da consideração de seu caráter dinâmico. No perfil estático, ela é vista apenas como uma ferramenta utilitária, obstruindo sua dimensão histórica intrínseca. No perfil dinâmico, podemos observar aspectos relevantes do desenvolvimento tecnológico, como o ciclo virtuoso ou vicioso de realimentação

[24] BRANDÃO, 2020.
[25] Em dissertação de mestrado defendido em 2020, Luiza Couto Chaves Brandão discorre com detalhe sobre o processo em debate (acerca de possíveis novos desenhos institucionais), inclusive sobre os atores dele integrantes. São mencionados diversos Estados soberanos, organizações internacionais – como a Organização Mundial do Comércio (OMC), a União Internacional de Telecomunicações (ITU) ou a Organização Mundial da Propriedade Intelectual (OMPI) – além de entidades privadas (refere-se aos grupos multinacionais *Google*, *Facebook* ou *Amazon*) e de entidades sem fins lucrativos, como a ICANN ou a *Web Foundation*, bem como de setores da sociedade civil organizada e da academia, a exemplo da Rede de Centros em Internet e Sociedade (NoC). (BRANDÃO, 2020)
[26] KRANZBERG *apud* DONEDA, 2021, p. 135.

que a sociedade fornece à tecnologia, envolvendo juízos de valor relacionados às dimensões financeiras, aceitação social, entre outros (Doneda, 2021, p. 55). Esse perfil dinâmico dialoga diretamente com a noção de progresso e carga cultural imanente presente na tecnologia.

Quanto ao Direito, surge a questão de como ele lida ou deve lidar com as preocupações relacionadas às novas tecnologias. De acordo com Erhard Denninger (1991), o homem deve ter uma preocupação permanente com a justiça, e o progresso técnico e científico não tem o objetivo principal de solucionar essas questões[27]. Nessa "sociedade pós-industrial", é necessário examinar as questões relacionadas às novas tecnologias sob a perspectiva da justiça, considerando os valores estabelecidos no ordenamento jurídico.

Com efeito, o desenvolvimento da tecnologia altera e cria relações jurídicas, sendo absorvida pelo Direito. Nas palavras de Bernard Edelman:

> Se por um lado o direito não julga a ciência, por outro ele não tem dúvidas de que ela existe e de que produz efeitos na ordem jurídica. A biologia revolucionou a visão jurídica do homem e da natureza, a informática, aquela dos direitos de autor e dos direitos da personalidade, a pesquisa nuclear renovou a ideia de soberania e de responsabilidade… Dito de outra forma, a evolução das ciências e das técnicas não é indiferente ao direito.[28]

Colocado na ordem do dia, o dinamismo do desenvolvimento tecnológico atrai a atenção do pensamento filosófico e jurídico, juntamente com as projeções futurísticas relacionadas às novas tecnologias, sejam elas otimistas, pessimistas ou pretensamente realistas.

---

[27] As seguintes menções são oferecidas por Doneda (2019, p. 135). Também Denninger (1991. pp. 57-73) se expressa nos seguintes termos: "*Cosa c'è allora di nuovo nei nuovi diritti dell'età tecnologica? Forse la convinzione che il secolare disagio dell'uomo verso la giustizia non sarà risolto neanche dal progresso tecnico e scientifico. Se ne derivasse la coscienza di dover continuamente affrontare questi problemi in maniera responsabile, ciò sarebbe già molto*". [Em tradução livre: "Então, o que há de novo nos novos direitos da era tecnológica? Talvez a crença de que o antigo desconforto do homem com a justiça não seja resolvido nem mesmo pelo progresso técnico e científico. Se a consciência de ter que enfrentar continuamente esses problemas de forma responsável, isso já seria muito]".

[28] A referência, e a tradução, é de Doneda (2021, p. 135): "*Si le droit ne juge pas la science, il n'en demande pas moins que la science existe et qu'elle produit des effets sur l'ordre juridique. La biologie a bouleversé la vision juridique de l'homme et de la nature, l'informatique, celle du droit d'auteur et des droits de la personnalité, le nucléaire a renouvelé l'idée de souveraineté et de responsabilité… Autrement dit, l'évolution des sciences et des techniques ne peut laisser le droit indifferent*.". (EDELMAN, 1999, p. 377 *apud* DONEDA, 2021, p. 50).

Numa abordagem realista, a análise de tendências e projeções tecnológicas é acompanhada do exame dos riscos e oportunidades, oferecendo indicativos de que a sociedade é forçada a tomar posições para o bem ou para o mal das gerações presentes e futuras[29].

É o Direito que fornece a estrutura responsável por disciplinar as escolhas relacionadas à tecnologia[30]. A tecnologia, poderosa e onipresente, desafia o Direito com novas questões[31] que exigem respostas adequadas do jurista, visando assegurar previsibilidade e segurança, com base nos vetores estabelecidos no ordenamento jurídico[32]. Aqui, além de determinar como o Direito deve agir, surge o desafiador problema de "interpretar" a tecnologia e suas possibilidades de acordo com os valores incorporados no ordenamento jurídico[33]. Na difícil tarefa de interpretar o fenômeno tecnológico, é necessário compreender seu papel no processo de transformação social, sendo esse o escopo do tópico que será abordado a seguir.

1.3 TRANSFORMAÇÃO DIGITAL, INOVAÇÃO E DESENVOLVIMENTO

[29] WROBLEWSKI, 1991, p. 197 *apud* DONEDA, 2021, p. 135.
[30] "*Per sua natura, la tecnica non comprende la capacità di scegliere un scopo; questa capacità appartiene pur sempre al diritto, sebbene indebolito dinanzi alla potenza della tecnica*". (MENGONI, 2001, p. 2 *apud* DONEDA, 2019, p. 135).
[31] Doneda menciona diversos autores nessa linha, dentre os quais aponta-se a atribuída a Natalino Irti (1986, p. 4 *apud* DONEDA, 2021, p. 135, nota 111): "*È sicuramente importante la struttura razionale del diritto e dell'amministrazione. Infatti il capitalismo aziendale razionale moderno abbisogna non solo di strumenti di lavoro tecnici e calcolabili, ma anche del diritto calcolabile e dell'amministrazione secondo regole formali, senza cui sono bensì possibile il capitalismo mercantile d'avventura e speculativo, ogni specie di capitalismo politicamente condizionato, non però una azienda privata razionale, con capitale fisso e sicuro calcolo dei costi*.".
[32] "*I nuovi codici, se dá un lato realizzavano un nuovo disegno delle istituzioni, corrispondente all'ordinamento sociale borghese liberale, dall'altro istituivano una tecnologia normativa fondata sulla generalità e sulla sistematicità, adeguata, dunque, ad un'applicazione del diritto più quotidiana e controllabile dal nuovo centro del potere: lo stato. Statualismo, certezza del diritto e prevedibilità, insieme e di pari passo, permetteranno l'attuazione e la stabilizzazione dei nuovi assetti sociali, politici e giuridici*" [Em tradução livre: "Os novos códigos, se por um lado criaram um novo desenho das instituições, correspondentes à ordem social liberal burguesa, por outro instituíram uma tecnologia normativa baseada na generalidade e na sistematicidade, adequada, portanto, para uma vida mais cotidiana e aplicação cotidiana do direito controlável pelo novo centro de poder: o Estado. Estatalismo, segurança jurídica e previsibilidade, juntos e de mãos dadas, permitirão a implementação e estabilização das novas estruturas sociais, políticas e jurídicas."]. Doneda menciona também Natalino Irti (1986, p. 4 *apud* DONEDA, 2021, p. 135), para quem: "*È sicuramente importante la struttura razionale del diritto e dell'amministrazione. Infatti il capitalismo aziendale razionale moderno abbisogna non solo di strumenti di lavoro tecnici e calcolabili, ma anche del diritto calcolabile e dell'amministrazione secondo regole formali, senza cui sono bensì possibile il capitalismo mercantile d'avventura e speculativo, ogni specie di capitalismo politicamente condizionato, non però una azienda privata razionale, con capitale fisso e sicuro calcolo dei costi*." [A estrutura racional do direito e da administração é certamente importante. De fato, o capitalismo corporativo racional moderno precisa não apenas de ferramentas de trabalho técnicas e calculáveis, mas também de leis e administração calculáveis de acordo com regras formais, sem as quais o capitalismo de aventura e mercantil especulativo, todo tipo de capitalismo politicamente condicionado é possível (...).].
[33] DONEDA, *op. cit*., p. 86.

A emergência do mercado digital trouxe consigo desafios para o Direito e conceitos específicos que permeiam o desenvolvimento desta pesquisa. É necessário, neste tópico, além de apresentar os conceitos que serão abordados, expor as principais características da transformação digital.

No início deste milênio, observa-se uma nova "revolução industrial" impulsionada pelo avanço da tecnologia digital, o que gera inquietações nos diversos setores socioeconômicos devido às mudanças em curso. Essas mudanças podem ser comparadas, se não superiores, às ocasionadas pela invenção da prensa tipográfica e da máquina a vapor.

Atualmente, a capacidade de coletar, tratar e gerenciar dados está em constante expansão devido à proliferação de dispositivos, serviços e sensores em toda a economia e sociedade. Esse fenômeno é conhecido por termos como "big data" e "Internet das coisas". Nesse ambiente altamente conectado, os algoritmos não apenas criam valor a partir dos dados, mas também são aprimorados por eles, resultando no "aprendizado de máquina" e no desenvolvimento de inteligência artificial.

A digitalização e a subsequente transformação digital têm o potencial de gerar mudanças ainda inimagináveis em todas as áreas da vida social, da economia à política, da comunicação pública à privada. Funcionalmente, a digitalização não é um processo novo; surgiu da necessidade de lidar com a complexidade e dificuldade de reunir, armazenar e gerenciar dados através de padronização por categorias e estruturação, transformando os dados analógicos e processos em formato legível por computadores, tornando-os acessíveis para gerenciamento algorítmico. Isso torna os dados mais significativos, utilizáveis e valiosos (HOFFMANN-RIEM, 2021, p. 208).

A digitalização consiste na conversão de dados e processos analógicos em um formato legível por máquina, ou seja, são convertidos em códigos binários (“1”s e “0”s), permitindo que sejam lidos e manipulados por computadores.

Em parte, esse conceito já está incorporado ao senso comum, já que muitos estão familiarizados com fenômenos do mercado consumidor de entretenimento, como a introdução de CDs e DVDs, que utilizam dados de forma mais eficiente e produtiva do que seus equivalentes analógicos (HOFFMANN-RIEM, 2021, p. 208). Isso é possível graças ao código

digital, ou seja, os algoritmos que podem interpretar, manipular, processar e transformar qualquer forma de dados digitais, sendo ativados por software em instruções executáveis.

Note-se, em parênteses e à guisa de ilustração, que a incorporação dos termos originados do inglês enseja confusão aos "não familiarizados" em relação aos seus usos, relacionados entre outros com digitalização, digitização e transformação digital[34]. O primeiro termo (equivale ao *digitisation,* no inglês)[35] consiste no ato de converter os dados físicos, analógicos, em dados digitais e poderia ser equiparado a porta de entrada ou ponta do iceberg dos processos de adequação à era digital. O termo digitização (que corresponde ao falso cognato *digitalisation,* no inglês), ainda não incorporado nos dicionários do País, é o processo de adaptação do negócio para uso desses dados, estabelecendo assim as interconexões da atividade com as tecnologias digitais. A transformação digital (*digital transformation*) é entendida como a priorização de todo processo de utilização de recursos tecnológicos no âmbito da organização.

A transformação digital tem os dados como elemento central, embora não seja um processo novo e esteja intrinsecamente ligada à história da computação[36]. Anteriormente, a coleta, o armazenamento e o gerenciamento de dados eram desafiadores, dispendiosos e trabalhosos. No entanto, na era digital, essas dificuldades foram superadas, resultando em processos mais rápidos, precisos e de custo marginal reduzido[37].

Através do estabelecimento de padrões para categorizar, estruturar, vincular e mover dados digitais, eles se tornaram acessíveis ao gerenciamento algorítmico, o que aumentou sua significância, utilidade e valor. Atualmente, a capacidade de adquirir e gerenciar dados está se expandindo rapidamente devido à proliferação de dispositivos, serviços e sensores em todos os setores da economia e da sociedade. Esse fenômeno tem sido descrito com termos como "big data" e "Internet das coisas"[38].

---

[34] Distinção é por nós realizada com base nas observações destacadas no artigo "As diferenças entre digitalização, digitização e transformação digital", publicado em 29.09.2021, na versão virtual (*rectus*, digital) da revista Exame. (CAETANO, 2021)

[35] *Digitizate* (ou *digitisate*, no inglês britânico): to put information into digital form (= into the form of a series of the numbers 0 and 1) so that it can be used by computers and other electronic equipment: **digitalize:** to start to use digital technology such as computers and the internet to do something. (CAMBRIDGE, 2021).

[36] Certamente iniciada por volta de 1847, com a publicação das notas sobre a "Máquina analítica de Babbage" pela Condessa de Lovelace, Ada. (ISAACSON, 2014. Linha do Tempo.)

[37] OCDE, 2023.

[38] OCDE, 2023.

Nesse ambiente altamente conectado, os algoritmos não apenas criam valor a partir dos dados, mas os próprios dados aprimoram os algoritmos, impulsionando o avanço do aprendizado de máquina e o desenvolvimento da inteligência artificial. É uma simbiose em que a disponibilidade e a qualidade dos dados impulsionam a eficiência e a eficácia dos algoritmos, ao passo que o aprimoramento desses algoritmos potencializa a interpretação e o uso dos dados[39].

Não se pode ignorar que com a ascensão da interconectividade e o progresso tecnológico, a coleta, gerenciamento e análise de dados assumem uma função crucial na evolução da sociedade na medida em que estas atividades passam a impulsionar a inovação, viabilizando decisões “inteligentes” e o desenvolvimento de soluções cada vez mais sofisticadas.

Ademais, tudo indica que a pedra angular da transformação digital são os dados, que, sem dúvida, estão se tornando cada vez mais valiosos e relevantes. A interação em ascensão entre dados, algoritmos, objetos e indivíduos resulta em uma economia e sociedade "orientadas por dados". Isto transforma os dados em um recurso valioso, e em ativos negociáveis que sustentam o comércio de outros bens e serviços.

No entanto, essa dependência cada vez maior dos dados e o surgimento de uma economia e sociedade orientadas por eles, também levantam desafios significativos. Implica dizer, é preciso aprender a aproveitar o potencial completo dos dados para promover inovação e produtividade, enquanto se equilibra a necessidade de proteger a privacidade, respeitar a propriedade intelectual e garantir a governança adequada dessas novas tecnologias. Fica claro que a relação entre a transformação digital e o direito é complexa e em constante evolução.

Assim, o direito desempenha um papel fundamental na regulamentação e governança da transformação digital, estabelecendo regras e padrões para proteger os direitos dos indivíduos e da sociedade. As leis relacionadas à proteção de dados, privacidade, segurança cibernética, propriedade intelectual e concorrência seriam apenas alguns exemplos de áreas em que o direito desempenha um papel crucial na transformação digital. Além disso, o direito também deve se adaptar às mudanças trazidas pela transformação digital. À medida que novas tecnologias emergem e transformam as interações sociais e econômicas, tem-se a ideia de que o direito precisa acompanhar essas mudanças e garantir que os princípios fundamentais, como

[39] OCDE, 2023.

justiça, igualdade e proteção dos direitos individuais, sejam preservados no ambiente digital. Isso requer a atualização e desenvolvimento de leis e regulamentos adequados, bem como a colaboração entre os profissionais do direito e especialistas em tecnologia para abordar questões complexas e interdisciplinares.

Em resumo, a transformação digital tem um caráter sócio-técnico e afeta diversos aspectos do direito e da sociologia jurídica. Ela exige a adaptação das leis e regulamentações existentes, levanta novas questões legais e redefine a relação entre o sistema jurídico e a sociedade. A sociologia jurídica pode contribuir para entender e analisar as implicações sociais dessas transformações e suas consequências para a justiça e o sistema legal.

Nesse ponto, ao que depreende do entendimento de Karen Yeung (2016), a regulamentação algorítmica tem um sentido amplo, representando tentativas intencionais de gerenciar riscos ou alterar comportamentos, com vistas a alcançar alguma meta pré-estabelecida.

Segundo a autora, a regulamentação não seria uma atividade exclusiva do Estado. Afinal, corporações como o Facebook também regulam o comportamento dos usuários (o direcionamento, mediante incentivos comportamentais, a um produto ou serviço também equivale à regulação).

Não parece ser novidade alguma afirmar que com o avanço da tecnologia, modelos de negócios – como serviços *online* – passaram a estruturar meticulosamente os dados de suas transações com os consumidores, "personalizando" aspectos dessas interações, com base nas vulnerabilidades detectadas, sabidamente oriundas de vieses comportamentais.

Incentivos como "preço zero"[40] são atrativos para que os usuários de um determinado serviço/plataforma forneçam seus dados e informações em tempo real e os fazem de forma imperceptível na medida que inferências algorítmicas são obtidas a partir de informações aparentemente inofensivas ao senso comum, como sites visitados, tempo despendido, localização geográfica, quantidade, valores e gêneros de produtos adquiridos num determinado dia, o que permite a elaboração de categorias ou padrões comportamentais a partir de perfis

[40] Plataformas digitais valem-se desse atrativo comportamental para atrair o maior número possível de usuários de sorte a monetizar o valor da intermediação dos produtos e serviços comercializados com apoio em sua rede (FRAZÃO, 2021, p. 544).

pessoalizados. Ou seja, a regulamentação é uma atividade intencional e não há como atingir uma meta regulatória à margem das metas determinadas pelo sistema regulatório em questão[41].

Segundo Silveira (2020), a maioria dos textos acadêmicos na área das ciências sociais aborda o algoritmo sob a perspectiva de suas questões críticas, das quais se mencionam as considerações de Zarsky (2016), que levariam à identificação de duas características centrais na governança algorítmica: a automação, ligada à eficiência; a injustiça, decorrente da opacidade. Não se ignoram as observações como a Danaher et al (2017, p.2), que apontam a rapidez, eficiência, abrangência e imparcialidade dos sistemas algorítmicos, na mesma linha das opiniões compartilhadas por Pedro Domingos (2015) e Viktor Mayer-Schönberger e Keneth Cukier (2013).

No que se refere à efetividade e legitimidade da governança algorítmica, Danaher et al (2016) elencam 12 (doze) barreiras que teriam sido identificadas por pesquisadores das áreas de Ciências da Computação, Direito, Biblioteconomia, Filosofia, Geografia, Psicologia, Ciência de Dados, Ciências Política e Sistemas de Informação: Opacidade dos algoritmos; Tecnoutopia (otimismo tecnológico, acriticidade tecnológica); Tecnopessimismo (medo e paralisia diante das possibilidades da tecnologia); Incerteza tecnológica; Capacidade / conhecimento entre tecnólogos; Capacidade dos gestores e servidores públicos; Capacidade dos operadores do Direito; Complexidade jurídica e institucional; Desequilíbrio entre interesses públicos e privados; Governança eficaz versus direitos individuais; Consciência Ética (ou falta dela); Privacidade e consentimento informado).

Em relação as expectativas relacionadas com os impactos dos algoritmos, é sugestivo elencar os temas apontados por Rainie Anderson acerca do trabalho "*Code-Dependent: Pros and Cons of the Algorithm Age"* (LEE, ANDERSON, 2017). O resultado é tabulado em quadros e tabelas as quais valem aqui compilar.

[41] Modelos de negócios centrados na coleta de dados e na formação de perfis de interesse e consumo são executados por sistemas algorítmicos, mediante utilização de algoritmos de aprendizado de máquina, de linguagem natural, de reconhecimento de imagens, e disparos de mensagens e anúncios. (SILVEIRA, 2020)

Quadro 1 - Pós e contras da Era do Algoritmo

Inevitabilidade dos algoritmos	**Tema 1 - Algoritmos continuarão a se espalhar por toda parte** - Os benefícios serão visíveis e invisíveis e podem levar a uma maior percepção humana do mundo - As muitas vantagens de algoritmos são acompanhadas de desafios. **Tema 2 - Coisas boas estão por vir** - As abordagens orientadas a dados para a solução de problemas serão expandidas - Processos de códigos serão refinados e aprimorados: questões éticas estão sendo trabalhadas; - "Algoritmos não precisam ser perfeitos; eles só precisam ser melhores que as pessoas" - No futuro, o mundo poderá ser governado por IA benevolente
Preocupações	**Tema 3 - Humanidade e julgamento humano são perdidos quando dados e modelagem preditiva se tornam primordiais** Programar principalmente na busca de proficias (sic) e eficiências é uma ameaça - Algoritmos manipulam pessoas e resultados e até "leem nossas mentes" - Tudo isso levará a uma sociedade orientada por lógica falha, mas inescapável - Alguns temem que as pessoas possam perder capacidades sofisticadas de tomada de decisão e inteligência local. - À medida que o código assume sistemas complexos, os humanos ficam fora do circuito - As soluções devem incluir o respeito pelo indivíduo **Tema 4 - Existem vieses em sistemas organizados por algoritmos** - Algoritmos refletem os vieses de programadores e conjuntos de dados - Os algoritmos dependem de dados frequentemente limitados, deficientes ou incorretos **Tema 5 - Categorizações algorítmicas aprofundam divisões** - Os desfavorecidos provavelmente serão ainda mais prejudicados de dados corporativos. Eles limitam a exposição das pessoas a um acaso. - **Tema 6 - O desemprego aumentará** - Algoritmos mais inteligentes e eficientes substituirão muitas atividades de trabalho humano. - Alguns buscam um sistema econômico global redefinido para apoiar a humanidade -
Desafios sociais	**Tema 7 - Cresce a necessidade de alfabetização algorítmica, transparência e supervisão.** - Começa com a alfabetização de algoritmos - isso vai além da alfabetização digital básica - As pessoas pedem processos de responsabilização, supervisão e transparência - Muitos são pessimistas quanto às perspectivas de regras e supervisão de políticas

Fonte: Adaptação feita por Sérgio Amadeu Silveira (2020) a partir do Quadro *Seven major themes about the algorithm* (LEE RAINIE; JANNA ANDERSON, 2017, n.p.)

Já as questões éticas relativas à utilização do algoritmo como objeto de políticas públicas são objeto do trabalho de Martin Lodge e Andrea Mennicken (2017, p.2 et seq.), e, para os efeitos desta pesquisa, importa atentar para os pontos positivos e negativos das ações realizadas e controladas por sistemas algorítmicos. É o que evidencia o quadro que a seguir compilamos.

Quadro 2 – Efeitos potenciais da regulação realizada pelos algoritmos

Aleatoriedade artificial aumentada (+) torna os jogos e a corrupção menos viáveis, pois os reguladores podem processar vastos fluxos de informações em vez de confiar em indicadores-chave. (-) Informações complexas e vastas podem reduzir a possibilidade de detectar informações essenciais / a não transparência dos algoritmos significa falta de compreensão dos padrões.	Maior supervisão (+) torna as avaliações baseadas em risco mais prováveis, pois vastos fluxos de informações permitem análises mais refinadas e supervisão sob medida (-) Aumenta substancialmente os poderes de intrusão e vigilância.
Maior rivalidade (+) aumenta a possibilidade de classificação e *benchmarking*. (-) Aumenta a vulnerabilidade a jogos e corrupção por ataques de *bots e malware*.	Maior mutualidade (+) aprimora informações para um envolvimento informado. (-) Aumenta o domínio do "analista de dados" em relação a outros tipos de conhecimento profissional/conversas tendenciosas.

Fonte: Adaptação feita por Sérgio Amadeu Silveira a partir do Quadro1 do texto *The importance of regulation of and by algorithm (*LODGE; MENNICKEN, 2017, p.5.)

Outra constatação importante no plano do discurso é que há um consenso em torno do tema ética. Pode aparecer no discurso empresarial o risco de que a regulação precoce mate o avanço técnico-científico. Isso gera uma contraposição entre regulação e progresso tecnológico. O desenvolvimento dos sistemas algorítmicos, por exemplo, deveria ser regido pela ética e não por legislações, afirmam diversos líderes empresariais. A ética é cultural e historicamente condicionada, e o debate relacionado aos algoritmos ainda não adquiriu relevância (SILVEIRA, 2020). As principais contraposições estão no quadro a seguir.

Quadro 3 – Contraposições discursivas

OPACIDADE	TRANSPARÊNCIA / ACCOUNTABILITY
INESCRUTABILIDADE	EXPLICABILIDADE
AUTONOMIA OPERACIONAL SISTÊMICA	RESPONSABILIZAÇÃO HUMANA
VIÉS E DISCRIMINAÇÃO	JUSTIÇA E REPARAÇÃO
PROFILING E RANKING	AUDITORIA
EFICIÊNCIA E EFICÁCIA	DENÚNCIA DO TOTALITARISMO NEOLIBERAL
SEGREGAÇÃO E EXCLUSÃO DE SEGMENTOS DA SOCIEDADE	TECNOPOLÍTICAS DE INCLUSÃO E DEFESA DA DIGNIDADE SOCIAL

Fonte: Sérgio Amadeu Silveira (2020)

CAPÍTULO 2 - INTELIGÊNCIA ARTIFICIAL: APRENDIZADO DE MÁQUINA E TOMADA DE DECISÃO

As novas tecnologias digitais, ditas disruptivas[42], tem suscitado acaloradas discussões acerca da oportunidade, necessidade de arranjos regulatórios a elas aplicáveis. Ademais, é fato que as inovações disruptivas, de um modo geral, desafiam os Estados a decidir "quando, por que, e até onde regular", e nesse rol se debruça o debate focado na definição de um desenho regulatório adequado a cada caso.

Como é sabido, ao lado das justificativas tradicionais para intervenção estatal é que se coloca o argumento de que a atuação normativa estatal deve se ater na promoção e preservação da inovação, no suporte à livre concorrência, com isso criando condições para que a inovação ocorra. Assim, quer-se alinhar tal linha de entendimento ao pressuposto deste trabalho de que, em princípio, a regulação das novas tecnologias deve concretizar as garantias de segurança do usuário e do respeito às liberdades fundamentais de todos por elas afetados.

Quanto ao "momento de regular", considera-se a doutrina de Baptista, Keller (2016) que sustenta que, embora se afigure prematura a intervenção nos estágios iniciais do surgimento da tecnologia, a regulação poderá se revelar tardia após a consolidação da inovação, "diante da possibilidade de haver resistência à regulação de um mercado já estabelecido" (dilema de *Collingridge)*. No tocante a essa questão, os autores sugerem que o desenho regulatório conjugue ferramentas de regulação "forte" e "fraca", que permitam a adaptação e o aprendizado gradativo, *pari passu* com a mudança do fenômeno tecnológico.

Nessas linhas gerais se encaminha o debate em curso no País com vistas à instituição do respectivo marco legal da IA[43], convergente – ao que parece - no sentido de sugerir a criação

[42] Termo inspirado no conceito de "destruição criativa", registrado pelo economista austríaco Joseph Schumpeter em 1939, para explicar os seus diversos ciclos. Para Clayton Christensen, o termo inovação disruptiva está notoriamente atrelada ao conceito: "É importante lembrar que a ruptura é uma força positiva. Inovações disruptivas não são avanços de tecnologias que fazem bons produtos – melhores; ao contrário, são inovações que tornam os produtos e serviços mais acessíveis e baratos, tornando-os disponíveis a uma população muito maior". (NETO, 2017)

[43] Exposição de motivos da minuta de substitutivo aos Projetos de Lei (PLs) nº 5.051, de 2019, nº 21, de 2020, e nº 872, de 2021, que tem como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil, elaborada pela Comissão de Juristas instituída em 17 de fevereiro de 2022, por meio do Ato do Presidente do Senado nº 4, de 2022, presidida por Ricardo Villas Bôas Cueva e relatada por Laura Schertel Ferreira Mendes, e também integrada por Ana de Oliveira Frazão; Bruno Ricardo Bioni; Danilo Cesar Maganhoto Doneda (*in memoriam*)*;* Fabrício de Mota Alves; Miriam Wimmer;

de ferramentas de governança e de arranjo institucionais de fiscalização e supervisão, com vistas a minimamente garantir segurança jurídica para inovação e o desenvolvimento econômico-tecnológico, com base na previsibilidade e interpretação das normas a serem instituídas com tais finalidades (BRASIL, 2022)[44].

Embora pouco conhecida e reconhecida no senso comum (fora do universo dos desenvolvedores), desde há muito os "especialistas" das mais diversas disciplinas estudam e debatem a IA[45], notadamente após o período na literatura denominado "inverno da IA"[46]. No âmbito da geopolítica internacional, líderes de Estado consideram a IA como tecnologia de natureza estratégica indispensável ao desenvolvimento econômico, político e social, assumindo com esses posicionamentos a adoção de políticas comerciais e industriais, inseridas na corrida tecnológica pelo protagonismo na área (VAINZOF e GUTIERREZ, 2021)

Sartor, Lagioia (2020) situam a IA como ramo da ciência da computação e a classificam, segundo o respectivo escopo: uma "inteligência artificial geral", conhecida como "IA forte"; e uma "inteligência artificial especializada", também conhecida como "IA fraca".

Ao entendimento desses autores, o objetivo buscado pela *inteligência artificial geral*[47] concerne ao desenvolvimento de sistemas de computador que "exibam a maioria das habilidades cognitivas humanas, em nível humano ou mesmo sobre-humano"[48]. De outro lado,

---

Wederson Advincula Siqueira; Claudia Lima Marques; Juliano Souza de Albuquerque Maranhão; Thiago Luís Santos Sombra; Georges Abboud; Frederico Quadros D'Almeida; Victor Marcel Pinheiro; Estela Aranha; Clara Iglesias Keller; Mariana Giorgetti Valente; Filipe José Medon Affonso (BRASIL, 2022).

[44] *Idem*.

[45] No debate global, a IA tem despertado o interesse de especialistas das mais diversas disciplinas. Os economistas se preocupam com o impacto na produtividade e no desemprego; psicólogos e neurocientistas decerto investigam as possíveis consequências na cognição e no comportamento; para os advogados, em princípio, estudar as mudanças no sistema judicial; aos sociólogos interessa observar, descrever e analisar as transformações sociais.

[46] "Em relação à sua trajetória de altos e baixos, não há mais dúvida do sucesso da IA. Uma base interdisciplinar sólida foi construída para a pesquisa de IA de modo que o núcleo original de computação, matemática e lógica foi ampliado com modelos e *insights* de várias outras disciplinas, como estatística, economia, linguística, neurociências, psicologia, filosofia e direito. Resulta daí um leque de aplicações de sucesso, que já ocupam o quotidiano da sociedade: reconhecimento de voz, imagem e face; tradução automática; análise documental; resposta a perguntas; jogos; negociação em alta velocidade; robótica industrial; veículos autônomos; etc." (NILSSON, 2010; O'NEIL, 2016; e PARISER, 2011).

[47] Em relação à Inteligência Artificial auto aprimorável, a humanidade pode se encontrar em uma condição de inferioridade semelhante à dos animais em relação aos humanos. Alguns cientistas e tecnólogos importantes (como Stephen Hawking, Elon Musk e Bill Gates) defenderam a necessidade de antecipar esse risco existencial (PARKIN, 2015 *apud* SARTOR, LAGIOIA, 2020).

[48] "*The future emergence of a general artificial intelligence is already raising serious concerns. A general artificial intelligence system may improve itself at an exponential speed and quickly become superhuman; through its superior intelligence it may then acquire capacities beyond human control.10 In relation to self-improving artificial intelligence, humanity may find itself in a condition of inferiority similar to that of animals in relation to humans. Some leading scientists and technologists (such as Steven Hawking, Elon Musk, and Bill Gates) have*

a *inteligência artificial especializada* teria objetivo menor, como a construção de sistemas satisfatoriamente capazes de desenvolver tarefas específicas que requeiram "inteligência".

A partir dessas considerações iniciais, nos tópicos seguintes, busca-se examinar aspectos básicos que, em princípio, seriam necessários à compreensão do fenômeno tecnológico da IA, em visão "holística", tudo na tentativa de se alinhar ao objetivo inicial deste estudo.

2.1 CODIFICAÇÃO DO CONHECIMENTO E TOMADA DE DECISÃO PELA INTELIGÊNCIA ARTIFICIAL

A inteligência artificial pode ser classificada com base em suas diferentes correntes de desenvolvimento. Essas correntes de desenvolvimento são mencionadas por outros autores, como Garnelo, M. Shanahan (2018), os quais, todavia, destacam os atributos estruturais da IA, classificando-a de IA simbólica (baseada em regras ou conhecimento) e *Machine Learning* (baseada no aprendizado estatístico).

Para esses autores, a IA simbólica considerava a possibilidade de codificar o conhecimento de especialistas humanos em um software e nesta corrente situa-se o chamado "sistema especialista" presente em aplicações comerciais desenvolvidas nas década de 80, inclusive na área da saúde (como é o caso do mapeamento das decisões de diagnósticos fornecidos pelos médicos), os desenvolvedores inseriam, em um software, as regras de

---

argued for the need to anticipate this existential risk,11 adopting measures meant to prevent the creation of general artificial intelligence or to direct it towards human-friendly outcomes (e.g., by ensuring that it endorses human values and, more generally, that it adopts a benevolent attitude). Conversely, other scientists have looked favorably on the birth of an intelligence meant to overcome human capacities. In an AI system's ability to improve itself could lie the 'singularity' that will accelerate the development of science and technology, so as not only to solve current human problems (poverty, underdevelopment, etc.), but also to overcome the biological limits of human existence (illness, aging, etc.) and spread intelligence in the cosmos" [Em tradução livre: "O futuro surgimento de uma inteligência artificial geral já está levantando sérias preocupações. Um sistema geral de inteligência artificial pode melhorar a uma velocidade exponencial e rapidamente se tornar sobre-humano; por meio de sua inteligência superior, pode então adquirir capacidades além do controle humano adotando medidas destinadas a impedir a criação de inteligência artificial geral ou a direcioná-la para resultados amigáveis ao ser humano (por exemplo, garantindo que ele endosse os valores humanos e, de forma mais geral, que adote uma atitude benevolente). Por outro lado, outros cientistas viram com bons olhos o nascimento de uma inteligência destinada a superar as capacidades humanas. Na capacidade de autoaperfeiçoamento de um sistema de IA pode residir a 'singularidade' que acelerará o desenvolvimento da ciência e da tecnologia, de forma não só a resolver os problemas humanos atuais (pobreza, subdesenvolvimento etc.), mas também a superar os limites biológicos da existência humana (doença, envelhecimento, etc.) e espalhar a inteligência no cosmos".] (KURZWEIL, 2012 *apud* SARTOR, LAGIOIA, 2020, p. 5)

especialistas no setor (VAINZOF, 2021) para lidar com o problema específico (porém, limitado) cuja solução era buscada.

Observam, ainda, que as desvantagens desse tipo de IA "*era que o sistema não apresentava capacidade de aprender coisas novas e nem generalizar para problemas as quais nunca tinha visto*".[49] Essa habilidade de aprender e adquirir aprendizado de generalização era feita no âmbito do *Machine Learning*.

Contudo – anotam -, embora essa última abordagem (de aprendizado estatístico) não contasse com a inserção de regras definidas na codificação do software, um conjunto de dados era inseridos no sistema devidamente acompanhado da respectiva "explicação" quanto ao conteúdo e, com base nessa amostragem, o algoritmo era programado e habilitado para criar regras de decisão.

Em suma, enquanto uma corrente da IA preconizava o desenvolvimento de um sistema inteligente, com base numa "representação formal de conhecimentos relevantes", geralmente expresso por meio de uma combinação de regras e conceitos e inseridos pelos humanos, juntamente com algoritmos desenvolvidos para fazer inferências a partir desses conhecimentos; uma outra dedicava-se a desenvolver sistemas baseados em conhecimentos formais e lógicos, mais sofisticados, como linguagens de regras, lógica clássica, lógica modal e descritiva, argumentação formal etc.. E nessa esteira foram desenvolvidos e aplicados modelos computáveis para processos inferenciais - dedutivo, revogável, indutivo, probabilístico, baseado em casos etc. (SARTOR, LAGIOIA (2020).

Conforme relatam Sartor, Lagioia (2020), a IA foi impulsionada a partir da concentração de esforços no desenvolvimento de aplicação de aprendizado de máquina e viabilizado a partir de grandes quantidades de dados, os quais ensejaram uma série de aplicações bem-sucedidas

[49] "Sistemas especialistas – ou seja, sistemas de computador incluindo vastas bases de conhecimento de domínio específico, por exemplo, em medicina, direito ou engenharia, juntamente com mecanismos inferenciais – deram origem a altas expectativas sobre sua capacidade de raciocinar e responder às perguntas dos usuários. Infelizmente, tais sistemas muitas vezes não tiveram sucesso ou tiveram sucesso limitado: eles só podiam fornecer respostas incompletas, eram incapazes de abordar as peculiaridades de casos individuais e exigiam esforços persistentes e caros para ampliar e atualizar suas bases de conhecimento. Em particular, os desenvolvedores de sistemas especialistas tiveram que enfrentar o chamado gargalo da representação do conhecimento: para construir uma aplicação bem-sucedida, as informações necessárias – incluindo conhecimento tácito e de senso comum – tinham que ser representadas antecipadamente usando linguagens formalizadas. Isso provou ser muito difícil e, em muitos casos, impraticável ou impossível". (SARTOR, LAGIOIA, 2020)

em vários setores, como a tradução automática, a otimização industrial, o marketing, as visões robóticas, o controle de movimento etc.

Como se sabe, algumas dessas aplicações tiveram e ainda têm impactos econômicos e sociais significativos. Ademais, conforme observam os autores, nas abordagens de aprendizado, as máquinas recebem métodos de aprendizado, e não exclusivamente conhecimento formalizado; e que, com base em tais métodos, as máquinas poderiam aprender automaticamente, realizando tarefas de forma eficaz, seja coletando ou inferindo informações relevantes a partir dos dados de entrada[50].

2.1.1 *Deep Learning* e redes neurais

A partir das noções sobre o modelo de funcionamento da *Machine Learning* de IA (possibilidade de criação de algoritmos ou programas que ensinem a máquina a desempenhar determinada tarefa a partir de um conjunto de dados) surge o termo *Deep Learning* para expressar a evolução do *Machine Learning*. Mediante a utilização das mesmas premissas, porém com capacidade de processar diferentes espécies de dados, aproxima-se do modo de funcionamento do cérebro humano[51] no tocante ao modo de "aprendizagem", de forma independente[52]; a partir de representações como imagens, sons ou outros tipos de dados viabiliza-se a construção de modelos estatísticos que se destinam à incorporação em algoritmos com vistas ao reconhecimento de padrões aplicáveis - à guisa de exemplos e como referenciais para correlações - na solução de uma generalidade de problemas (PIRES, SILVA, 2017).

A ilustração concreta de utilização dessas técnicas (*Machine Learning* e *Deep Learning*) é dada por Caitlin Mulholland (2020, p. 332):

> Por meio do uso dessas técnicas – *machine learning* e *deep learning* –, uma das aplicações mais interessantes – e, eventualmente, problemática – é a que se concretiza por meio da delegação total de processos decisórios para a IA. Inteligências Artificiais que estabelecem tomadas de decisão podem ser utilizados em uma variedade de modelos, desde os mais simples, como os utilizados em ODRs (*online dispute*

[50] Segundo os autores, Alan Turing já teria teorizado na década de 1950 que uma máquina capaz de aprender alcançaria seus objetivos de maneiras não previstas pelos criadores e treinadores e que haveria casos em que sequer seriam conhecidos os detalhes de seu funcionamento interno. (SARTOR; LAGIOIA, 2020).

[51] Vainzof e Gutierrez (2021) relatam que, embora nas décadas de 1970 a 1990 os pesquisadores estivessem céticos em relação aos métodos estatísticos, notadamente quanto à abordagem conexionista de rede neurais, esses modelos de IA eram disseminados no mercado de aplicações comerciais, que teria atingido sua inflexão nos últimos dez anos em detrimento da IA baseada em regras (que passou a ser denominada GOFAI – "*good old fashioned IA*"), a ponto da abordagem do aprendizado estatístico passar a fazer parte do que hoje se fala em sistemas de recomendação, antifraude e reconhecimento facial.

[52] "(...) quando o sistema aprende a compreender inter-relações, estruturas e arquiteturas sem intervenção humana adicional, de tal forma que pode melhorar seu desempenho de forma independente." (HOFFMANN-RIEM, 2018, pp. 56-59).

> *resolutions*), que substituem as decisões ‘humanas’ em mediação de conflitos, até os utilizados em sistemas de polícia preditiva que identificam potencialidade criminosa e probabilidade geográfica de atividade criminosa.

Naturalmente, a extensão e precisão dessa aprendizagem estarão limitadas à quantidade e qualidade dos dados e informações disponíveis ou utilizados na construção e avaliação do modelo algorítmico, mesmo porque é possível que nem todos os dados necessários para o desenvolvimento/melhoria da aplicação tenham sido registrados digitalmente.

Ao mencionar o caso de avaliação de crédito, Fernando Amaral (2016) indica que um modelo pode classificar um cliente como bom pagador, mas, na prática, pode ocorrer que ele não pague o empréstimo devido a circunstâncias ou atributos que influenciem significativamente a classificação, mas não estejam registrados digitalmente (não "datificados").

Portanto, um evento na vida real pode dificultar o pagamento da dívida, e esses dados ou informações podem não ter sido considerados na classificação desejada pelo modelo. Isso sugere que melhorias podem ser alcançadas através da troca do algoritmo, da seleção de atributos relevantes ou até mesmo da mudança do próprio modelo.

O *Deep Learning*, ou Aprendizado Profundo, é uma subárea do *Machine Learning* que consiste em Redes Neurais Artificiais (CETAX, 2022). Essa área busca simular o cérebro humano em uma máquina computacional de aprendizado, aproveitando o aumento contínuo da capacidade, velocidade e precisão dos modelos computacionais e dos computadores[53].

Além das diversas técnicas utilizadas no aprendizado de máquina, como árvores de decisão, regressão estatística, máquina de vetores de suporte, algoritmos evolucionários e métodos de aprendizado por reforço[54], o aprendizado profundo baseado em redes neurais tem sido implementado com sucesso. Isso se deve, em parte, à ideia de que os padrões podem ser reconhecidos e relacionados a classificações e decisões.

Seguindo essa ideia, as redes neurais são compostas por nós, chamados neurônios, organizados em várias camadas e conectados por links, emulando alguns aspectos do sistema nervoso humano. Esses neurônios artificiais recebem e transmitem informações, assim como

[53] *Idem.*
[54] AMARAL, 2016, cap. 7.

os neurônios biológicos, e os dados são amplificados ou reduzidos ao cruzar os links de entrada, de acordo com os pesos atribuídos a eles[55].

Esse quadro também é descrito por Sartor e Lagioia (2020), que afirmam que o neurônio realiza cálculos nos dados de entrada. Se o resultado atingir o limite do neurônio, ele é ativado e envia sinais para os neurônios conectados ou para fora da rede. Essa ativação começa nos nós que recebem entradas externas e se espalha pela rede. Durante o treinamento, a rede informa a si mesma se suas respostas estão corretas ou erradas. Se uma resposta estiver errada, um algoritmo de aprendizado atualiza os pesos das conexões, para que, da próxima vez que a mesma entrada for apresentada, a rede possa fornecer a resposta correta.

Portanto, é importante entender que a inteligência artificial, ao se valer de métodos estatísticos, depende do fluxo contínuo de dados (*Machine Learning* e *Deep Learning*) como principal matéria-prima para aprendizado. Isso explica a demanda comercial e dos serviços de redes sociais pela total digitalização da vida, que permite a geração diária de enormes quantidades de dados, servindo como fonte de conhecimento para os algoritmos aprenderem (VAINZOF, GUTIERREZ, 2021) [56].

Após esse "processo de treinamento", o modelo estará apto a generalizar seu aprendizado para novos dados que ainda não existiam na etapa de treinamento. Isso envolve buscar correlações e gerar previsões para a realização da tarefa especificada, conceitos que serão explorados posteriormente, como "aprendizado supervisionado", "aprendizado não supervisionado" e "aprendizado por reforço"

2.1.2 Aprendizado supervisionado, aprendizado não supervisionado, aprendizado por reforço

Como observado, um algoritmo pode "aprender" a alcançar um objetivo a partir de um grande volume de dados, incorporando experiências para melhorar seu desempenho à medida que reconhece padrões aplicáveis a situações gerais não identificadas anteriormente. Isso é conhecido como "Aprendizado de Máquina Supervisionado", em que tentamos prever uma

[55] *Idem*.

[56] Os autores exemplificam, nesse caso, a evolução na área de diagnóstico médicos por imagem, cuja evolução decorreu da quantidade de dados hoje disponíveis, em comparação àquela existente 20 anos antes. Ressaltam também que existem diferentes estratégias de aprendizado e que diferentes algoritmos podem ser utilizados a depender da situação, entre os quais mencionam os de regressão linear, regressão logística, redes neurais e até a *deep learning* propriamente dita, cujas distinções demandariam estudos mais aprofundados, ora inviabilizados em razão da limitação do escopo deste ensaio.

variável "dependente" com base em variáveis independentes, anotando os dados em relação às respostas ou classes a serem previstas[57].

No entanto, essa abordagem não é aplicável a todos os tipos de problemas, especialmente quando é difícil ou impossível coletar e anotar os dados necessários, como no caso da perfilização de clientes. Como podemos reconhecer o padrão de compra de um consumidor em compras sequenciais de vinho e queijo, carne e carvão, leite em pó e fraldas? Como podemos decidir como rearranjar esses produtos nas prateleiras para melhorar as vendas? E como determinamos quantos perfis existem ou a qual perfil cada compra efetuada pertence, se não temos dados anteriores ou padrões de correlação baseados em dados anteriores? [58]

Nesses casos, a tarefa do desenvolvedor é criar programas de computador capazes de elaborar e descobrir perfis sem depender de dados previamente anotados. Nesses casos, recorremos ao método de "aprendizado não supervisionado", no qual o algoritmo recebe um conjunto de dados "não rotulados" e suas correspondentes saídas corretas, permitindo que ele alcance a saída desejada e faça ajustes nos parâmetros até atingir um limiar aceitável previamente determinado[59].

Uma terceira abordagem de aprendizado de máquina é chamada de "aprendizado por reforço", na qual a máquina tenta aprender a melhor ação a ser tomada com base nas circunstâncias em que essa ação será executada. Esse conceito tem origem na psicologia, especialmente no behaviorismo de B.F. Skinner[60]. Essa abordagem é aplicada em ambientes de incerteza em relação aos eventos futuros, e o modelo incorpora a possibilidade de mudanças com base em estímulos de recompensa ou punição dados a um agente em decorrência de uma determinada decisão ou de seus efeitos.

Por meio de experimentações repetidas, espera-se que o agente aprenda, associando esses estímulos aos resultados e evitando ações que levem a punições ou recompensas menores, escolhendo aquelas que proporcionem maiores e melhores recompensas dentre as opções

[57] O item “salário” seria uma variável dependente em relação ao item “anos de carreira, formação e idade”, variáveis independentes. Dentre as técnicas mais conhecidas para resolver problemas de aprendizado supervisionado estão regressão linear, regressão logística, redes neurais artificiais, máquinas de suporte vetorial (ou máquinas *kernel*), árvores de decisão, k-vizinhos mais próximos e *bayes* ingênuo.
[58] VAINZOF; GUTIERREZ, 2021.
[59] *Idem*.
[60] A ideia de recompensas e punições do treinamento de pombos de Skinner teria sido usada para conduzir mísseis na Segunda Guerra Mundial. (HONDA; FACURE; YAOHAO, 2017).

apresentadas pelo ambiente em cada situação[61]. Essa ideia de processo de aprendizado permite que a máquina observe um conjunto de cenários futuros possíveis.

Essa abordagem pode ser aplicada em diferentes contextos. Por exemplo, ao invés de treinar cães, podemos construir uma máquina para montar carteiras de investimento no mercado financeiro, combinando ativos com base no retorno financeiro da carteira anterior e na evolução do mercado[62]. Em um veículo autônomo, as decisões são tomadas com base no cenário observado e o sistema recebe "recompensas negativas" quando ocorrem colisões, estimulando-o a contornar obstáculos após várias etapas[63].

Podemos adicionar níveis adicionais de complexidade a partir desses exemplos, como aumentar a distância em que o estímulo (por exemplo, um pedaço de carne) é colocado ou combinar outras ações e situações para explorar mais possibilidades, usando reforços positivos ou negativos e testando diferentes combinações em diversas situações[64]. Essa abordagem pode ser facilmente aplicada ao contexto financeiro, levando em consideração o grau de aversão ao risco de um agente econômico, ou seja, o quanto ele está disposto a correr mais riscos em busca de retornos maiores ou menos riscos para obter um retorno menor, porém mais seguro[65].

Portanto, fica evidente que a capacidade desses sistemas de interagir com o ambiente e extrair aprendizados dessas interações constitui a principal característica da inteligência artificial como a conhecemos hoje. Esse processo contínuo e potencialmente ilimitado de autoaprendizagem tende a aumentar cada vez mais a complexidade das interações desenvolvidas por esses sistemas "autônomos" (TEPEDINO, SILVA, 2021). Consequentemente, surge a observação de Hoffmann-Riem (2021, p.14) de que a programação humana, que antes era necessária para programar algoritmos e sistemas algorítmicos complexos, está se tornando cada vez menos relevante no campo do aprendizado de máquina.

Inicialmente ancorados em passos lógicos individuais, esses sistemas estão se tornando gradualmente indetermináveis em um cenário de interações contínuas, dificultando sua compreensão, inclusive para os programadores. É nesse ponto que reside, segundo o autor mencionado, a abordagem do problema da falta de controle humano, que é inerente aos desenvolvimentos futuros de programas autônomos, e isso implica na perda de transparência e

---

[61] *Idem*.
[62] *Idem*.
[63] VAINZOF; GUTIERREZ, 2021.
[64] *Idem*.
[65] *Idem*.

rastreabilidade dos processos, inclusive para os próprios programadores (HOFFMANN-RIEM, 2021, p.14).

Além dessas dificuldades de supervisão ou intervenção humana, o autor destaca a possibilidade de ocorrerem desenvolvimentos equivocados, catastróficos ou resultados omitidos. Isso justifica os alertas sobre o uso ilimitado da IA, inclusive por parte dos mesmos atores que protagonizaram seu desenvolvimento e a utilizaram intensamente em suas atividades comerciais[66].

Em resumo, é importante destacar a visão dos especialistas, que em sua maioria concordam que a Inteligência Artificial tem uma natureza complexa, como observado por VAINZOF e GUTIERREZ (2021). Eles argumentam que a IA não deve ser entendida como uma tecnologia específica, única ou exclusiva, mas como uma área de conhecimento que se materializa em diversos modelos por meio de diferentes técnicas e algoritmos, resultando em modelos cada vez mais complexos, o que os torna difíceis de entender, de explicar, de governar e de regular.

2.2 Decisões automatizadas por sistemas de inteligência artificial

Os sistemas de IA, associados ao uso de tecnologias big data e apoiados em modelos matemáticos e estatísticos, permitiram o processamento eficiente de grandes volumes de dados pessoais. Eles também possibilitaram a identificação de padrões comportamentais consistentes que seriam difíceis ou até impossíveis de serem detectados por humanos sem o auxílio dessas ferramentas técnicas.

Uma das principais características da IA é a capacidade de automatizar a tomada de decisões sem intervenção humana. No entanto, essa automatização levanta várias questões e discussões, como: quais tipos de decisões podem ser delegadas a máquinas; quais decisões exigem necessariamente intervenção humana; se os indivíduos têm o direito de solicitar a revisão de decisões totalmente automatizadas com base no tratamento de seus dados pessoais;

[66] Menção é feita em alusão ao cofundador da *PayPal* e proprietário da *Tesla*, Elon Musk, o fundador da *Microsoft*, Bill Gates, ou o cofundador da *Apple*, Steve Woznak. São referenciadas obras especificamente alarmantes escritas por Bostrom, “Superintelligence” (2013) e Tegmark, “Life 3.0” (2017); Harari, “Homo Deus” (2017); Colwin, “Breakdown” (2018). (HOFFMANN-RIEM, 2021, p. 75).

se é relevante identificar o direito ou interesse afetado como consequência da decisão, entre outros. Essas polêmicas também englobam decisões relacionadas à definição do perfil pessoal, profissional, de consumo, crédito e qualquer aspecto da personalidade dos titulares de dados.

Em geral, dependendo do grau de riscos ou impactos causados aos indivíduos, são comumente utilizadas ferramentas para revisão dos processos automatizados de tomada de decisão. Um exemplo disso são as companhias aéreas que utilizam tecnologias de reconhecimento facial para verificar os cartões de embarque e os funcionários da alfândega que fazem triagem de entrada de indivíduos no País. Essas decisões podem ser consideradas significativas, pois afetam a liberdade de locomoção dos indivíduos.

Outro exemplo é o caso do anúncio direcionado, onde uma oferta é apresentada de forma incorreta ao jovem profissional, sugerindo um produto ou serviço destinado a aposentados. Esses exemplos ilustram o uso da IA em decisões automatizadas que podem ter, ou não, impactos significativos na vida dos indivíduos, indo além das técnicas de personalização e moderação de conteúdo em redes sociais e mecanismos de busca.

Embora a IA tenha passado por um período de "inverno", tanto o presente quanto o futuro se apresentam promissores para o desenvolvimento dessas técnicas [67]. Tanto assim é que os termos e a gramática utilizados na tecnologia da IA, como internet das coisas, Machine Learning, Realidade Virtual e robôs de inteligência artificial como o "Chat GPT", desenvolvido pela OpenAI, estão cada vez mais difundidos [68].

Diante desses exemplos, fica evidente a importância do direito de revisão e explicação das decisões tomadas por sistemas automatizados. Portanto, busca-se compreender melhor esse fenômeno tecnológico, considerando suas implicações sociotécnicas.

No entanto, além das oportunidades oferecidas pela IA, é importante analisar os riscos relacionados às decisões que afetam indivíduos e grupos sociais, sob a perspectiva da justiça e dos direitos fundamentais, como o princípio da "não discriminação". Esse princípio é relevante nas questões relacionadas à elaboração automatizada de perfis e às possibilidades de influência e manipulação decorrentes dessas decisões.

[67] V. Seção 2.
[68] LOPES, 2023; e OPENAI, 2023.

Para compreender melhor esses riscos, é necessário analisar os elementos integrantes dos ciclos de previsão e avaliação preliminar dos dados pessoais. A previsão, nesse contexto, envolve saltar de características conhecidas de um caso-base (preditores ou variáveis independentes) para um atributo desconhecido (variável dependente ou rótulo) [69]. Modelos capturam aspectos gerais dos contextos considerados, permitindo a conexão entre os valores dos preditores e alvos.

Atualmente, a construção desses modelos de aprendizado de máquina é cada vez mais confiada às máquinas, como parte das abordagens de *Machine Learning* e *Deep Learning*. As máquinas descobrem as correlações probabilísticas entre os preditores e alvos, possibilitando previsões mais precisas e avaliações automatizadas, graças ao grande conjunto de dados disponíveis.

A previsão decorrente é baseada em modelos que capturam aspectos gerais dos contextos em consideração, o que possibilita a conexão com os valores dos preditores e alvos respectivos. Num modelo na área médica, é possível conectar os sintomas a doenças; um modelo psicométrico possibilita associar o comportamento *online* (por exemplo, amigos, postagens e curtidas em uma rede social) com a atitudes psicológicas etc.[70]

Ocorre que, embora tais modelos possam ser criados por humanos (que formulam as regras e conceitos no modelo, ou mesmo no caso dos sistemas especialistas baseados em regras), para além da aplicação do modelo, a própria construção (no caso do modelo de aprendizagem) está sendo cada vez mais confiada à máquinas.

Nessas abordagens (*Machine Learning* e *Deep Learning*), as máquinas descobrem as correlações probabilísticas entre os preditores e alvos para aplicá-las para fazer previsões em casos seguintes. Da combinação dessas técnicas com a grande massa de dados e poder de

---

[69] Especificamente em relação ao termo técnico "rótulo", constata-se sua utilização com significados aparentemente similares (categorizar, classificar e agrupar dados) na área de engenharia da automação. É o que se depreende do resumo que em parte se transcreve: "Problemas de classificação multirrótulo (MLC) relacionam uma instância a um ou mais rótulos, este tipo de problema está presente em nosso dia a dia, desde a classificação do tema de artigos de jornais, até classificação funcional genômica. Dois principais métodos são estudados para a resolução de problemas de MLC, o primeiro é o *algorithm adaptation*, onde os algoritmos tradicionais de classificação binária e multiclasse são adaptados para considerar N rótulos, outro método é o *problem transformation*, onde é feito a transformação do problema possibilitando a solução através de abordagens já existentes. Neste trabalho, será utilizado este segundo método fazendo a transformação de MLC para HMC (classificação multirrótulo hierárquica), com o objetivo de capturar melhor as relações entre as classes". (PELENCE, 2022, p. 68).

[70] SARTOR; LAGIOIA, 2020, p. 28.

computação (v. *big data*), tornou-se possível aumentar o nível de acurácia dessas previsões e avaliações automatizadas, dada a disponibilidade desse grande conjunto de dados[71].

Por exemplo, no contexto da publicidade direcionada, os preditores podem ser baseados em registros que relacionam características e comportamento dos consumidores a suas respostas aos anúncios[72]. Em avaliações de candidatos a emprego, os registros focam nas características de trabalhadores anteriores e seu desempenho profissional[73]. A previsão da reincidência de um infrator pode ser feita com base em registros que combinam características de infratores anteriores com dados sobre sua reincidência[74]. A qualidade de crédito de um interessado pode ser prevista com base em registros que relacionam características de mutuários anteriores com dados ou avaliações de sua qualidade de crédito. Da mesma forma, diagnósticos médicos e tratamentos personalizados podem ser embasados em registros de pacientes anteriores[75].

Assim, ocorre um ciclo vicioso em que a IA precisa aprender a partir da análise de uma grande quantidade de dados, o que estimula a coleta contínua de dados[76]. A disponibilidade de dados eletrônicos, a digitalização massiva e a infraestrutura global de processamento de dados interconectada contribuem para essa retroalimentação[77]. No entanto, o desenvolvimento da IA e sua convergência com o big data também podem trazer graves riscos para indivíduos, grupos e sociedade em geral, devido a seu uso inadequado por agentes econômicos e pelo poder público[78]. É necessário, portanto, implementar ações efetivas para controlar estruturas de

[71] *Idem.*
[72] *Idem.*
[73] *Idem.*
[74] SARTOR; LAGIOIA, *op. cit.*, p. 28 e ss.
[75] *Idem.*
[76] MAYER-SCHÖNBERGER; CUKIER, 2013.
[77] Por exemplo, enormes quantidades de dados são coletadas a cada segundo por computadores que executam transações econômicas (como em *e*-comércio), por sensores monitorando e fornecendo entrada para objetos físicos (como veículos ou dispositivos domésticos inteligentes), pelos fluxos de trabalho gerados por atividades econômicas e governamentais (como bancos, transporte ou impostos etc.); por dispositivos de vigilância (como câmeras de trânsito ou sistemas de controle de acesso); e sistemas que suportam atividades não relacionadas ao mercado (como acesso à internet, busca ou redes sociais). (SARTOR; LAGIOIA, 2020, p. 30)
[78] Os governos teriam oportunidades de usar a IA com fins políticos e administrativos legítimos (na melhoria da eficiência, da qualidade dos serviços etc.), mas também para manipular o comportamento dos cidadãos, restringindo liberdades individuais ou interferindo no processo democrático. No âmbito privado, a IA pode impactar o nível de empregos em setores em que o humano corra o risco de perder a "corrida contra a máquina". (McAFEE; BRYNJOLFSSON, 2011 *apud* SARTOR; LAGIOIA, 2020).

poder[79], abusos[80] e atividades ilegais[81] viabilizados pela IA e *big data*[82].

2.3 INTELIGÊNCIA ARTIFICIAL E A CLASSIFICAÇÃO SOCIAL: ENTRE A PERSONALIZAÇÃO E A PERFILIZAÇÃO

No contexto do tópico anterior, são revelados aspectos cruciais da Inteligência Artificial (IA), especificamente relacionados à aprendizagem de máquina. Isso consiste na capacidade de combinar diferentes valores e estabelecer correlações entre características, atitudes e comportamentos de indivíduos, a fim de tratá-los de maneira igual ou diferenciada com base em previsões diferentes. Essas abordagens podem afetar interesses e direitos, seja de forma positiva ou negativa. Conforme resumido por SARTOR e LAGIOIA (2020, p. 28):

> Uma nova dinâmica de estereótipos e diferenciação acontece. Por um lado, os indivíduos cujos dados suportam a mesma previsão serão considerados e tratados da mesma forma. Por outro lado, os indivíduos cujos dados suportam previsões diferentes, serão considerados e tratados de forma diferente. Essa equalização e diferenciação, dependendo dos domínios em que é usado e dos propósitos a que se destina, podem afetar positiva ou negativamente os indivíduos em questão, mas

[79] A IA propicia concentração de riquezas apoiada nos modelos "o vencedor leva tudo". Essas posições de monopólio tendem a prevalecer, graças ao efeito de rede (os usuários preferem redes maiores), aliado a economias de escala (possibilitadas pela automação) e acesso exclusivo ou preferencial a dados e tecnologias. Certos abusos de poder podem ser incentivados pelo fato de muitas empresas de tecnologia – como as principais plataformas que hospedam conteúdo gerado pelo usuário – operam em mercados de dois ou vários lados. Seus principais serviços (pesquisa, gerenciamento de redes sociais, acesso a conteúdo etc.) são oferecidos a consumidores individuais, mas o fluxo de receita vem de anunciantes, influenciadores e formadores de opinião (por exemplo, em campanhas políticas). Isso significa não apenas que qualquer informação útil para publicidade direcionada será coletada e usada para esse fim, mas também que as plataformas empregarão qualquer meio para capturar usuários, para que possam ser expostos a anúncios e tentativas de persuasão. Isso pode levar não só a uma recolha massiva de dados pessoais sobre os indivíduos, em detrimento da privacidade, mas também a uma influência generalizada no seu comportamento, em detrimento da autonomia individual e dos interesses coletivos. Além disso, algoritmos orientados ao lucro podem se combinar para avançar estratégias anticompetitivas, em detrimento não apenas dos concorrentes, mas também dos consumidores. (SARTOR; LAGIOIA, 2020, p. 40)

[80] No âmbito do poder da IA, pode ser usado para perseguir interesses econômicos de maneiras prejudiciais aos indivíduos e à sociedade: usuários, consumidores e trabalhadores podem estar sujeitos à vigilância generalizada, controlada em seu acesso à informação e oportunidades, manipulados em suas escolhas.

[81] Sistemas de IA e *big data* podem estar sujeitos a ataques cibernéticos (projetados para desabilitar infraestrutura crítica ou roubar ou manipular grandes conjuntos de dados etc.), e podem até ser usados para cometer crimes (por exemplo, veículos autônomos podem ser usados para assassinatos ou ataques terroristas, e algoritmos inteligentes podem ser usados para fraudes ou outros crimes financeiros).

[82] Assim como a IA pode ser mal utilizada pelos atores econômicos, também pode ser mal utilizada pelo setor público. Os governos têm muitas oportunidades de usar a IA para fins políticos e administrativos legítimos (por exemplo, eficiência, economia de custos, serviços aprimorados), mas também podem empregá-la para antecipar e controlar o comportamento dos cidadãos de maneira a restringir as liberdades individuais e interferir no processo democrático. A IA também pode contribuir para a polarização e fragmentação na esfera pública (SUNSTEIN, 2007), e para a proliferação de notícias sensacionais e falsas, quando usado para capturar usuários, expondo-os a informações de que possam gostar ou que estejam de acordo com suas preferências, explorando assim seus vieses de confirmação. (PARISER, 2011 *apud* SARTOR; LAGIOIA, 2020, p. 32).

também os arranjos sociais mais amplos.[83]

A literatura apresenta muitos relatos de casos de discriminação. Por exemplo, Cathy O'neil, citada por Zanatta (2019), descreve o uso de bancos de dados de agências de crédito por empresas de recrutamento para selecionar candidatos a empregos, sem que o candidato soubesse do critério potencialmente discriminatório baseado em sua pontuação de crédito, que prevê um suposto "grau de risco" determinado matematicamente, resultando na alocação do candidato a um "grupo social" rotulado estatisticamente.

Virginia Eubanks (2018), *apud* Zanatta (2019), assevera que o escrutínio digital foca predominantemente o grupo social ao qual o indivíduo estaria associado (ou correlacionado) [84]; importa dizer, o dado relevante tem por base o preditor do grupo social e não o da pessoa, individualmente.

Além disso, para Eubanks (2018, p.6) *apud* Zanatta (2019), "pessoas de cor, imigrantes, grupos religiosos, minorias sexuais, pobres, e outras populações oprimidas, carregam muito mais o peso do monitoramento e rastreamento do que grupos avantajados".

Esse aspecto é corroborado por Ruaro, Sarlet (2022, p. 184 et seq.) [85], ao destacarem, com base em Fukuyama (2020) e Knobloch et al. (2013), as consequências duradouras na vida individual e coletiva decorrentes da identidade digital, que não se limita ao endereço IP[86] inserido na URL [87], mas é forjada no "cyberspace" a partir do conjunto de informações transformadas em bits e pixels. Eles enfatizam que a "caracterização pessoal, mesmo quando se trata de dados, diz respeito à singularização da pessoa em relação aos outros, sendo, portanto, uma forma de diferenciação da pessoa que pode se estender aos bens"[88].

---

[83] No original: "*A new dynamic of stereotyping and differentiation takes place. On the one hand, the individuals whose data support the same prediction, will be considered and treated in the same way. On the other hand, the individuals whose data support different predictions, will be considered and treated differently. This equalization and differentiation, depending on the domains in which it is used and on the purposes that it is meant to serve, may affect positively or negatively the individuals concerned but also broader social arrangements*". (SARTOR; LAGIOIA, 2020, p. 28)

[84] EUBANKS, 2018, p. 6 *apud* ZANATTA, 2019.

[85] SARLET; RUARO *apud* DONEDA *et al*., 2021, pp. 177-198.

[86] Protocolo de Internet.

[87] *Uniform Resource Locator*.

[88] Em complemento, afirmam que: "Os dados (...) assumem agora uma indiscutível proeminência em relação ao tema da identidade e, em decorrência, da proteção à personalidade. (...) esse mosaico identitário (...) é igualmente extraído das pegadas ou das sombras digitais, a dizer, do histórico de todas as transações efetuadas pelo usuário que formam os registros dos sites e dos portais de acesso à internet. (...) as sombras ou pegadas digitais incluem as imagens em câmeras de vigilância, os dados advindos das movimentações bancárias, das ligações telefônicas, das informações, dos diagnósticos e dos prontuários médicos, das cópias de scanners e de exames hospitalares, das

Por outro lado, Sartor e Lagioia (2020, p. 28) analisam o uso de tecnologias de aprendizagem de máquina na área da saúde. Esses autores consideram positivo - legítimo e proporcional em relação aos riscos à privacidade - o monitoramento da epidemia de COVID-19 por meio de aplicativos de IA, que possibilitaram um tratamento personalizado e eficaz para os indivíduos cujos dados foram coletados para esse fim[89]. No entanto, essa mesma avaliação não se aplica ao uso de dados de saúde no setor de seguros, uma vez que isso permitiria que os segurados com melhor saúde se beneficiassem em detrimento daqueles com perspectivas negativas, resultando em uma dupla penalização para estes últimos. Nesse caso, embora seja legítimo que as seguradoras possam distinguir eficientemente os riscos ao fazer contratos, essas considerações éticas sugerem que o uso de dados pessoais nesse setor seria incompatível com os princípios de proteção de dados pessoais[90].

Além do exemplo dos contratos de seguros, pode-se argumentar que em alguns mercados, a precificação individualizada pode resultar do cálculo de riscos, desde que não seja abusiva e esteja em conformidade com as regulamentações. No entanto, em relação à proteção do consumidor (CDC, art. 51) [91], é eticamente questionável a precificação personalizada que se

informações de crédito, do histórico de compras e de condenações, sobretudo as penais. (...) plêiade de todas as informações que podem ser acessadas nos *Datacenters*." (SARLET; RUARO *apud* DONEDA et *al*., 2021, p. 184 *et seq*.)

[89] "*Consider for instance the use of machine learning technologies to detect or anticipate health issues. When used to direct patients to therapies or preventive measures that are most suited to their particular conditions, these AI applications are certainly beneficial, and the benefits outweigh at least when accompanied by corresponding security measures whatever risks that may be linked to the abuse of patients' data. The benefits, moreover, concern in principle all data subjects whose data are processed for this purpose since each patient has an interest in a more effective and personalised treatment. Processing of health-related data may also be justified on grounds of public health (Article 9 (2)(h)), and in particular for the purpose of 'monitoring epidemics and their spread' (Recital 46). This provision has become hugely relevant in the context of the Coronavirus disease 2019 (COVID-19) epidemics. In particular a vast debate has been raised by development of applications for tracing contacts, in order to timely monitor the diffusion of the infection. AI is being applied in the context of the epidemics in multiple ways, e.g., to assess symptoms of individuals and to anticipate the evolution of the epidemics. Such processing should be viewed as legitimate as long as it effectively contributes to limit the diffusion and the harmfulness of the epidemics, assuming that the privacy and data protection risks are proportionate to the expected benefit, and that appropriate mitigation measures are applied*." (SARTOR; LAGIOIA, 2020, p. 28. Omitem-se as referências internas dos autores.)

[90] Ilustrativamente, mencione-se o princípio da especificação da finalidade ou limitação para fins de tratamento (*purpose specification principle*) previsto no *Fair Information Practice Principles/(FIPPs* (OCDE, 2013), incorporada na LGPD (Art. 6, I).

[91] CDC: "Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que: (...) IV – estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a equidade." No entender da professora Frazão, nos mercados de aquisição de produtos e serviços em geral, tal prática – de preços "personalizados" – seria questionável em razão da não dependência do cálculo individualizado de risco para o funcionamento. Nesses casos, segundo a professora, não estaria preenchido o pressuposto da justa causa mencionada pelo CDC para a elevação do preço de produtos ou serviços, se a diferenciação é feita por critérios potencialmente subjetivos e bastante personalizados. (FRAZÃO, 2018; FRAZÃO; CARVALHO; MILANEZ, 2022.)

baseia na exploração das fragilidades e vulnerabilidades individuais, incentivando a discriminação abusiva a partir de dados sensíveis indevidamente obtidos dos consumidores, como indicativos de depressão, ansiedade, compulsão por compras, vícios, entre outros.

Nesses domínios, como a publicidade direcionada, a prática comercial de anúncios personalizados pode parecer adequada aos interesses dos consumidores, "ajudando-os" a navegar por um grande número de opções disponíveis online. No entanto, sabe-se que a publicidade personalizada envolve a coleta massiva de dados pessoais, usados no interesse dos anunciantes e intermediários, provavelmente indo contra os interesses dos proprietários dos dados.

Nessas circunstâncias, como observado por Cohen (2019), conforme citado por Sartor e Lagioia (2020) [92] , ocorre a manipulação, influência e controle por meio da entrega de mensagens enganosas ou agressivas - geralmente mensagens que apelam para fraquezas e emoções, contornando a racionalidade. Em vez de estimular o uso da razão, as redes de informações atuais tendem a reforçar padrões automáticos e quase instintivos de motivação, cognição e comportamento que podem ser manipulados instrumentalmente.

Isso abre oportunidades para a manipulação, como afirmado por BURR (2019), citado por Sartor e Lagioia (2020) [93], por meio de técnicas psicográficas que permitem inferências comportamentais a partir de atitudes psicológicas. As pessoas são induzidas a comprar produtos de que não precisam, gastar excessivamente e se envolver em transações financeiras arriscadas, ou mesmo ceder a tendências latentes, como jogos de azar e uso de drogas[94].

Portanto, para além das garantias de liberdades e direitos individuais e considerando os impactos potenciais na esfera coletiva, as novas possibilidades oferecidas pela IA no campo da diferenciação entre indivíduos exigem reflexões sobre a rigorosa supervisão dessas atividades

---

[92] "*Rather than predominantly stimulating the development and exercise of conscious and deliberate reason, today's networked information flows* (…) *employ a radical behaviorist approach to human psychology to mobilize and reinforce patterns of motivation, cognition, and behavior that operate on automatic, near- instinctual levels and that may be manipulated instrumentally*" (COHEN, 2019 *apud* SARTOR; LAGIOIA, 2020, p. 29)

[93] "*Thus, people may be induced to purchase goods they do not need, to overspend, to engage in risky financial transactions, to indulge in their weaknesses (e.g., gambling or drug addiction). The opportunity for undue influence is emphasised by the use of psychographic techniques that enable psychological attitudes to be inferred from behavior, and thus disclose opportunities for manipulation*." (BURR; CRISTIANINI, 2019 *apud* SARTOR; LAGIOIA, *op. cit.*, p. 29)

[94] Sartor e Lagioia (2020) pontuam que, após o caso *Cambridge Analytica*, houve o reconhecimento por parte de várias empresas de internet que a publicidade política microdirecionada poderia afetar negativamente a formação da opinião política e, assim, adotaram algumas medidas corretivas, seja recusando transmissão de anúncios políticos pagos (*Twitter*), seja restringindo fatores usados para segmentação (excluiu-se aspectos como filiação política ou registros públicos de eleitores (*Google*).

medidas por algoritmos. Não se aplica mais a ingênua ideia de neutralidade que prevalecia na era "pré-IA".

Com base nesse cenário, o próximo tópico examinará as principais discussões sobre o desenvolvimento ético da IA.

2.4 INTELIGÊNCIA ARTIFICIAL COMO SISTEMA SOCIOTÉCNICO E O SEU DESENVOLVIMENTO ÉTICO, RESPONSÁVEL E EXPLICÁVEL

Para além dessas considerações gerais, é relevante examinar brevemente o caráter "sociotécnico" dos sistemas de IA. Esse conceito está associado à inter-relação entre os aspectos sociais e técnicos de uma sociedade, e é expresso pelo termo "Sistemas sociotécnicos" (SST) [95] utilizado no domínio da administração. De acordo com Sichman (2021), a premissa dos SST é que as organizações são compostas por elementos sociais e técnicos que trabalham juntos para realizar tarefas organizacionais. Essas interações resultam tanto em produtos físicos quanto em resultados sociais e psicológicos.

Sichman (2021) argumenta que esses sistemas existem no cotidiano há pelo menos duas décadas, mencionando experiências em diferentes tipos de *call centers* e serviços bancários. Atualmente, a visão geral é de que os elementos técnicos fornecem subsídios para que os seres humanos possam tomar decisões. Em certos domínios, os recursos técnicos podem ser usados na revisão de decisões equivocadas, aplicando sanções aos envolvidos, visando melhorar os resultados futuros do sistema (Sichman, 2021, p. 42).

No entanto, o autor ressalta que a incorporação da tecnologia de IA nesses sistemas tem o potencial de alterar a lógica original, levando os próprios elementos técnicos a tomar algumas decisões. Essa mudança de paradigma não é necessariamente boa ou ruim, mas indica que esses sistemas precisam incorporar outras propriedades relacionadas à interação humana (Sichman, 2021, p. 42).

Atualmente, o processamento da informação tornou-se indispensável na sociedade moderna, onde o conhecimento é ampliado na crença de que é possível aprender mais, de

[95] O termo foi cunhado por Eric Trist, Ken Bamforth e Fred Emery, no período da Segunda Guerra Mundial, derivado de seu estudo com trabalhadores em minas de carvão inglesas no Instituto Tavistock em Londres. (TRIST *et al*., 2013 *apud* SICHMAN, 2021, pp. 37-50)

maneiras diferentes e mais rapidamente, mesmo diante do caos informacional. No entanto, Bunge (1985) argumenta que o computador não substitui o ser humano, pois não é um cérebro que "sabe". Ele apenas recebe, armazena e transforma representações físicas do conhecimento. Mesmo nas versões mais sofisticadas, o computador não cria nada e suas decisões sempre resultam da programação. É a informação fornecida a ele que permite deduzir logicamente a partir das premissas e instruções do programa. O pensamento é um ato humano por trás do computador. Além disso, Bunge afirma que o computador não analisa se o problema está bem formulado, se os dados são de qualidade ou quantidade suficientes para a resolução prática. São os cérebros humanos e não o computador que avaliam se vale a pena resolver o problema. O computador pode buscar uma solução possível e verificar se ela efetivamente resolve o problema (Bunge, 1985, p. 235).

Os juristas estão conscientes das motivações ideológicas que relacionam as novas tecnologias de tratamento de dados ao caos ou à falta de controle técnico. Essa perspectiva é refletida nas estratégias em andamento em todo o mundo para o desenvolvimento de uma IA responsável, ética e explicável.

Na visão de Virginia Dignum (2019, apud Sichman (2021, pp. 42-43), o desenvolvimento e utilização de sistemas de IA devem ser realizados de forma ética e responsável, posturas essas a serem adotadas nas seguintes instâncias:

> • no processo de projeto de tais sistemas, garantindo que as equipes tenham em mente e antevejam as possíveis consequências do sistema para os indivíduos e sociedades;
>
> • no projeto do comportamento de tais sistemas, visando representar de forma adequada capacidades de raciocínio ético nos agentes inteligentes;
>
> • no código de conduta dos projetistas e desenvolvedores, mediante uma regulação adequada e processos de certificação que garantam um comportamento adequado dos atores envolvidos, como já existe em outras profissões.

Dignum defende uma abordagem ética dos projetos de IA (*ART of AI),* que garanta a inclusão de valores humanos e princípios éticos de maneira transparente e sistemática. Essa abordagem inclui três aspectos principais: prestação de contas (a*ccountability*), responsabilidade (*responsibility*) e transparência (t*ransparency*) (Sichman, p. 43).

Em relação à ética comportamental, a autora destaca a necessidade de reconhecer que as sociedades humanas geralmente se baseiam em normas para facilitar a interação entre seus

membros e com o conjunto da sociedade. Valores morais normalmente compõem as regras que embasam as decisões. O desafio é incorporar essas normas e valores nos sistemas de IA. Essas questões têm preocupado os pesquisadores há mais de uma década, buscando mecanismos de decisão que levem em conta sentimentos e valores morais dos agentes autônomos, tanto em relação a seus próprios comportamentos quanto aos comportamentos de outros agentes. Além da dimensão individualista, é necessário estabelecer mecanismos de governança adequados, capazes de sancionar comportamentos contrários às expectativas dos agentes sociais (Sichman, 2021, p. 43 et seq.). Nesse sentido, a transparência é fundamental para a interação dialética com esses agentes inteligentes, permitindo a contestação e a explicação das decisões tomadas por eles.

CAPÍTULO 3 – TUTELA DO SEGREDO DE NEGÓCIOS NA TECNOLOGIA

Como sinalizado em capítulos anteriores, a proteção de dados pessoais e o segredo de negócios estão interligados com as questões tecnológicas contemporâneas. Por exemplo, como proteger os dados pessoais ao permitir que os sistemas de IA aprendam e melhorem, e como garantir que as decisões automatizadas sejam justas e imparciais, ao mesmo tempo em que as informações relevantes sejam protegidas pelo segredo de negócios.

Este estudo interdisciplinar busca compreender o regime de proteção aplicável, as justificações normativas e as principais polêmicas relacionadas a cada um desses institutos, que estão interligados. O presente capítulo é dedicado ao segredo de negócios.

Para os fins deste trabalho, adota-se a expressão "segredo de negócios" de acordo com a expressão "conhecimentos tecnológicos confidenciais" utilizada por Balmes Vega Garcia (2008) e substancialmente acolhida na doutrina de Denis Borges Barbosa (2015) e Nuno Souza e Silva (2014) [96]. Essa expressão abrange diversos institutos da propriedade intelectual, como segredo de fábrica, know-how, segredo industrial, segredo comercial, savoir-faire e trade secret.

Além disso, o uso desse conceito “expansionista” de segredo comercial parece não discrepar daquele adotado no âmbito da Diretiva (UE) 2016/943 do Parlamento Europeu, relativa à proteção de *know how* e de informações comerciais confidenciais (segredo comerciais). A diretiva adota uma abordagem abrangente em relação ao conceito, afirmando que, além dos direitos de propriedade intelectual, os segredos comerciais são um meio legítimo utilizado por empresas e instituições de pesquisa não comerciais para apropriarem-se dos resultados de suas atividades relacionadas à inovação, a fim de permitir a plena exploração de seu investimento em pesquisa e inovação[97].

---

[96] Nuno Sousa e Silva (2014) observa que a designação (*informações não divulgadas*) fora adotada no TRIPS, com vistas a denotar neutralidade na escolha do termo, isto é, que não fizesse referência a uma tradição normativa. Segundo o autor, temia-se que a utilização da designação tradicional “segredos de negócio” (*trade secrets*) representasse uma concessão à visão americana, baseada na ideia de propriedade, que havia sido vigorosamente rejeitada pela delegação indiana. Ressalva, porém, que “como é geralmente sublinhado, não se trata de informações não divulgadas, mas sim de informações divulgadas selectivamente e sob confidencialidade”.

[97] “Considerando 1” da Diretiva (UE): As empresas e as instituições não comerciais de investigação investem na aquisição, no desenvolvimento e na aplicação de know-how e de informações que são a moeda de troca da economia do conhecimento e proporcionam uma vantagem competitiva. Este investimento na criação e na aplicação de capital intelectual é um fator determinante no que diz respeito à sua competitividade e ao seu desempenho relacionado com a inovação no mercado e, consequentemente, ao seu retorno sobre o investimento,

Nesse ponto, percebe-se a relevância e o valor atribuídos aos bens intangíveis nesta revolução digital, representados pelos conhecimentos tecnológicos, cujo monopólio ou protagonismo parece se expandir para a esfera da disputa geopolítica global, conforme indicado pelas declarações de Vladimir Putin sobre a inteligência artificial e como a liderança nesse setor definirá "quem será o líder do mundo"[98].

Nesse contexto - de disputa pelos bens intangíveis – coloca-se a avaliação de SOUSA e SILVA[99] no sentido de que a evolução do tema da apropriação dos conhecimentos tecnológicos alçou o instituto do segredo de negócios – outrora um tópico obscuro, "patinho feio", "enteado" da propriedade intelectual, "órfão negligenciado da análise econômica" - ao patamar de um tema essencial no estudo da propriedade intelectual e da concorrência desleal.

Além disso, atualmente, as escolhas estratégicas dos agentes econômicos não se limitam mais às hipóteses clássicas disponíveis nas leis de propriedade intelectual. Tornou-se imperativo para a sobrevivência, especialmente em certos mercados, reconhecer que o pioneirismo na inovação é um fator determinante para o sucesso ou a sobrevivência.

Dado o escopo deste trabalho de refletir sobre as potencialidades técnicas, culturais e políticas das novas tecnologias, é importante explorar brevemente os diferentes discursos que embasam e orientam as justificações protetivas de cada instituto.

---

que é o motivo subjacente à investigação e ao desenvolvimento empresariais. As empresas recorrem a diferentes meios de apropriação dos resultados das suas atividades relacionadas com a inovação, quando a abertura não permite a plena exploração do seu investimento em investigação e inovação. A utilização de direitos de propriedade intelectual, como patentes, desenhos ou modelos ou direitos de autor, constitui um desses meios. Outro meio de apropriação dos resultados da inovação é a proteção do acesso e da exploração de conhecimentos valiosos para a entidade que não sejam do conhecimento geral. Esse valioso know-how e essas valiosas informações empresariais, que são confidenciais e que se pretende que permaneçam confidenciais, são designados como segredos comerciais. (UNIÃO EUROPEIA, 2016)

[98] Conforme artigo publicado em 4 de setembro de 2017, na revista eletrônica Convergência Digital. "Quem dominar a Inteligência Artificial vai ser líder do mundo (...) A Inteligência Artificial está no centro dos debates globais e não mais apenas pelo embate entre homens e robôs. Nesta segunda-feira, 04/09, o presidente da Rússia, Vladimir Putin, falou sobre o tema da inteligência artificial (IA) perante uma plateia de estudantes e indicou a sua importância crucial para o futuro da humanidade. 'A IA é o futuro, não só da Rússia, como de toda a raça humana. Surge com oportunidades colossais, mas também ameaças que são difíceis de prever. Quem quer que seja o líder nesta esfera tornar-se-á o líder do mundo', advertiu. (...) Não por acaso, Musk e outros 160 líderes do mercado de tecnologia enviaram à ONU um pedido para que seja criada uma regulação para o uso de inteligência artificial em materiais bélicos. Mais uma vez, a ideia não seria impedir uma possível insurreição das máquinas, mas sim normatizar a utilização de drones, equipamentos de vigilância e outros dispositivos que possam ser controlados de maneira remota, sem interferência humana".

[99] Do mesmo referencial, anotamos a ilustrativa opinião no sentido de que a informação passa, agora, a ser a alma do negócio, diferencial competitivo necessário, "seja em grandes mercados, com elevados níveis de complexidade nos quais as empresas envidam esforços para criar perfis de consumidor e investem enormes maquias em estudos de mercado procurando conhecer melhor os consumidores e daí retirar uma vantagem; quer seja um pequeno comerciante num mercado local". (SOUSA E SILVA, 2014. Omitimos as referências internas do texto original.)

3.1 SEGREDO DE NEGÓCIOS: JUSTIFICAÇÕES E ÂMBITOS DE PROTEÇÃO

A amplitude e complexidade das questões decorrentes dos impactos das novas tecnologias de tratamento de dados levantam a necessidade[100] de revisitar os antigos e atuais debates sobre as justificações do segredo de negócios, antes de abordar o conceito em si. A controvérsia no âmbito desse debate indica a extensão da disparidade em torno desse instituto, o que torna relevante explorar aspectos dessa rica discussão.

A construção doutrinária em torno da concorrência desleal, que em muitos países, como o Brasil, justifica o segredo de negócios, sempre esteve relacionada à reprovação moral de comportamentos contrários às normas e práticas comerciais[101]. José De Oliveira Ascensão (1996, p.7) argumenta que o "princípio da prestação" (*Leistungswettbewer*b) justifica a existência de regras gerais que impedem comportamentos concorrenciais desleais. Segundo ele, esse princípio justifica a proteção da concorrência, pois leva à vitória do concorrente cuja oferta seja superior em termos de qualidade/preço, enquanto a concorrência falseada ocorre quando alguém divulga segredos para atacar a posição do concorrente.

Por outro lado, Michael Risch (2007) [102] justifica o segredo comercial com base na ideia geral do véu de ignorância de John Rawls, que parte da teoria da justiça e da "negociação da posição original". Essa perspectiva parte do pressuposto de que o detentor de informações valoriza o objeto de sua criação, ignorando a perspectiva dos outros[103]. Com base nisso, haveria

---

[100] Não nos é dado ignorar que a convergência tecnológica se coloca como pano de fundo da complexa discussão nos domínios do diálogo entre o segredo de negócios e proteção de dados, e, no mesmo patamar, importaria refletir sobre a convergência regulatória decorrente do fenômeno. Daí, o estudo das diversas perspectivas doutrinárias poderia eventualmente auxiliar no entendimento da complexa convergência tecnológica, alterada de tempos em tempos. "(...) todos os horizontes apontam agora para outro tipo de convergência, mais alargada e cujas oportunidades de aplicação são ainda mais abrangentes do que as da *Web*, o encontro entre a nanotecnologia, biotecnologia e tecnologia da informação (...)". (CONVERGÊNCIA..., 2022)

[101] AMORIM, 2017.

[102] "*Even if the current set of rules cannot be predicted, veil of ignorance analysis is still useful from a normative point of view. One might be able to consider the balancing those in the original position might have considered given the current set of rules. This may be sufficient for justifying the existence of trade secret law. After all, even with efficiency analysis we have no way of knowing whether a particular rule really is the most efficient in all circumstances. For example, if one assumes that people value that which they create more than others do, but at the same time that people want to build on the work of others, it is well within the bounds of reason that some form of limited protection of trade secrets would be the outcome of a negotiation under the veil of ignorance.*" (RISCH, 2007, p. 33)

[103] Rawls sugere que você se imagine em uma posição original por trás de um véu de ignorância. Por trás desse véu, você não sabe nada de si mesmo e de suas habilidades naturais ou de sua posição na sociedade. Você não sabe nada sobre sexo, raça, nacionalidade ou gostos individuais. (VÉU..., 2023)

uma justificativa ética para a obtenção de uma proteção específica dos segredos comerciais. Risch (2007) vê a proteção dos segredos como uma garantia para a concorrência honesta[104].

No entanto, essa visão vai de encontro ao argumento de JACOBS (2007) citado por SOUSA e SILVA (2014), que afirma que o que um homem chama de "injusto", outro pode chamar de "justo"[105]. Uma teoria de compartilhamento seletivo de informações também poderia justificar a proteção dos segredos comerciais como um meio de promover a confiança suficiente para que os detentores de segredos possam revelar pelo menos algumas informações.

Essa ideia parece compatível com a instituição de níveis escalonados de transparência, de acordo com os diferentes graus de risco e sensibilidade da inteligência artificial. SOUSA e SILVA (2014) argumenta que um detentor de segredos nunca compartilharia informações se não houvesse uma proteção legal efetiva em caso de violação. No entanto, ROBERT BONE (2014) argumenta que há uma diferença entre compartilhar e divulgar publicamente, como acontece na Propriedade Intelectual, que promove a utilização inovadora das informações divulgadas, uma finalidade ausente no segredo de negócios.

Entretanto, sinaliza SOUSA e SILVA (2014), do mesmo problema padece o conceito de "concorrência desleal", indeterminado como tantos outros presentes em diversas leis de propriedade intelectual. Confira-se na seguinte transcrição:

> Outra crítica que lhe pode ser feita é a sua falta de justificação económica e os efeitos nefastos da protecção em excesso(MARK LEMLEY, 2014). Claro que isto constitui uma contestação com base em argumentos pragmáticos e é sempre possível contrapor que o Direito é mais do que um mecanismo de promoção da eficiência económica(ANDREAS RAMAIAN, 2013). ROBERT BONE(2014) assinala ainda que este argumento não tem fundamento empírico, não sendo claro se empresas concorrentes, na ausência da lei, consagrariam uma protecção de segredos de negócio(RISCH, Michael, 2007). Um argumento de carácter mais jurídico prende-se com a protecção de direitos fundamentais/direitos humanos/direitos de personalidade[106] (JORGE MIRANDA, 2008). A protecção legal de segredos de negócio seria um imperativo resultante, para uns, da privacidade das empresas (BONE, 2014), e, para outros, do seu direito de propriedade(MARCO BRONCKERS & NATALIE MCNELIS, 2012). Neste último aspecto parece confluir a ideia de protecção do investimento e da concorrência pela prestação (Leistungwettbewerbs)(OLIVEIRA ASCENÇÃO, 1996). Também quanto a esta

[104] "*Another populist justification for trade secret law is the enforcement of commercial ethical standards. This justification does not work from a utilitarian point of view, nor is commercial morality a primary component of the philosophical analysis. The more likely explanation is simply that people do not like bad acts*." [Em tradução livre: "Outra justificativa populista para a lei de segredo comercial é a aplicação de padrões éticos comerciais. Essa justificativa não funciona a partir um ponto de vista utilitário, nem a moralidade comercial é uma componente da análise filosófica. A explicação mais provável é simplesmente que as pessoas não gostam de más ações."]. Risch (2007)

[105] Em tradução livre: "O que um homem chama de 'injusto' outro chama de 'justo'."

[106] Nesse aspecto, sugere-se leitura do interessante trabalho de autoria de Thais Ricci Conesa (2017).

> justificação são apontadas críticas sobretudo de carácter económico, especialmente o risco de protecção em excesso(RISCH, 2007)[107].

A tutela do segredo de negócios justificada no estímulo à inovação[108] e produção da informação é defendida por Michael Rischi (2009)[109] (*apud* SOUSA E SILVA, 2014)[110], todavia contestada por Michael Abramowicz e John F. Duffy (2008)[111].

Para esses últimos autores, na maioria das vezes a proteção dos segredos de negócio não poderia ser justificada com base na premissa do estímulo à inovação se considerarmos que em verdade a inovação (ou ao menos a informação objeto de segredo) ocorreria ou seria produzida no curso normal da operação de uma empresa, ainda que não tutelada juridicamente. Nesse entendimento, o que está em causa é a promoção do teste de mercados *(market experimentation).*[112]

Nesse aspecto, portanto, a proteção dos segredos de negócio se prestaria a estabelecer barreiras à entrada nesses mercados específicos, e nessa medida restaria suficientemente encorajado o seu desenvolvimento.

---

[107] SOUSA E SILVA, 2014, pp. 230-232.

[108] Vale registrar, nesse aspecto, as perspectivas dos estudos OCDE, em tradução livre: "A literatura econômica descreve a justificativa econômica para a lei de segredos comerciais em termos dos incentivos que ela fornece. Ele descreve três tipos de incentivos. Em primeiro lugar, fornece incentivos para inventar e investir no desenvolvimento de informações comerciais valiosas. Em segundo lugar, alivia as empresas da necessidade de investir em algumas medidas dispendiosas para evitar a quebra de segurança. Em terceiro, incentiva as empresas a se envolverem em uma disseminação mais ampla (embora limitada) de informações do que fariam de outra forma, aumentando assim a probabilidade de transbordamento de conhecimento. Dada a importância dos segredos comerciais em muitas economias, os impactos potenciais de tais incentivos parecem ser significativos. Vários estudos indicam que a proteção de segredos comerciais pode estimular o desenvolvimento de invenções e informações valiosas, ajudando a garantir o retorno do investimento na criação de tais inovações. Kitch (1980) caracteriza o incentivo em termos de redução de risco: segredos comerciais estão particularmente sob risco de roubo por apresentarem baixa taxa de depreciação. Friedman *et al*. (1991) da mesma forma veem o efeito de incentivo como o aumento do retorno à pesquisa e desenvolvimento ao diminuir o custo da proteção. Outros veem a função de incentivo como semelhante às patentes, onde os segredos comerciais servem essencialmente como um substituto para as patentes quando estas não estão disponíveis ou são muito caras. Maskus (2000) e Friedman *et al*. (1991) argumentam que os segredos comerciais podem substituir patentes e fornecer incentivos para inovar, onde: 1) uma invenção não é patenteável, mas é difícil de imitar, de modo que há valor em manter as informações confidenciais (por exemplo, uma lista de clientes), 2) uma empresa pode preferir evitar a divulgação pública exigida por uma patente, e 3) quando uma empresa pode desejar evitar o custo de obtenção de uma patente. Outros ainda veem o incentivo para investir decorrente de efeitos competitivos. Lemley (2011) observa que a proteção de segredos comerciais pode ajudar os inovadores a manter uma vantagem competitiva, tal como poderia ser obtida por meio de um processo único de produção ou produto; isso pode contribuir para a lucratividade e, assim, fornecer incentivos para mais investimentos em inovação". (SCHULTZ; LIPPOLDT, 2014)

[109] RISCH, 2010.

[110] SOUSA E SILVA, 2014.

[111] DUFFY, 2008, pp. 389-391.

[112] SOUSA E SILVA, 2014.

Ainda com relação à teoria do teste de mercado, tem-se a opinião crítica de BONE[113] centrada no argumento de que a não divulgação da informação, ao manto da proteção do segredo, implicaria em duplicação de esforços de inovação porque, ao contrário do que ocorreria no caso das patentes, os concorrentes continuariam a investir nas soluções de problemas já solucionados, fato que diminuiria o ritmo de inovação.

Interessante perspectiva é desenvolvida por Sandeen, Rowe (2013)[114] *apud* Sousa e Silva (2014)[115], a partir da ideia de que o regime de tutela legal dos segredos de negócio constituiria em possível **resolução do paradoxo de Arrow.**

A referência a esta teoria tem por base o artigo do economista Kenneth Arrow (1962)[116] que identificara a dificuldade na comercialização de informações, atribuindo tal dificuldade ao fato de que para que um "comprador" possa avaliar o objeto ofertado, primeiro precisará inspecionar a informação; todavia, uma vez inspecionada, o "comprador" já possuiria a informação e não teria razão alguma para pagar por ela.

Ao que se vê, então, na visão de Sandeen, Rowe (2013) *apud* Sousa e Silva (2014) (2014), de forma assemelhada à Propriedade Intelectual, a proteção de segredo de negócios teria por função evitar que, após a revelação confidencial de informação, o receptor pudesse utilizá-la livremente e que a limitação pela via da tutela do segredo teria o condão de criar as condições necessárias para a comercialização e exploração dessas informações.

Em meio à gama de possíveis justificações, Fritz Machlup (1958)[117] (*apud* SOUSA; SILVA, 2014)[118], a partir de seus estudos sobre patentes, assevera que dado que os agentes de mercado estruturam suas atividades com base em bens intangíveis em tese protegidos pelo manto dos segredos de negócios, seria tão irresponsável protegê-los quanto irresponsável abolí-los.

No que diz respeito à antijuridicidade da proteção dos segredos de negócios, Stefan Rützel (1995) [119] se opõe à proteção de segredos ilegais, argumentando que isso poderia contradizer o sistema legal. No entanto, SOUSA e SILVA (2014) observa que, no direito

[113] BONE, 2014.
[114] ROWE; SANDEEN, 2013 *apud* SOUSA E SILVA, 2014.
[115] SOUSA E SILVA, 2014.
[116] ARROW, 1962.
[117] EUA, 1958 *apud* SOUSA E SILVA, 2014.
[118] SOUSA E SILVA, 2014.
[119] RÜTZEL, 1995, pp. 557 e ss. *apud* SOUSA E SILVA, 2014.

português, embora a proteção não se aplique a segredos cujo conteúdo seja ilegal, a preterição de uma regra legal, como no caso da proteção de dados, não exclui necessariamente a tutela[120]. No Brasil, a LGPD (Art. 44) considera "irregular" o tratamento realizado sem observância da legislação pertinente, mas apenas exige a reparação do dano causado.

E o Código Civil Brasileiro parece também não afastar a dúvida[121]. Embora ofereça a definição de "ato ilícito" (em tese, distinto do "ato irregular), não leva à conclusão peremptória de que a cominação ao ato ilícito implicaria perda de direito (na hipótese, à tutela do segredo de negócios).

No âmbito da doutrina civil, dentre as categorizações dos atos ilícitos no plano da eficácia, depara-se com o "ilícito caduficiante", entendido como aquele cujo efeito é a perda de um direito. É nesse sentido o entendimento de Felipe Peixoto Braga Neto (2010, p. 208)[122] sustentado com base em exemplos de cominações (perda do direito) diretamente previstas nas disposições do Código Civil (artigo 1638 – perda do poder parental e artigo 1992 – perda ao quinhão de herança).

Inexistindo regras diretas de subsunção, como é o caso enfrentado nesta pesquisa[123], é preciso ponderar os valores e princípios do Ordenamento, o que abala a segurança jurídica dos atores sociais cujas atividades se estruturem em torno da confidencialidade tecnológica.

Considere-se, nesse sentido, a observação de Francisco Amaral (1993, p. 44-56)[124]:

> Sob o ponto de vista axiológico, a segurança jurídica perde terreno para os valores do bem comum e da justiça social. O pensamento jurídico passa a orientar-se mais em função dos valores do que dos interesses, recorrendo cada vez mais às cláusulas gerais e aos princípios jurídicos, categorias que não permitem maior rigor no trabalho lógico-dedutivo, ou raciocínio de subsunção, o que leva a falar-se atualmente em "perdas de certeza" no pensamento jurídico".

---

[120] SOUSA E SILVA, 2014.

[121] O Código Civil brasileiro oferece algumas indicações no tocante à definição do ato ilícito (*v.g*. art. 122, art. 187). Todavia, não parece claro no tocante às consequências do ato (Ar. 927), *in verbis*:
"Art. 122. São lícitas, em geral, todas as condições não contrárias à lei, à ordem pública ou aos bons costumes; entre as condições defesas se incluem as que privarem de todo efeito o negócio jurídico, ou o sujeitarem ao puro arbítrio de uma das partes. Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes."
"Art. 927. Aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo."

[122] BRAGA NETO, 2010, pp. 175-212.

[123] Enquanto se escreve este tópico, tem-se a discussão corrente implicada com a liberdade de expressão nas redes sociais e a correspondente indicação do Supremo Tribunal Federal no tocante à inexistência de direitos absolutos, ainda que na perspectiva da imunidade parlamentar (ademais, a imunidade parlamentar não é salvo-conduto para o cometimento de ilícitos). O mesmo entendimento há de se aplicar ao segredo de negócios, ousa-se afirmar. (CONJUR, 2022)

[124] AMARAL, 1993, p. 44-56.

Neste cenário de consensos impossíveis, estaria o regime protetivo dos segredos aberto à reforma em face da sua potencial incoerência com os demais interesses e valores protegidos no sistema jurídico?

Embora não se pretenda responder peremptoriamente a tão complexa questão, a resposta deveria ser positiva se e quando se aventa a possibilidade de que a tutela do segredo de negócios possa implicar no acobertamento de condutas em tese antijurídicas ou ilícitas. Nesse raciocínio, em princípio, dela haveria de ser excluída, por exemplo, um plano de sonegação de tributos — figura essa em linha tênue com a da elisão fiscal, em tese lícita.

No entanto, a questão da tutela do segredo de negócios em relação a um sistema algorítmico hipotético de perfilamento e automação de decisões, comprovadamente eficaz para controlar o comportamento de indivíduos ou grupos de indivíduos[125] para fins estritamente mercadológicos, permanece indefinida e em uma zona cinzenta.

Diante dessa variedade de perspectivas e argumentos, é importante reconhecer que existem fortes argumentos a favor da proteção dos segredos de negócios, desde que sejam atendidos os requisitos básicos estabelecidos pelo TRIPS[126], cujos aspectos gerais serão analisados na próxima seção. No entanto, a complexidade da questão sugere a possibilidade de reforma no regime de proteção dos segredos de negócios, a fim de evitar conflitos com outros interesses e valores protegidos pelo sistema jurídico.

3.2 CENÁRIO INTERNACIONAL - CONVERGÊNCIA NORMATIVA E O ACORDO TRIPS

O pensamento jurídico em relação à proteção jurídica dos segredos comerciais apresenta uma variedade de posicionamentos na doutrina. Essa diversidade de concepções reflete nas

[125] Não se está aqui a ignorar os avanços teóricos em torno do princípio da função social da propriedade, cuja violação certamente seria indiscutível em hipóteses extremas. Talvez, em estudos futuros, possa-se especular que a problemática da aplicabilidade desse princípio se situe no campo das metanarrativas, propositalmente fragmentadas com o suposto "fim da história" do socialismo e a emergência do capitalismo digital, segundo pensadores da pós-modernidade (ARAÚJO, 2007).

[126] Secretismo (de conhecimento restrito, não caída em domínio público, não facilmente acessível etc.); valor comercial (represente uma vantagem, valiosa enquanto secreta, prejudicial se divulgada etc.

diferentes abordagens normativas adotadas em cada jurisdição, que também são examinadas e criticadas na doutrina.

A Suprema Corte dos Estados Unidos justifica a proteção dos segredos comerciais com base na noção de propriedade, influenciada por John Locke e Blackstone[127]. No entanto, há estudiosos[128] que rejeitam esse caráter proprietário, argumentando que os segredos comerciais são uma forma distinta de direito de propriedade, sem o direito exclusivo de excluir terceiros[129].

Diferentes consequências jurídicas decorrem dessas concepções. Os autores Schultz e Lippoldt (2014) afirmam que a tutela proprietária conferida aos segredos comerciais pela Suprema Corte dos EUA permite ao titular exigir compensação em caso de violação, de acordo com a Constituição dos EUA. Por outro lado, a maioria dos países europeus não considera os segredos comerciais como propriedade, mas ainda estabelecem procedimentos e soluções específicas para investigação e reivindicações baseadas na propriedade intelectual[130].

De modo geral, uma pesquisa conduzida pela OCDE[131] revelou que a maioria dos países pesquisados possui definições semelhantes sobre sigilo comercial no contexto do Acordo TRIPS, combinando-o com a natureza dos segredos comerciais e os requisitos estabelecidos no Artigo 39 do acordo[132].

---

[127] Como pode-se ver em *Ruckelshaus v. Monsanto Co*., 467 *U.S.* 986, 1002-1003 (1984) *apud* SCHULTZ; LIPPOLDT, 2014.
[128] BONE, 1998 *apud* SCHULTZ; LIPPOLDT, 2014.
[129] CLAEYS, 2013 *apud* SCHULTZ; LIPPOLDT, 2014.
[130] *Idem*.
[131] SCHULTZ; LIPPOLDT, 2014.
[132] Decreto nº 1.355, de 1994, promulgação e incorporação dos resultados da Rodada Uruguai de Negociações Comerciais Multilaterais do GATT. "SEÇÃO 7: PROTEÇÃO DE INFORMAÇÃO CONFIDENCIAL ARTIGO 39 *1. Ao assegurar proteção efetiva contra competição desleal, como disposto no ARTIGO 10bis da Convenção de Paris (1967), os Membros protegerão informação confidencial de acordo com o parágrafo 2 abaixo, e informação submetida a Governos ou a Agências Governamentais, de acordo com o parágrafo 3 abaixo. 2. Pessoas físicas e jurídicas terão a possibilidade de evitar que informação legalmente sob seu controle seja divulgada, adquirida ou usada por terceiros, sem seu consentimento, de maneira contrária a práticas comerciais honestas, desde que tal informação: a) seja secreta, no sentido de que não seja conhecida em geral nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão, seja como um todo, seja na configuração e montagem específicas de seus componentes; b) tenha valor comercial por ser secreta; e c) tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta. Os Membros que exijam a apresentação de resultados de testes ou outros dados não divulgados, cuja elaboração envolva esforço considerável, como condição para aprovar a comercialização de produtos farmacêuticos ou de produtos agrícolas químicos que utilizem novas entidades químicas, protegerão esses dados contra seu uso comercial desleal. Ademais, os Membros adotarão providências para impedir que esses dados sejam divulgados, exceto quando necessário para proteger o público, ou quando tenham sido adotadas medidas para assegurar que os dados sejam protegidos contra o uso comercial desleal*." (BRASIL, 1994)

Em relação à interpretação do TRIPS, Sousa e Silva (2014) [133] destaca que o acordo oferece indicações de dupla proteção para informações não divulgadas, protegendo tanto os segredos comerciais em si quanto as informações relacionadas a produtos químicos-farmacêuticos ou agrícolas que envolvam esforços consideráveis na sua obtenção[134].

Ainda segundo o autor acima referido, a leitura das notas ao Artigo 39 sinaliza que embora ao titular do segredo deva ser conferido o poder de impedir que terceiros divulguem, adquiram ou se utilizem das respectivas informações, de uma forma contrária às práticas comerciais leais, **tal proteção não teria natureza de direito absoluto**. Em verdade - obtempera – o que está em jogo é a proteção das práticas honestas (e nesse sentido seria a conotação de vedação à concorrência desleal mencionada no dispositivo).

No Brasil, a lei da propriedade industrial (lei 9.279/96) não oferece a definição do que seriam tais informações confidenciais, na forma referida no TRIPS.

Todavia, a violação do segredo **é tipificada como crime de concorrência desleal,** como atos de divulgação, exploração ou utilização — sem autorização — de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que tenha tido acesso mediante relação contratual ou empregatícia, inclusive após o término do contrato.

No Brasil, a lei da propriedade industrial não define explicitamente o que são informações confidenciais, mas a violação dos segredos comerciais é tipificada como crime de concorrência desleal. Isso abrange atos de divulgação, exploração ou utilização não autorizados de conhecimentos, informações ou dados confidenciais utilizáveis na indústria, comércio ou

[133] SOUSA E SILVA, 2014.

[134] Neste particular, na análise de Schultz e Lippoldt (2014) em relação aos integrantes da OCDE, conclui-se que, embora não formuladas de forma idêntica, os países tendem a seguir as três categorias definidas Tratado: (1) informações técnicas; (2) informações comerciais confidenciais; e (3) know-how. Para esses autores, nas **informações técnicas** se incluem – no mais das vezes – processos industriais, projetos, fórmulas e informações assemelhadas relacionadas à tecnologia. Por **informações comerciais confidenciais** compreendem-se normalmente as listas de clientes (em tese, aquelas informações não públicas), informações financeiras, planos de negócios e informações relacionadas à operação do agente econômico. O termo **know-how** abrange informações sobre métodos, etapas e processos para alcançar resultados eficientes. Embora não se verifique uniformidade nesse rol no tratamento jurídico desses conhecimentos, trata-se de termo usualmente adotado em discussão de informações proprietárias em relação aos quais se reconhece tratar de uma categoria separada e definida de segredos comerciais. (SCHULTZ; LIPPOLDT, 2014).

prestação de serviços, exceto quando sejam de conhecimento público ou evidentes para um técnico no assunto[135].

Nesta tipificação legal (crime de concorrência desleal) também se enquadra a obtenção desses conhecimentos ou informações - reputados confidenciais - por meios ilícitos ou mediante fraude. Além da ação criminal, faculta-se ao prejudicado, a propositura de ações cíveis, fundado, por exemplo, no direito de haver perdas e danos, com base nos prejuízos suportados[136].

Elizabeth Kasznar Fekete (2017) defende que o segredo de negócio não possui o status de propriedade no Brasil, diferentemente das marcas registradas e invenções patenteadas. A proteção ao segredo de negócio é distinta e baseia-se na lealdade das práticas comerciais.

No Brasil, a proteção aos segredos de negócios está incorporada à legislação de propriedade industrial, que segue as regras do Acordo TRIPS e combate a concorrência desleal[137]. Os elementos constitutivos e requisitos dos segredos de negócios são definidos nos incisos XI e XII do Artigo 195 da Lei de Propriedade Industrial (Lei nº 9.279/96) **[138]**.

Também, em razão do Acordo TRIPS, especificamente do seu artigo 39, 2, hão de ser protegidas as informações que ***(i)*** forem secretas; ***(ii)*** tiverem valor comercial e ***(iii)*** forem

[135] Lei nº 9.279, de 1996: art. 195.

[136] É interessante mencionar as considerações de Sousa e Silva (2014), relativamente ao segredo adquirido por terceiros, em diversas situações que se reputam não passiveis de controle pelo titular: "(...) vezes há em que o que está em causa não é a aquisição mas a **utilização** ou **divulgação** de segredo de negócio. O princípio é que segredos ilicitamente adquiridos não poderão ser licitamente utilizados ou divulgados e vice-versa: segredos licitamente adquiridos serão livremente utilizáveis e divulgáveis. No entanto, há situações em que o segredo foi fortuitamente adquirido (logo de forma lícita) mas que, após notificação por parte do titular do segredo de negócio, será ilícito divulgá-lo ou utilizá-lo. Há ainda situações em que um segredo ilicitamente adquirido pode ser licitamente divulgado ou utilizado com fundamento em **defesas** como liberdade de expressão ou conflito de deveres. A maior parte destes casos será resolvido com apelo a considerações de proporcionalidade. Um aspecto importante a realçar é que os **consumidores finais**, ainda que beneficiem de um segredo de negócio ilicitamente adquirido, não são responsáveis pela sua violação. Utilizando a imagem do juiz RUSHING no caso *Silvaco v. Intel:* 'Aquele que faça uma tarte a partir de uma receita certamente que a 'utiliza'; mas aquele que come a tarte não 'utiliza' a receita em virtude apenas desse facto, e isto é verdade mesmo que o cozinheiro seja acusado de ter roubado a receita de um concorrente e o comensal esteja ciente dessa acusação. Esta é substancialmente a mesma situação quando alguém utilize software que seja compilado de código-fonte alegadamente roubado. O código-fonte é receita a partir da qual a tarte (programa executável) é cozinhado (compilado)." (SOUSA E SILVA, 2014. Omitem-se as referências internas da citação.

[137] JABUR; SANTOS; 2007, p. 360.

[138] LPI: "Art. 195. Comete crime de concorrência desleal quem:(...) XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato; XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude."

objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta.

No conceito de segredo de negócios restariam contempladas as informações a respeito de métodos de produção, fórmulas, algoritmos e ingredientes de um produto, assim como aqueles dados referentes às pesquisas feitas para melhoramento de produtos. Assim, por segredo comercial, há de se compreender – exemplificativamente - as informações referentes às análises de marketing, pesquisas de mercado, projetos de criação de novos produtos e serviços, cuja proteção em princípio é objeto de preocupação no âmbito dos sistemas de IA.

Neste aspecto, não é demais registrar a existência de debate [139] indicativo de uma possível "zona cinzenta" ou paralelismo com o conceito "expansionista" de "dados pessoais" adotado na LGPD (art. 5 I)[140], com amplas possibilidades de neles serem acolhidas todas as informações "relacionadas a pessoa identificada ou identificável"[141].

Em resumo, o debate internacional sobre a proteção dos segredos comerciais segue uma linha similar à doutrina nacional, onde o segredo de negócio não é considerado propriedade, mas sim um direito a ser respeitado com base na lealdade das práticas comerciais. No Brasil, a proteção aos segredos de negócios é realizada por meio da tipificação penal da concorrência desleal e pela legislação de propriedade industrial[142].

3.3 DISTINÇÕES COM OUTRAS FIGURAS DE PROPRIEDADE INTELECTUAL

Neste exame pretende-se abordar o tema do segredo de negócios em relação a outras formas de propriedade intelectual. A doutrina especializada costuma abordar as distinções entre

[139] MALGIERI, 2016, pp.102-116.
[140] Note-se que a definição adotada na LGPD corresponde àquela já adotada na LAI (Lei 12.527, de 2011: art. 4º, IV), segundo a qual informação pessoal é aquela relacionada à pessoa natural identificada ou identificável, e diz respeito àquela informação apta a vulnerar os direitos fundamentais de personalidade, como os definidos no art. 5º, X, da Constituição Federal.
[141] Importa dizer, um dado é considerado pessoal na medida em que, com base nele, se viabiliza a identificação, direta ou indireta, da pessoa natural a ele referida, a exemplo de nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, carteira de trabalho, passaporte e título de eleitor), endereço residencial ou comercial, telefone, *e-mail*, *cookies* e endereço IP.
[142] O Grupo de Trabalho do Artigo 29 (GT Art. 29) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD). No particular, a indicação do GT Art. 29 inclinou por incluir os dados inferidos no conceito de dados pessoais, questão ainda objeto de polêmicas no debate regulatório. (EDPB, 2023)

essas figuras. Neste contexto, destaca-se a revisão de literatura realizada por Schultz e Lippoldt (2014) [143], que menciona Pooley (1997) [144]. Esses autores observam que consultorias empresariais sugerem a adoção diferenciada entre patentes e segredos comerciais, dependendo do tipo de proteção desejada. Destaca-se que as patentes oferecem uma proteção mais adequada para invenções tecnológicas específicas que sejam úteis, novas e não óbvias. No entanto, o processo de patenteamento pode ser demorado e custoso. Além disso, argumenta-se que, uma vez concedida a patente, há exclusividade de mercado por um período determinado, exigindo-se divulgação pública da ideia.

As pesquisas conduzidas por Schultz e Lippoldt (2014) indicam que a escolha entre proteção por segredo ou por patente pode ter implicações no bem-estar social. Em uma perspectiva, os autores apresentam o argumento de Friedman et al. (1991) [145] de que as patentes são vantajosas para o bem-estar social, pois estimulam a divulgação do conhecimento, com efeitos positivos óbvios. Por outro lado, eles mencionam Cugno e Ottoz (2006) [146], que argumentam que o segredo comercial é socialmente mais adequado do que as patentes, seja pela abertura de possibilidade para invenção independente (possível no regime do segredo comercial, mas impedida pela lei de patentes), seja porque os proprietários de segredos comerciais têm menos oportunidades de cobrar preços acima da concorrência.

Na prática, as empresas tendem a confiar muito em segredos comerciais, como observado por Schultz e Lippoldt (2014) [147]. Eles mencionam as observações de Arundel (2001) [148] sobre a preferência das empresas europeias por segredos comerciais em vez de patentes, especialmente nas pequenas e médias empresas. Conclusões semelhantes foram apontadas em pesquisas realizadas por Cohen et al. (2000) [149], com foco em empresas americanas. Estudos econométricos e conclusões de Png (2012) [150] indicam que, nos estados dos EUA que promulgaram leis de segredos comerciais entre 1976 e 2006, houve um aumento nos gastos com pesquisa e desenvolvimento de alta tecnologia por grandes empresas, acompanhado de uma redução na dependência de patentes.

[143] SCHULTZ; LIPPOLDT, 2014.
[144] POOLEY, 1997 *apud* SCHULTZ; LIPPOLDT, 2014.
[145] FRIEDMAN; LANDES; POSNER, 1991, pp. 61-72 *apud* SCHULTZ; LIPPOLDT, 2014.
[146] CUGNO; OTTOZ, 2006 *apud* SCHULTZ; LIPPOLDT, 2014.
[147] SCHULTZ; LIPPOLDT, 2014.
[148] ARUNDEL, 2001 *apud* SCHULTZ; LIPPOLDT, 2014.
[149] COHEN; NELSON; WALSH, 2000 *apud* SCHULTZ; LIPPOLDT, 2014.
[150] PNG, 2012 *apud* SCHULTZ; LIPPOLDT, 2014.

A opinião de Maskus (2012, p. 237) [151] é utilizada pelos autores para destacar o papel dos segredos comerciais nos países em desenvolvimento, onde essa forma de proteção pode estar prontamente disponível para inovação incremental, enquanto as patentes podem não ser viáveis. Por outro lado, Sousa e Silva (2014) observa que há consenso de que um segredo comercial deve ser informação e que informações são dados organizados no contexto do Direito de Propriedade Intelectual (DPI). [152] Segundo Joanne Roberts (2000) [153] e Floridi (2010) [154], no contexto do DPI, apenas a informação econômica estruturada e factuais seria relevante, e uma informação precisa ser verdadeira para ter valor comercial, uma vez que é o significado da informação que é valioso para fins comerciais.

Sousa e Silva (2014) menciona uma polêmica interessante relacionada às informações da "imprensa amarela", dedicada à coleta e divulgação de notícias relacionadas a celebridades. Essas informações podem ser consideradas segredos comerciais, uma vez que possuem um valor comercial relevante. O autor argumenta que, à luz do DPI, a proteção não se destina ao conteúdo da informação em si, mas sim à legitimidade dos meios adotados para proteger o alegado segredo. Não existem critérios claros para o assunto que pode ser objeto de segredo, sendo suficiente atender aos elementos definicionais, sem a aplicação das limitações e requisitos da propriedade intelectual.

Em resumo, segundo Sousa e Silva (2014) [155], o princípio básico dos segredos comerciais é a confidencialidade. Um segredo comercial não é um direito de propriedade intelectual nem um direito fundamental derivado da dignidade humana ou da personalidade do seu detentor. Não faz sentido registrar o segredo, como ocorre com marcas ou patentes, uma vez que a opacidade é plenamente compatível com a proteção jurídica do segredo. Essencialmente, um segredo comercial é uma informação valiosa em termos competitivos, mantida em segredo com base na proteção legal.

De acordo com as lições de Denis Borges Barbosa (2015) [156], enquanto as patentes têm prerrogativas elementares do direito de propriedade, como o uso, fruição e direito de sequela, no segredo industrial, a norma objetiva proibir a concorrência desleal, sem proteção de propriedade. O autor argumenta que a conduta é proibida para indiretamente legitimar outro

[151] MASKUS, 2012 *apud* SCHULTZ; LIPPOLDT, 2014.
[152] SOUSA E SILVA, 2014.
[153] ROBERTS, 2000, p. 430 *apud* SOUSA E SILVA, 2014.
[154] FLORIDI, 2010, p. 88 *apud* SOUSA E SILVA, 2014.
[155] SOUSA E SILVA, 2014.
[156] BARBOSA, 2015. p. 369.

direito (que não é o direito de propriedade). No âmbito do segredo comercial, não há direito de sequela, ou seja, não há um direito exercitável sobre a coisa que permita aos autores reivindicar o objeto segredo daquele que o detenha. Além disso, fica claro que, se o comportamento não puder ser atribuído ao réu, a ação respectiva não pode prosperar. Nas palavras do autor:

> O fato de ser atribuído a terceiros, que não aos réus, um comportamento alegadamente desleal não contaminaria a informação – recebida de boa-fé – de forma a impedir o seu uso, ou fazê-lo ilícito. A possibilidade de que se exerça o *jus persequendi* sobre a informação transforma o segredo em propriedade; o que não existe no nosso sistema jurídico, inclusive por razões constitucionais, sem falar da regra do *numerus clausus*.

Para concluir, é importante repisar que, neste estudo, o termo "segredo de empresa" (também chamado de "segredo de negócio") abrange segredos industriais, relacionados aos processos de fabricação e fórmulas de produtos, bem como segredos comerciais, como a lista de clientes e fornecedores, estudos de viabilidade de comercialização e pesquisas de mercado[157].

Também é relevante mencionar que, no Brasil, a proteção dos segredos de negócios ganha destaque na Lei Geral de Proteção de Dados (LGPD: Lei 13.709/2018) [158], sendo

---

[157] Elisabeth Kasznar Fekete elenca os "múltiplos vocábulos" adotados pelos legisladores, juristas e julgadores, brasileiros e estrangeiros, em referência aos dados confidenciais objetos da proteção legal, de modo que expressões como "segredo industrial" e "segredo comercial" reputam-se englobadas no gênero "segredo de negócio", o que corresponde, grosso modo, à fórmula expressa no termo "*trade secret*" para designar tanto o segredo de fábrica quanto o de comércio". (FEKETE, 2003, p. 17).

[158] LGPD (Lei nº 13.709, de 2018): "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. (...)

§ 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."

"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: (...) 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; [...] Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: (...) II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. (...)

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento."

"Art. 38. 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. 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."

interpretada como uma barreira ao princípio da transparência[159]. A interação entre essa legislação e a proteção dos segredos de negócios tem sido objeto de polêmica, cuja complexidade justifica a reflexão baseada na experiência da União Europeia.

3.4 A EXPERIÊNCIA DA UNIÃO EUROPEIA – A DIRETIVA DOS SEGREDOS COMERCIAIS (*TRADE SECRETS*) E O RGPD

O "Considerando nº 1" da Diretiva de Segredos Comerciais (U.E) 943/2016 esclarece o contexto e a racionalidade subjacentes à proteção dos segredos comerciais.

Empresas e instituições não comerciais de pesquisa investem em know-how e informações que são essenciais para a economia do conhecimento e proporcionam vantagem competitiva. Esse investimento no capital intelectual é crucial para a competitividade, inovação e retorno sobre o investimento. As empresas empregam várias formas de apropriação dos resultados de suas atividades inovadoras quando a abertura não permite a exploração completa do investimento em pesquisa e inovação. O uso de direitos de propriedade intelectual, como patentes, desenhos, modelos e direitos autorais, é uma dessas formas. A proteção do acesso e da exploração de conhecimentos valiosos não amplamente conhecidos também é uma maneira de apropriar os resultados da inovação, e esses conhecimentos valiosos são chamados de segredos comerciais.

O ponto de controvérsia explorada neste trabalho está refletido nos debates locais[160], os quais dão conta de que a Diretiva Segredos Comerciais (Diretiva EU 2016/943) não define

---

"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. (...) III – a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;"
"Art. 55-J. Compete à ANPD: (...) 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. 2.º desta Lei; (...) X – dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial."

[159] Do cotejo de uma e da outra lei protetiva abre-se margem para uma leitura alternativa, *i.e.*, no sentido de que a tutela dos dados pessoais implica em possível "barreira" (limitação, restrição) ao segredo de negócios, na medida em que condiciona o tratamento dos dados pessoais à observância do dever de cuidado e respeito à prerrogativas asseguradas ao titular dos dados pessoais (devida explicação, revisão, correção, anonimização etc.), sem os quais as respectivas informações não poderiam ser "incorporadas" ao patrimônio empresarial intangível. Ademais, como se sabe, se uma norma soa conflituosa ou contraditória em relação a outra, ao vedar uma conduta e ao mesmo tempo permiti-la (ou vice e versa), a solução há de passar pela aplicação do critério cronológico ou o da especialidade, caso a aparente antinomia não se resolva pelo critério hierárquico.

[160] HUSTINX, 2014, § 15 - § 22 *apud* SOUSA E SILVA, 2014.

especificamente o conceito de "informações comerciais", oferecendo todavia as "indicações" hermenêuticas para tanto.

Ao explicar o escopo da proteção de segredos comerciais, o texto normativo sugere que os "dados comerciais" (enquanto informações protegidas) englobam os planos de negócios, pesquisas e estratégias de mercado e informações sobre clientes e fornecedores (de fato, o "considerando nº 2 da Diretiva parece confirmar tal assertiva)[161].

Sobre tal questão, nota-se que a Autoridade Europeia para a Proteção de Dados destaca que a informação relacionada aos indivíduos (dados pessoais) é relevante para o conceito de segredo de negócios fazendo-se assim necessário analisar amplamente esses direitos de privacidade dentro da Diretiva de Segredos Comerciais[162].

Segundo a Diretiva sobre Segredos Comerciais (Diretiva U.E 2016/943) - alinhada ao Acordo TRIPS (Art. 39) – qualquer informação pode ser abrangida pela proteção de segredos comerciais desde que mantida em segredo, tenha valor econômico (i.e., ao decidir manter a informação segregada em face da concorrência, presume-se que o agente econômico considerou o "custo" de mantê-la em segredo)[163].

No entanto, a análise de dados pessoais é complicada devido à definição ampla de dados pessoais no GDPR

Tanto o GDPR quanto a Diretiva de Segredos Comerciais não oferecem orientação clara para resolver essas questões. Quanto à proteção dos segredos de negócios, o RGPD estabelece direitos de acesso e portabilidade de dados para os titulares dos dados, mas também

[161]"Considerando nº 2" da Diretiva (EU) 2016/943, de Segredos Comerciais: As empresas, independentemente da sua dimensão, valorizam os segredos comerciais tanto como as patentes e outras modalidades de direitos de propriedade intelectual. Utilizam a confidencialidade como um instrumento de gestão da competitividade empresarial e da inovação na investigação, em relação a um conjunto variado de informações que vão para além dos conhecimentos tecnológicos e abarcam dados comerciais tais como informações sobre os clientes e os fornecedores, planos de negócios e estudos e estratégias de mercado. As pequenas e médias empresas (PME) valorizam ainda mais os segredos comerciais e são ainda mais dependentes. (g.n.)

[162] HUSTINX, 2014, § 15 - § 22 *apud* SOUSA E SILVA, 2014.

[163] "**Artigo 2º - Definições** Para efeitos da presente diretiva, entende-se por: 1) «Segredo comercial», as informações que cumprem cumulativamente os requisitos seguintes: a)serem secretas, no sentido de, na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, não serem geralmente conhecidas pelas pessoas dos círculos que lidam normalmente com o tipo de informações em questão, ou não serem facilmente acessíveis a essas pessoas; b) terem valor comercial pelo facto de serem secretas; c) terem sido objeto de diligências razoáveis, atendendo às circunstâncias, para serem mantidas secretas pela pessoa que exerce legalmente o seu controlo;"

ressalva a proteção dos segredos comerciais. Portanto, é desafiador determinar qual critério geral de "prevalência" deve ser observado.

O Instituto Max Planck para Inovação e Concorrência apresentou seus argumentos sobre a proteção especial dos algoritmos no contexto da União Europeia Europeia (DREXL et all, 2016, p. 5). Eles não veem a necessidade de criar uma proteção legal especial para os algoritmos usados no processamento de dados, como na análise de big data. Argumenta-se que os desafios tecnológicos estão relacionados ao desenvolvimento de ferramentas de processamento de dados, e não à proteção específica dos algoritmos [164]. Programas de computador para o processamento de dados já são protegidos pela legislação de direitos autorais, mas essa proteção não abrange a funcionalidade geral do programa ou o algoritmo subjacente. Proteger algoritmos e assuntos abstratos causaria restrições desnecessárias à concorrência e dificultaria o progresso técnico.

Em resumo, há falta de orientação clara nas regulamentações sobre a solução dessas questões relacionadas à proteção de segredos comerciais, dados pessoais e algoritmos. A discussão sobre a proteção legal de algoritmos e dados continua no contexto da União Europeia.

[164] "Os *datasets* formam a base de qualquer análise de dados de alto nível. No Brasil o termo mais utilizado para ele é 'conjunto de dados', porém este conceito pode gerar dúvidas porque é mais abrangente do que a ideia de *dataset* para *analytics*". (DATASETS..., 2018)

CAPÍTULO 4 - PROTEÇÃO DOS DADOS PESSOAIS E DECISÕES AUTOMATIZADAS NO ORDENAMENTO JURÍDICO BRASILEIRO

No Brasil, os dados pessoais são protegidos pela Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) [165]. Essa lei estabelece os direitos dos titulares de dados e define os requisitos e procedimentos aplicáveis ao tratamento desses dados, independentemente do país de origem da pessoa física cujos dados são tratados ou pessoa jurídica que realiza a coleta ou tratamento dos dados[166].

Inspirada no regulamento da União Europeia (RGPD), a LGPD converge na linha principiológica de servir de barreira de contenção ao uso – e abusos – no contexto do crescente interesse do mercado pelos dados pessoais, "ativo" de maior valor agregado numa "economia movida a dados" (*data-driven economy*)[167].

Nesse contexto, pretende-se abordar os aspectos essenciais da regulação de proteção de dados pessoais, a fim de identificar os conflitos entre os diversos interesses protegidos pelo ordenamento jurídico. São levantadas as seguintes questões: (i) qual é a extensão da proteção conferida aos dados pessoais? (ii) quais são os principais paradigmas dessa proteção? (iii) quais são as formas de proteção em relação ao acesso aos dados pessoais que se destacam no debate sobre a regulação da Inteligência Artificial?

De acordo com Bruno Miragem (2019, p.2)[168], a legislação brasileira de proteção de dados pessoais está fundamentada nos direitos fundamentais consagrados, como a proteção da vida privada, da intimidade, a dignidade da pessoa humana e a promoção do bem de todos. O

[165] Por intermédio da Emenda Constitucional nº 115, de 2022, o direito à proteção de dados pessoais, inclusive nos meios digitais, foi alçado ao rol dos direitos fundamentais (e, portanto, de aplicação imediata), a partir da inclusão do inciso LXXIX ao art. 5º, nos seguintes termos: *"*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)"

[166] "Há forte convergência da lei brasileira com a regulação precedente estabelecida na União Europeia (conhecida como RGPD), com destaque para aspectos como: semelhante base principiológica, regulação igualmente calcada no modelo '*ex-ante*' de proteção e centralidade, em ambas, do papel da *accountability*". (BIONI; MENDES, 2019, p. 803)

[167] Para além do caráter protetivo, a LGPD pode também traduzir os esforços estatais de se inserir no fluxo internacional de dados de se adequar às condicionantes sinalizadas na RGPD, em princípio também endereçadas a qualquer não membro da União Europeia, na medida em se exige um nível adequado de proteção de dados como requisito necessário ao compartilhamento de dados. Em termos "práticos", regra geral, se dado país não satisfizer o referido critério e se assim não for oficialmente reconhecido pela União Europeia, estará em princípio impedido de jogar naquele rico mercado informacional. (BIONI; MENDES, 2019, pp. 818-819)

[168] MIRAGEM, 2019, p. 2.

objetivo da LGPD é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade das pessoas naturais.

Ana Frazão (2021, *passim*) destaca a complexidade e a abrangência da regulamentação do tratamento de dados pessoais. Segundo ela, além da perspectiva jurídica, a concretização dos objetivos da LGPD requer iniciativas que envolvam toda a sociedade e a política. A proteção de dados pessoais permeia diferentes áreas do Direito, como o Direito da Concorrência e a Defesa do Consumidor, exigindo a compatibilidade entre elas para a harmonia e unidade do ordenamento jurídico[169].

A interseção entre a proteção de dados pessoais, o Direito da Concorrência e a Defesa do Consumidor é mencionada por Borges (2020, p. 111)[170], indicando que a maximização do bem-estar do consumidor é um objetivo presente em diferentes jurisdições. Essa interconexão dos microssistemas jurídicos citados é evidente.

Além disso, Monteiro (2018)[171] destaca os impactos da proteção de dados pessoais na defesa da concorrência, como possíveis barreiras à entrada de novos concorrentes, maior impacto sobre as empresas de tecnologia estabelecidas e o direito dos usuários à portabilidade de dados, que pode promover a concorrência entre plataformas e reduzir os incentivos à inovação.

Em reação às polêmicas em torno do caráter proprietário dos dados pessoais (presente nos discursos de atores representativos do mercado) Laura Schertel Mendes (2014) assevera que a regulação de proteção de dados não pode ser compreendida como atributiva de um direito de propriedade a quem quer que seja.

Nas lições da professora, por definição, o instituto da Proteção de Dados Pessoais tem natureza multidimensional, objetiva equilibrar os direitos de proteção, de defesa e de participação do indivíduo nos processos comunicativos. Em suma, na doutrina de Laura SCHERTEL MENDES, a proteção de dados pessoais se presta a proteger a personalidade do indivíduo contra os riscos ocasionados pela coleta, processamento e circulação de dados pessoais.

Na linha da autora, implica dizer, portanto, que a justificação da tutela dos dados

---

[169] FRAZÃO *apud* DONEDA *et al.*, 2021, pp. 535-555.
[170] BORGES, 2020, p. 111.
[171] Análise dos potenciais impactos da LGPD, cf.: MONTEIRO, 2018.

pessoais extrapola os interesses meramente individualista e a proteção da privacidade e do livre desenvolvimento da personalidade, inerentes à regulação, tem seu campo de aplicação no tempo-espaço do convívio social da pessoa a ela relacionado.

Em relação aos interesses do mercado, a regulação de dados pode ser vista como um potencial "direito de propriedade" para o titular dos dados. Segundo opinião de Francis GURRY (expressa em contexto e perspectivas diversos) no sentido de que “quando criamos restrições ao livre fluxo de dados no que diz respeito à coleta, ao armazenamento e ao uso, elas podem, a certa altura, equivaler a um direito de propriedade” [172].

No entanto, Laura Schertel Mendes (2014) ressalta que a proteção de dados não deve ser entendida como a atribuição de um direito de propriedade a qualquer pessoa. A proteção de dados pessoais tem como objetivo equilibrar os direitos de proteção, defesa e participação do indivíduo nos processos de comunicação[173].

Alan Westin *apud* Laura Schertel (2014, n.p.)[174]destaca que o desejo de privacidade de um indivíduo nunca é absoluto, pois a participação na sociedade também é importante. Existe um equilíbrio contínuo entre o desejo de privacidade e o desejo de exposição e comunicação, levando em consideração as condições e normas sociais do ambiente em que a pessoa vive.

Assim, a LGPD pode ser compreendida como um microssistema jurídico que garante direitos aos titulares de dados pessoais, entendidos como as pessoas naturais identificadas ou identificáveis pelas informações (art. 5º, incisos I e V da LGPD) constantes em bancos de dados ou tratadas nos termos da lei (art. 5º, inc. X da LGPD).

A lei estabelece os princípios para o tratamento de dados, como finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Para boa parte da literatura referenciada, o consentimento do titular de dados deve ser analisado com atenção, pois é uma das bases para o tratamento de dados elencadas no art. 7º da LGPD. A *autodeterminação informacional* é exercida por meio do consentimento do titular dos dados pessoais[175].

---

[172] PROPRIEDADE..., 2019.
[173] MENDES, 2014.
[174] WESTIN, 1970 *apud* MENDES, 2014.
[175] LIMA, 2009.

A LGPD oferece um conceito de consentimento em seu art. 5o, inc. XII, com base no qual há que ser ele entendido como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Por consentimento entenda-se um consentimento qualificado. A LGPD o adjetiva como "informado", o que ressalta ainda mais o dever — que se atribui ao controlador — de informar e o de transparência, conforme já destacado supra, ou seja, deve-se dar efetiva oportunidade para que o titular possa tomar conhecimento dos termos das políticas de proteção de dados, os quais devem obedecer as linhas gerais da lei protetiva.

Caberá à ANPD fiscalizar as práticas dos agentes de tratamento de dados com relação às políticas de proteção de dados, bem como orientá-los sobre as melhores práticas[176].

São encontrados vários conceitos relevantes na LGPD, dos quais, por ora, limita-se a mencionar os estabelecidos no art. 5º, a exemplo daquele definido no inciso I, particularmente da acepção legal de *dado pessoal* tida como "informação relacionada a pessoa identificada ou identificável".

No inciso II do mesmo artigo tem-se por definição que por **dados sensíveis** há que entender aqueles relacionados à:

> LGPD. Art. 5º II – "dados sensíveis: 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".

Segundo o inciso III do art. 5º da LGPD, *informação anonimizada* é "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

De forma expressa, a LGPD estabelece, no Inciso X do artigo 5º, que a *coleta* compõe uma das etapas do *tratamento de dados*, o qual restaria autorizado nas hipóteses das *bases legais* mencionadas no art. 7º: ***(i)*** consentimento do titular; ***(ii)*** cumprimento de obrigação legal/regulatória pelo controlador; (***iii***) estudos por órgão de pesquisa; ***(iv)*** execução de contrato ou procedimentos ligados a contrato do qual seja parte o titular; ***(v)*** exercício regular de direitos

[176] DE LUCCA; LIMA *apud* LIMA, 2019, pp. 373-398.

em processo judicial, administrativo ou arbitral; ***(vi)*** proteção da vida ou incolumidade física do titular/ terceiro; (***vii***) proteção de crédito; ***(viii)*** tutela de saúde; ***(ix)*** atendimento de legítimo interesse do controlador ou de terceiros; e (***x***) proteção do crédito.

A LGPD estabelece vários conceitos relevantes, como dados pessoais, dados sensíveis e informação anonimizada. À coleta de dados, enquanto etapa do tratamento de dados, aplica-se igualmente as bases legais (endereçadas do tratamento de dados pessoais), como consentimento do titular, cumprimento de obrigações legais/regulatórias, execução de contrato, exercício regular de direitos, proteção da vida, proteção de crédito, entre outros.

A transferência de dados [177] requer consentimento do titular, a menos que seja dispensada pela LGPD. A transferência internacional de dados exige um grau de proteção adequado no país ou organismo internacional de destino, juntamente com garantias de cumprimento dos princípios e direitos previstos na LGPD.

Ao fim, merecem destaques os direitos dos titulares: ***(i)*** direito à revogação do consentimento (art. 15, III e art. 18, IX); direito à liberdade (art. 17); ***(ii)*** direito à intimidade (art. 17); ***(iii)*** direito à privacidade (art. 17); (***iv***) direito à confirmação da existência de tratamento (art. 18, I); (***v***) direito ao acesso aos dados (art. 18, II); (***vi***) direito à correção de dados incompletos, inexatos ou desatualizados; (***vii***) direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV); (***viii***) direito à portabilidade dos dados (art. 18, V); (***ix***) direito à eliminação dos dados pessoais tratados com o consentimento do titular, salvo exceções legais (art. 18, VI); ***(x***) direito à informação das entidades públicas e privadas com as quais o

[177] Lei nº 13.709, de 2018: "Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente está de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional".

controlador realizou uso compartilhado de dados (art. 18, VII); (***xi***) direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (art. 18, VIII).

4.1 O CONCEITO DE DADOS PESSOAIS E A UTILIZAÇÃO DE TECNOLOGIAS DE INTELIGÊNCIA ARTIFICIAL

A LGPD (Lei nº 13.709/2018) segue a maior parte das leis gerais de proteção de dados pessoais ao redor do mundo e os instrumentos internacionais vigentes (BIONI, 2021, p.65)[178] no tocante ao conceito "expansionista"[179] —, já adotado na Lei de Acesso à Informação brasileira (LAI) — prosseguindo na técnica de não oferecer rol exemplificativo, limitando-se a definir dado pessoal como "a informação relacionada a pessoa natural identificada ou *identificável* (art. 5º, I).

No âmbito deste estudo transversal do segredo de negócios e proteção de dados pessoais, muita discussão tem suscitada a questão da identificação do objeto juridicamente protegido[180].

Embora não se pretenda neste tópico especular sobre a origem da celeuma - em princípio decorrente do foco na letra da lei e não no sentido finalístico[181] da norma -, é preciso alinhavar as considerações doutrinárias acerca da definição legal, não isenta de consequências práticas.

Ademais, ao valer-se de elementos conceituais abrangentes como "informação relacionada" e de variáveis como "dado anonimizado" (Art. 5º III), o próprio dispositivo legal parece indicar seu alinhamento com a realidade tecnológica, corroborada com o fato de que o

---

[178] BIONI, 2021, p. 65.

[179] Em contraposição, diz-se que o conceito de dado pessoal é restrito ou "reducionista", como adotado em países como os EUA, quando concernente aos dados identificadores diretos (o nome, por exemplo) e indiretos (número de documentos, o endereço ou o CEP). (FRAZÃO *et al*., 2022, p. 49)

[180] O debate centrado nos "dados pessoais" em si, sem qualquer referência aos demais elementos protegidos, parece refletir celeuma das discussões em torno do "mercado digital de dados pessoais". Maglieri (2016, pp. 102-116), em excelente artigo, propõe uma abordagem "descontextualizada", entendida como uma limitada divulgação de dados, daqueles especificamente relacionados ao cliente (titular dos dados), ao argumento que, nessa medida, a informação não importaria em revelação alguma dos segredos de negócios.

[181] Por todos, mencionamos a opinião de Laura Schertel Mendes, para quem a regulação de proteção de dados não pode ser compreendida como atributiva de um direito de propriedade, prestando-se a proteger a personalidade do indivíduo contra os riscos ocasionados pela coleta, pelo processamento e pela circulação de dados pessoais. Por definição, o instituto da proteção de dados tem natureza multidimensional, objetiva equilibrar os direitos de proteção, de defesa e de participação do indivíduo nos **processos comunicativos** (a hipótese deste ensaio está alinhada nessa ideia, diga-se).

requisito é relativizado em consideração ao estado de arte da técnica[182], e, neste aspecto, sabe-se que o processo de anonimização não é suficiente para a quebra do vínculo entre o dado e o seu titular, notadamente em razão dos avanços exponenciais das novas técnicas no âmbito das aplicações de IA.

Daí, a necessidade de examinar as demais técnicas disponíveis como supressão, generalização, randomização e pseudoanonimização, com a igual ressalva de que — em contexto de *big data* e utilização de sistemas de IA — nenhuma delas parece assegurar peremptoriamente o grau absoluto de desvinculação, em tese almejado na "anonimização"[183].

Inicialmente, considere-se que tanto o artigo 5º, II da LGPD[184] como o GDPR, em seu art. 4 (1)[185] , não contemplam no conceito de dados pessoais aquelas informações que embora relacionadas a seres humanos não se refiram a indivíduos específicos (por exemplo, informações médicas gerais sobre fisiologia ou patologias humanas) ou que tenha sido efetivamente anonimizadas, no sentido de perda de conexão com indivíduos específicos[186].

A questão da identificabilidade - entendida como as condições em que um dado, embora não explicitamente associado a uma pessoa, é considerado dado pessoal ante a consideração de que existe a possibilidade de identificar a pessoa relacionada - é tratada no Considerando (26) da RGPD.[187]

Essa identificabilidade depende da disponibilidade de "meios razoavelmente prováveis de serem usados" para uma reidentificação bem-sucedida, que por sua vez, depende do estado da arte tecnológico e sociotécnico (SARTOR, LAGIOIA, 2020).

---

[182] É a partir dessa problemática que parecem derivar as muitas questões – sem respostas, *a priori* – cuja solução passaria pelo procedimento dialógico, como parece sugerir a própria a regulação, conforme se argumenta neste ensaio.

[183] Em tempos atuais, afastou-se a ideia de que seria possível uma anonimização efetiva e irreversível a partir de estudos empíricos no sentido de evidenciar a natureza tecnologicamente imperfeita do processo de anonimização, que pode ser revertido, entre outros meios, por meio de um processo de combinação de diferentes bases de dados ou de pequenos *bits* de informação. (BIONI, 2021, pp. 61-62)

[184] Segundo a LGPD (Art. 5º, II), "dado anonimizado" é qualquer "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

[185]Artigo 4 (1) GDPR: «dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da natureza física, fisiológica, identidade genética, mental, económica, cultural ou social dessa pessoa singular.

[186] SARTOR; LAGIOIA, 2020.

[187] *Idem*.

Significa dizer que para determinar se uma pessoa singular é identificável, deve-se levar em conta todos os meios razoavelmente susceptíveis de serem utilizados, pelo responsável pelo tratamento ou por outra pessoa, para identificar a pessoa singular direta ou indiretamente[188]. Para determinar se os meios são razoavelmente susceptíveis de serem utilizados para identificar a pessoa singular, devem ser levados em conta todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível no momento do processamento e evolução tecnológica[189].

A técnica de pseudonimização, mencionada no artigo 13 da LGPD[190], implica na substituição dos dados identificadores de uma pessoa (v.g., o nome) por um "pseudônimo", ainda que por meio de criptografia.

Todavia, a ligação entre o pseudônimo e os itens de dados de identificação pode ser novamente traçada por meio de informações separadas (como, por exemplo, uma tabela que liga os pseudônimos a dados reais). Por isso, o Considerando (26) é explícito em considerar dados pseudônimos como dados pessoais[191].

Duas outras questões ganham relevância no contexto de *Big data* e Inteligência Artificial (objeto de consideração neste Ensaio): (***i)*** a "repersonalização" de dados anônimos, ou seja, a reidentificação dos indivíduos aos quais esses dados estão relacionados; e ***(ii)*** a inferência de outras informações pessoais a partir de dados pessoais já disponíveis.

Conforme antecipado, com o advento da IA a identificabilidade passou para outro patamar de possibilidades na medida em que a tecnologia potencializa a aplicação de métodos de correlações estatísticas, apoiadas em meios computacionais, aumenta-se exponencialmente a identificabilidade dos dados ditos "anônimos" — dados não identificados, aqui incluídos os dados anonimizados ou pseudonimizados — permitindo-se doravante que sejam eles conectados a indivíduos específicos.

---

[188] *Idem*.
[189] *Idem*.
[190] A pseudonimização é mencionada na LGPD (art.13) como medida a ser adotada (se possível) para se legitimar o tratamento de dados no âmbito dos estudos em saúde pública conduzidos por órgãos de pesquisa, a serem mantidos em ambiente controlado e seguro, e é criticada em razão da aparente discricionariedade conferida ao agente de tratamento. (FRAZÃO; CARVALHO; MILANEZ, 2022)
[191] "De acordo com o Considerando (9) do Regulamento 2018/1807 se os desenvolvimentos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais".

Importa dizer, mediante correlações estatísticas e a partir de dados não identificados, viabiliza-se a reidentificação do indivíduo a quem os dados se referem.

Sobre essa possibilidade, vale examinar as constatações empíricas mencionadas por Rocher et al (2019).

Em 2016, jornalistas teriam reidentificado políticos a partir de um conjunto de dados de histórico de navegação anônimo de 3 milhões de cidadãos alemães, descobrindo suas informações médicas e suas preferências sexuais.

Alguns meses antes, o Departamento de Saúde da Austrália teria publicado registros médicos não identificados para 10% da população o que permitiu que os pesquisadores os reidentificassem seis semanas depois[192].

Os autores relatam que, anteriormente, estudos já teriam mostrado que dados constantes em alta hospitalar, embora não identificados, podiam ter seus titulares reidentificados mediante análise de atributos demográficos básicos. Além disso, códigos de diagnósticos, como ano de nascimento, sexo e etnia podem identificar pacientes de forma única em dados de estudos genômicos[193].

Em outra situação, narram que os pesquisadores foram capazes de identificar indivíduos exclusivamente em trajetórias de táxi anônimas em NYC27, em viagens de compartilhamento de bicicletas em Londres, em dados de metrô em Riga e em conjuntos de dados de telefone celular e cartão de crédito[194].

A partir do caso “prático”, resta evidente que, com apoio das novas tecnologias associadas a IA e à *big data*, a análise contextualizada de dados específicos de natureza pessoal pode ser realizada de forma (re)contextualizada de sorte que mediante o processo de reidentificação aquelas informações aparentemente anônimas conduzem à identificação do respectivo titular[195].

No dizer dos referidos autores, a partir de qualquer configuração 'razoável' da informação - ainda que em si, inocente, se isoladamente considerada - no conjunto analisada

[192] SARTOR; LAGIOIA, 2020.
[193] *Idem.*
[194] *Idem*.
[195] *Idem.*

com outras informações (numa configuração modificada), é possível que ocorra a violação da privacidade (SARTOR, FAGIOIA, 2020)[196].

Assim, a reidentificação pode ser equiparada a um tipo especial de inferência de dados pessoais, uma vez que novos elementos, não identificados anteriormente, são adicionados no processo de associação na nova identificação do titular. É preciso observar, contudo, que para que um item seja vinculado a pessoa específica, não é necessário que o titular dos dados seja identificado com absoluta certeza, bastando um grau de probabilidade para permitir um tratamento diferenciado desse indivíduo (ainda que tal diferenciação se resuma no mero envio de publicidade direcionada)[197].

Das considerações dos autores referenciados, extrai-se que a existência de técnicas potencialmente aptas a dificultar a reidentificação — mediante desidentificação prévia ou mediante implementação de processos e medidas de segurança na liberação dos dados —, tais possibilidades estão sujeitas à falhas.

Conforme se observa, mediante aplicação de modelos algorítmicos, os sistemas computacionais de IA "podem" inferir novas informações sobre os titulares dos dados.

Uma questão relevante para fins de determinação do objeto protegido sob a lei protetiva de dados pessoais (para eventual contraposição com aquele tutelado sob o manto do segredo tecnológico) é saber se as informações inferidas devem ser consideradas como novos dados pessoais, distintos dos dados a partir dos quais foram inferidos. Subsiste, portanto, a questão de saber que se os dados inferidos — a partir desses recursos tecnológicos — são acessíveis ao titular dos dados originário, objeto do tratamento, ou se tais informações (dados inferidos) estariam cobertos pelo manto do segredo/confidencialidade.

Neste particular, SARTOR e LAGIOIA (2020) [198] sugerem detida reflexão sobre a possibilidade de que uma inferência relacionada com algum tipo de personalidade ou de orientação sexual possa ser tecnicamente realizada a partir da análise das características faciais ou com base em suas atividades *online* atribuídas ao titular dos dados analisados.

---

[196] *Idem*.
[197] *Idem.*
[198] V., nesse sentido, os estudos de Sartor e Lagioia (2020) sobre a compatibilidade da IA, tendo a RGPD como referencial normativo.

Alertam para o fato de que essa suposta orientação sexual, ou se o aventado tipo de personalidade inferido, enquanto resultante de estimativa (inferência) probabilística, poderá se constituir em elemento integrante dos dados pessoais do indivíduo a ele referido. Em tom reflexivo indagam: e se tais estimativas (inferidas) são utilizadas para embasar decisões que poderão afetar a esfera de interesses juridicamente protegidos do indivíduo em causa?

HOFFMANN-RIEM (2021, p. 208)[199] parece corroborar com tal linha de preocupações ao sugerir que a evolução das técnicas de desanonimização coloca em xeque a anonimização inicialmente imaginada, medida por si só insuficiente para desvinculação do titular aos dados em questão, quando se leva em conta que todas as possibilidades tecnológicas de desanonimização poderão ser exploradas.

O autor considera, neste aspecto, a necessidade de efetivamente estender o conceito de relação pessoal a dados anonimizados, para nele abranger os processos de desanonimização, mesmo porque a partir do processo de agregação de dados torna-se possível tirar conclusões sobre indivíduos específicos[200].

Contudo, pondera o autor que embora a adoção de conceito de dados pessoais estendido se afigure necessária e benéfica na proteção de dados individuais nos domínios de *Big data*, tal medida não será suficiente para cobrir todas as áreas problemáticas associadas a essas tecnologias[201].

Em meio a essa miríade de questões "existenciais" a demandar soluções no âmbito da regulação protetiva de dados pessoais (algumas delas exploradas neste Trabalho), recorre-se à experiência europeia, com base na análise levada a efeito por SARTOR e LAGIOIA (2020, p. 38 et seq.)[202], refletida no relato adiante parafraseado.

No primeiro caso, tem-se a interpretação jurisprudencial no tocante ao "status legal" de informações automaticamente inferidas e aquela obtida/inferida mediante intervenção humana. Ao fim e ao cabo, busca-se saber se em detrimento das incertezas em relação às afirmações relativas a indivíduos tais inferências e raciocínios (realizados por humanos e não de forma "automática") poderiam ser igualmente considerados dados pessoais.

---

[199] HOFFMANN-RIEM, 2021, p. 208.
[200] HOFFMANN-RIEM, 2021, p. 103.
[201] *Idem.*
[202] SARTOR; LAGIOIA, 2020.

Questão com esses contornos (especificamente relacionada com um pedido de autorização de residência) fora examinada por tribunal local — TJ nos Processos Comuns C-141 e 372/12[203] —, restando negado que a análise jurídica levada a efeito pelo funcionário competente pudesse ser considerada "dados pessoais" para os efeitos legais, concluindo-se, contudo, que no conceito poderiam ser enquadrados (como dados pessoais) tão somente os dados nos quais se baseou a análise (os dados de entrada sobre o recorrente), bem como a conclusão final da análise (a decisão de indeferimento do pedido), os quais deveriam ser considerados dados pessoais.

Em suma, a qualificação pessoal inferida não se aplicaria às etapas intermediárias (as conclusões intermediárias na cadeia de argumentos) que levaram à conclusão final, esta sim, em tese integrante dos dados pessoais, se implicada com o indivíduo específico.

Em outra decisão — relacionada com o exercício de proteção de dados pessoais visando explicação e revisão no âmbito do roteiro de exame e dos comentários dos examinadores — o mesmo TJE (processo C-434/16,72)[204] concluiu que os comentários dos analistas integravam os dados pessoais, neste ponto aparentemente divergindo do entendimento proferido nos processos anteriores (C-141 e 372/12).

Em ressalva, anotam os autores, na interpretação do Tribunal, embora os direitos de proteção de dados pessoais em geral e o de retificação em particular sejam conexos com a finalidade do tratamento, isso não implicaria o direito de ter corrigidas as respostas do candidato ou os comentários do examinador, a menos que tivessem sido registradas incorretamente.

Em outros termos, aduzem os comentadores referenciados[205] ainda com base no entendimento do TJCE (Tribunal de Justiça da União Europeia), que a lei de proteção de dados não visa garantir a precisão dos processos decisórios ou boas práticas administrativas, de sorte que, na hipótese analisada, o examinando teria o direito de acessar tanto os dados do exame (as respostas do exame) quanto ao raciocínio baseado nesses dados (os comentários), mas não teria o direito de retificar ou corrigir nem as inferências dos examinadores (o raciocínio), tampouco o resultado final.

[203] A questão em análise teve origem em pedido de autorização de residência, a questão era saber se a análise poderia ser considerada dado pessoal. (INFOCURIA, 2014).
[204] INFOCURIA, 2014.
[205] SARTOR; LAGIOIA, 2020.

Ainda no que se refere à questão dos dados inferidos, Sartor e Lagioia (2020) trazem a opinião do WP ao Artigo 29º[206] no tocante à amplitude da definição de dados pessoais e que nela estão abarcadas as inferências automatizadas (elaboração de perfis), parecendo não haver dúvida de que, sob a perspectiva da regulação da União Europeia, aos titulares dos dados é conferido o direito de acessar tanto os dados de entrada quanto as conclusões (finais ou intermediárias), automaticamente inferidas a partir dos dados a eles relacionados, ainda que indiretamente[207].

Em solo pátrio, a polêmica em torno do conceito de dados pessoais afeta a interpretação dos parâmetros do Art. 20 da LGPD relacionados com a garantia do potencial direito de explicação e mesmo de oposição em relação aos dados inferidos utilizados em apoio a uma decisão automatizada.

De fato, em primeira leitura, o dispositivo parece sinalizar que o titular de dados terá acesso aos critérios e à lógica decisória, elementos indispensáveis para mínima inteligibilidade e compreensão "do que, como, e porque" foi decidido. [208]

Neste aspecto, Frazão, Carvalho e Milanez (2022, p.341, et seq.) entendem que a invocação do segredo de negócios — em tese apta a fundamentar negativa de revelação de todos os passos do julgamento algorítmico — não obstaria o acesso do titular aos dados a ele relacionados e integrantes dos "i*nputs*" e dos "*outputs*" de uma decisão automatizadas[209].

Em declarado alinhamento com outras vozes da doutrina nacional, os mesmos autores[210] destacam ainda ser necessário o avanço do debate com vistas à definição de um ponto de equilíbrio que conjugue a proteção do segredo de negócios com a expectativa de transparência e com o direito de autodeterminação conferido aos titulares de dados, no ponto em que abstratamente lhes assegura acesso às informações que a eles se relacionem.

---

[206] O Grupo de Trabalho do Artigo 29.º (GT Art. 29.º) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD). (EDPB, 2023)

[207] Parecer nº 216/679, adotado em 3 de outubro de 2017, revisto em 6 de fevereiro de 2018 (https://ec.europa.eu>article29>documentCOMISSÃO EUROPEIA, 2018)

[208] O entendimento, nesse particular, no âmbito do direito à portabilidade, parece se afastar da regra de inclusão dos dados inferidos, pelo controlador, de sorte a admitir que o "direito a portabilidade" abrange somente aqueles dados fornecidos pelo próprio titular, tudo aos auspícios da tutela do segredo de negócios. (SCUDIERO, 2017 *apud* FRAZÃO; CARVALHO; MILANEZ, 2022)

[209] FRAZÃO; CARVALHO; MILANEZ, 2022.

[210] *Idem*.

Nesse desafio, em tópico seguinte examina-se outras relevantes polêmicas derivadas da interpretação do artigo 20 da LGPD.

4.2 CONCEITO DE DECISÕES AUTOMATIZADAS POR SISTEMAS DE INTELIGÊNCIA ARTIFICIAL NA LGPD

A Lei Geral de Proteção de Dados (LGPD), em seu artigo 20, estabelece a disciplina aplicável ao direito de revisão de decisões tomadas unicamente com base no tratamento automatizado de dados pessoais que afetem os interesses do titular[211]. Isso inclui decisões destinadas a definir seu perfil pessoal, profissional, de consumo, de crédito ou aspectos de sua personalidade. O parágrafo 1º trata do procedimento aplicável à solicitação de informações pelos titulares dos dados pessoais sobre os critérios e procedimentos utilizados para a decisão automatizada [212] . O controlador é obrigado a fornecer, de forma clara e adequada, as informações solicitadas, exceto quando envolver segredos comerciais e industriais, sujeitando-se a auditorias da autoridade nacional de proteção para verificar aspectos discriminatórios no tratamento automatizado de dados pessoais.

Muitas polêmicas e controvérsias têm suscitado a leitura do texto normativo e é preciso então empreender esforços para identificar o cerne do debate e, quiçá, no futuro, examinar a aplicabilidade das eventuais soluções que venham a ser apontadas.

É importante destacar que a LGPD não oferece uma definição do termo 'decisão automatizada' mencionado no Artigo 20, sendo necessário buscar essa definição na doutrina especializada. Geralmente, a expressão refere-se às etapas em que um sistema computacional toma uma decisão sem intervenção humana. Essa decisão é resultado das operações do sistema e se assemelha ao processo decisório humano (ALMADA, 2020) [213].

---

[211] RGPD: art. 22, § 1, 3; 13, § 2 f.; 14, § 2, alínea g; 15, § 1 Hs. 2, alínea h".

[212] Lei Complementar nº 95, de 1998, que dispõe sobre a elaboração, a redação, a alteração e a consolidação das leis, conforme determina o parágrafo único do art. 59 da Constituição Federal, e estabelece normas para a consolidação dos atos normativos que menciona: "Art. 11. (...) III. para obtenção de ordem lógica: (...) b) restringir o conteúdo de cada artigo da lei a um único assunto ou princípio; c) expressar por meio dos parágrafos os aspectos complementares à norma enunciada no caput do artigo e as exceções à regra por este estabelecida; (...)" (g.n.)

[213] ACEMOGLU, RESTREPO, 2018 *apud* ALMADA, 2020.

Isoladamente, os termos "decisão" e "automatizada" parecem sugerir vagamente a imagem da evolução do uso de computadores (designadamente, "máquinas automáticas de tratamento da informação", segundo a Lei do Software[214]).

Por seu turno, a expressão *decisão automatizada* é frequentemente usada em referência às etapas em que um sistema computacional "toma" uma decisão "sem" o concurso de uma ação humana, o que enseja a ideia de que a aludida decisão foi resultado não só das operações deste sistema como também se assemelha ao processo decisório normalmente seguido pelos humanos.

No entendimento de ACEMOGLU e RESTREPO (2018), tornou-se corriqueira a menção conjunta dessa expressão com a inteligência artificial, notadamente no contexto do mercado de trabalho, no âmbito do qual se considera que as atividades profissionais humanas podem em certa medida ser decompostas e passíveis de automação. Tarefas simples — por exemplo, carregar uma caixa — podem ser substituídas pela ação de um robô (que na hipótese, faz a força que seria necessária para deslocar a caixa).

Conforme esses autores, com base na ideia de que, em tese, não há limites para que ocorra a substituição da ação humana pelo autômato, inclusive nas atividades mais complexas, seguiram-se os desenvolvimentos para a automação de atividades em que estão presentes fatores de incertezas, sujeitos naturalmente ao interesse e/ou impacto envolvidos na tomada de decisão.

Entretanto, lembram os especialistas que o artefato somente pode emular uma parte calculável da inteligência humana, não o livre-arbítrio, não os sentimentos, não as emoções.

Ademais, enquanto ação de uma máquina, a decisão somente pode ser assim denominada em seu sentido metafórico uma vez que ela não "age" de modo consciente ou "com propósito", limitando-se a efetuar cálculos aritméticos, conforme as regras ditadas pelo programador e com base nos dados inseridos no modelo (algoritmo) [215].

---

[214] Lei nº 9.609, de 1998: "Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados."

[215] "O que distingue a inteligência humana da Inteligência Artificial (IA)? A inteligência viva não é uma máquina de cálculos. É um processo que articula afetividade, corporalidade e erros. Em seres humanos, é pressuposta a presença de desejo e da consciência de sua própria história em longo prazo. A inteligência humana não é concebível

As decisões ou julgamentos tomados por máquinas são pautados em *predições* realizadas a partir de critérios, regras predeterminadas e demais "dados de entrada", como aqueles representativos de imagens, textos, sons etc., por sua vez convertidos em "linguagem" compreensível para a máquina (código em formato digital legível para o computador)[216].

A predição consubstancia o conhecimento adquirido pelo algoritmo (ou modelo) na fase de treinamento (nesta fase, denominados dados de treinamento). Predição e julgamento — pautados em dados de entrada — traduzem a escolha da solução, expressa no algoritmo ou no modelo[217] e denotam idealmente o interesse do programador ou do desenvolvedor[218][219].

A decisão automática se direciona para a saída dos dados e é indicativa de que a ação humana a ser efetivada pelo humano ou por outra máquina tende a convergir para o resultado pretendido pela respectiva ação, eventualmente associada a uma recompensa[220], ainda que não se descarte a hipótese de retorno desses dados para eventual reavaliação.

---

separadamente de todos os outros processos cerebrais e corporais. Diferente de humanos ou animais que pensam com a ajuda de um cérebro localizado dentro de seus corpos – que existe em um meio ambiente – uma máquina processa cálculos e premonições sem a capacidade de dar sentido a eles. A ideia de que uma máquina pode substituir humanos é, de fato, absurda. É o ser vivo que cria significado, não a computação. Muitos pesquisadores de IA estão convencidos de que a diferença entre a inteligência viva e a inteligência artificial é quantitativa, enquanto ela é qualitativa". opinião de Miguel Benasayag, expressa em entrevista a Régis Meyran, em artigo intitulado "São os humanos, não as máquinas, que criam significado" (MEYRAN, 2018).

[216] AGRAWAL; GANS; GOLDFARB, 2018 *apud*. REIS; FURTADO, 2022.

[217] No sistema de IA, o modelo poderá corresponder a um conjunto de algoritmos, e normalmente o são. Todo modelo é composto de algoritmo, embora o inverso não seja verdadeiro. Nas palavras de Kearns e Roth (2019, p. 9): "*These models, which make the actual decisions of interest, are the result of powerful machine learning (meta-)algorithms being applied to large, complex datasets*". [Em tradução livre: "Esses modelos, que tomam as decisões reais de interesse, são o resultado de poderosos algoritmos de aprendizado de máquina (meta) aplicados a conjuntos de dados grandes e complexos."].

[218] AGRAWAL; GANS; GOLDFARB, 2018, p. 74 *apud* REIS; FURTADO, 2022.

[219] Nesse particular, é oportuno o esclarecimento de Ricardo Silveira Ribeiro (2022): "Na origem, os cientistas esperavam que programas complexos pudessem ensinar computadores a simular tarefas tipicamente humanas (RUSSELL; NORVIG, 2016, p. 17). Os sistemas computacionais não teriam então a habilidade de aprender, por si mesmos, a mimetizar o comportamento humano; teriam que ser detalhadamente programados para isso. Na década de 1980, contudo, fortaleceu-se uma segunda tradição de pesquisa, denominada *machine learning* (aprendizado de máquina). Nessa abordagem, há o desenvolvimento de algoritmos capazes de ensinar o computador a aprender com os dados a ele informados como *inputs* (imagens, vídeos, planilhas, textos ou sons) (GOODFELLOW; BENGIO; COURVILLE, 2016, p. 2; SEJNOWSKI, 2018, p. 40). Assim como aprendemos desde crianças a distinguir, intuitivamente e por experiência, imagens e sons de diferentes animais e pessoas, os algoritmos de *machine learning* permitem 'alimentar' um sistema computacional com um número suficientemente grande de 'exemplos' (*inputs*), para que ele seja 'ensinado' a distinguir ou revelar padrões nos dados. Com isso, informações preciosas podem ser analisadas e sintetizadas automaticamente com o objetivo de fornecerem parâmetros objetivos para a tomada de decisão. A despeito dessa vantagem, há um risco latente nessa abordagem: como a sociedade é permeada por desigualdades, modelos de *machine learning* são também capazes de 'aprender' a reproduzir políticas discriminatórias presentes no ambiente socioeconômico e, sem medidas corretivas, podem até mesmo gerar um círculo vicioso de retroalimentação, no qual o sistema de inteligência artificial contribui para o agravamento de problemas sociais."

[220] AGRAWAL; GANS; GOLDFARB, 2018, p. 74 *apud* REIS; FURTADO, 2022.

De fato, o ciclo poderá ser contínuo e haverá momentos em que o tomador de decisão (humano ou máquina), em retorno, possa recorrer a novas informações de entrada, reavaliando aquelas coletadas no cenário original específico, inicialmente consideradas como *insumos* (*inputs*), para com base nelas fazer novas *predições*[221] dos novos desfechos possíveis e propiciando as escolhas de ações alternativas cabíveis no novo contexto.

Conforme descreve AGRAWAL, 2018, *apud* REIS e FURTADO, 2022[222], essas etapas abrangem todo o processo de tomada de decisão automatizada, desde a aquisição de dados até o ajuste contínuo do modelo para garantir resultados precisos e confiáveis; e, em princípio, poderiam ser resumidas nos seguintes pontos:

1. Aquisição de dados: nesta fase, os dados relevantes são coletados e armazenados para uso posterior no processo de tomada de decisão.

2. Preparação de dados: os dados coletados são preparados para serem utilizados pelo modelo de IA, incluindo a limpeza, integração e transformação de dados.

3. Modelagem: nesta etapa, o modelo de IA é criado e treinado com base nos dados preparados.

4. Validação: o modelo é validado para garantir que ele esteja produzindo resultados precisos e confiáveis.

5. Uso: o modelo é utilizado para tomar decisões automatizadas com base nos dados de entrada.

6. Monitoramento: o modelo é monitorado para garantir que continue funcionando corretamente e para detectar possíveis problemas ou erros.

7. Ajuste: se necessário, o modelo é ajustado para melhorar sua precisão e eficácia na tomada de decisões.

[221] Salientam Agrawal e outros (2018 *apud* ALMADA, 2020) que o termo *predição* está relacionado ao acesso a determinada informação oculta. A existência de lacunas no registro histórico impede o acesso a determinadas informações atuais ou passadas e a predição nos sistemas de IA vale-se da "dedução" para inferir a informação faltante a partir dos dados disponíveis, atuais ou não. Inclui na predição as ações cabíveis, com base em avaliações em relação aos desfechos possíveis, segundo variáveis externas aplicáveis a cada alternativa de escolha; diante de imposições legais que tornaria ilícita a decisão, outra escolha poderá ser considerada, uma ação alternativa poderá ser desejável. Os resultados prováveis ou efetivos comporão o resultado da ação considerada no processo, em conformidade ou não com a previsão, servindo de "retorno" ou "novos subsídios" (novos dados de entrada, *inputs*) que subsidiariam a tomada de decisão seguinte, sujeita a novo processo de predição ou nova reavaliação, em processo contínuo de aprendizagem, com base nos resultados, efeitos ou consequências das próprias ações. (ALMADA, 2020)

[222] AGRAWAL; GANS; GOLDFARB, 2018, p. 74 *apud* REIS; FURTADO, 2022.

Como se verifica, o algoritmo do sistema de IA vale-se de dados de treinamento para experimentos; é a partir desses passos que os dados de treinamento são aprimorados por meta-algoritmos que otimizam o trabalho de construção do modelo, revisando continuamente os dados de saída, perseguindo o resultado desejado pelo programador, no sentido de adequadamente agrupá-los e interrelacioná-los. Desses meta-algoritmos, o mais conhecido e usado é o *back propagation*, que, em resumo, consiste num conjunto de instruções para reanalisar continuamente os dados de saída corrigindo erros de avaliação porventura detectados, mediante um processamento inverso, seja melhorando o desempenho do modelo, seja reequilibrando os pesos dos fatores em jogo para a tomada de decisão (AGRAWAL, 2018, *apud* REIS e FURTADO, 2022, p.10)[223].

Para além do programa do computador (genericamente falando, "algoritmos"), é preciso considerar que a robustez e acurácia de uma decisão automatizada depende da qualidade (e quantidade) de dados, os quais são classificados em três principais tipos: ***a)*** os dados de treinamento; ***b)*** os dados de entrada; e ***c***) os dados de feedback.

Os *dados de treinamento* antecedem o funcionamento do programa; já na primeira fase de aplicação ou de interação com o ambiente, tem-se os *dados de entrada*; a geração do resultado do processo "decisório" corresponde aos dados de saída, os quais, eventualmente, "retornam" à máquina, tal qual os "dados de entradas", para reinício/reavaliação, como *feedback* positivo ou negativo, viabilizando o autoajuste (na dimensão "autônoma") sem prejuízo de ajustes a cargo do desenvolvedor (neste âmbito, uma intervenção humana no processo decisório, a princípio automatizada)[224].

Com base em exemplos da "vida real", REIS e FURTADO (2022, p.11) traçam o seguinte roteiro (transcreve-se):

---

[223] Esse tipo de meta-algoritmo é usado para otimizar mecanismos de *deep learning* mais utilizados atualmente em aplicações práticas da chamada Inteligência Artificial. (AGRAWAL; GANS; GOLDFARB, 2018, 21 e ss. *apud* REIS; FURTADO, 2022, p. 10)

[224] "Como explicam Ajay Agrawal, Joshua Gans e Avi Goldfarb [2018], quando a máquina toma uma decisão, ela usa dados de entrada (imagens, textos, sons etc., que têm de ser reduzidos a um formato digital legível pela máquina), para fazer uma predição. A predição está baseada no 'conhecimento' que o algoritmo ou modelo adquiriu na fase de treinamento, com os chamados dados de treinamento. Combinando a predição com o julgamento (escolha da solução, segundo o interesse do programador/desenvolvedor, expresso no algoritmo ou modelo), a máquina de decisão automática indica uma ação a ser efetivada (por humano ou outra máquina) e essa ação leva a um resultado (eventualmente com uma recompensa associada pelo programador). O resultado fornece ao modelo um *feedback* (positivo ou negativo), que assim realimenta todo o processo para decisões futuras". (REIS; FURTADO, 2022)

> (...) por exemplo, uma máquina de reconhecimento facial para fins de localização de possíveis foragidos da justiça que estejam circulando em áreas públicas funciona da seguinte maneira: 1º) ela coleta os dados automaticamente (imagens), por meio de câmeras apontadas para os transeuntes em vias públicas (dados de entrada); 2º) o modelo utilizado para analisar esses dados, comparando-os com as imagens dos foragidos armazenadas em seus arquivos, foi previamente treinado com dados de muitos prisioneiros (dados de treinamento), de modo a fazer a associação tida como "correta" pelo programador; 3º) feito o cruzamento, se for encontrado uma correspondência (*match*), a máquina faz a *predição* de que ali está um foragido, com base no alto nível de probabilidade de a imagem coincidir com a do foragido X, por exemplo; 4º) em seguida, a máquina "julga" e aponta aquele suspeito para o operador; 5º) com base nesse julgamento, adota-se uma ação, que são os atos posteriores (que podem ser humanos ou automatizados também—no caso, a detenção do sujeito) que levarão ao resultado (no caso, prisão correta ou incorreta). Conforme esse resultado tenha sido correto ou incorreto, a depender de uma análise humana posterior, a máquina é informada, por *feedback*, para reforçar ou não aquele julgamento[225].

Em relação ao funcionamento do processo decisório automatizado, por ora, cumpre destacar que à semelhança do funcionamento da mente humana, o processo automatizado — no caso, do modelos de IA, que trabalham com *machine learning*, especialmente os de *deep learning* — procura reproduzir a capacidade adaptativa do cérebro humano na busca por reconhecimento de padrões, visando à generalização e ajustes nesses padrões[226] (aspecto central do desenvolvimento das aplicações que se convencionou denominar de inteligência artificial)[227].

REIS e FURTADO (2022) [228] asseveram que no ciclo do processo da decisão automatizada os dados pessoais integram tanto os "dados de entrada" como os "dados de saída", estes últimos correspondentes ao "julgamento" (ou decisão automatizada propriamente dita). Depreende-se daí que na medida em que esses "dados de saída" correspondam a determinada

---

[225] REIS; FURTADO, 2022, p. 11.

[226] Aspectos do funcionamento do cérebro humano, no tocante aos julgamentos e escolhas, são explorados por Daniel Kahneman (2012).

[227] ERTEL, Wolfgang. *Introduction to Artificial Intelligence*. Cham (Switzerland): Springer, 2017, *apud* REIS, Nazareno César Moreira; FURTADO, Gabriel Rocha. ***Decisões automatizadas: definição, benefícios e riscos*.** Civilistica.com. Rio de Janeiro, a. 11, n. 2, 2022. Disponível em: <http://civilistica.com/decisoes- automatizadas/>. Data de acesso.

[228] Op. Cit. REIS, N. C. M.; FURTADO , G. R**. Decisões automatizadas: definição, benefícios e riscos**. civilistica.com, v. 11, n. 2, p. 1-44, 7 out. 2022. https://civilistica.emnuvens.com.br/redc/article/view/763, acesso em 31.01.2023

pessoa natural eles passariam a integrar o conteúdo do direito de explicação, *direito subjetivo* atribuído a essa pessoa identificada ou identificável, se afetada pela decisão automatizada[229].

Da imbricação desses aspectos "técnicos" com os elementos normativos (LGPD: Artigo 20), os aludidos autores com argúcia asseveram que sempre haverá um titular dos dados (sejam dos dados de entrada sejam dos dados de saída) e que a indicação clara, nos domínios da decisão automatizada, é que a esse titular (pessoa natural a quem os dados pessoais se referem) que a norma confere o direito de solicitar a revisão da decisão respectiva[230].

Em suma, as decisões tomadas por máquinas são baseadas em predições feitas com base em critérios e regras predeterminados, utilizando dados de entrada. Essas predições refletem a escolha da solução no algoritmo ou modelo, expressando o interesse do programador ou desenvolvedor. A decisão automática busca alcançar o resultado desejado e pode ser ajustada com base em feedback e novas informações.

O processo de tomada de decisão automatizada abrange etapas como a aquisição e preparação de dados, modelagem do sistema de IA, validação, uso, monitoramento e ajuste contínuo do modelo. A qualidade dos dados é fundamental para a robustez e acurácia das decisões automatizadas.

De acordo com a LGPD, os dados pessoais fazem parte tanto dos dados de entrada como dos dados de saída do processo decisório automatizado. Portanto, o titular dos dados tem o direito de solicitar a revisão da decisão automatizada que o afete. A LGPD também estabelece a obrigação de fornecer informações claras e adequadas sobre os critérios e procedimentos utilizados, levando em consideração os segredos comercial e industrial.

---

[229] "Os dados de uma pessoa coletiva (jurídica) não se enquadrariam na definição legal do art. 5º, I da LGPD, referida exclusivamente à pessoa natural. (...) processos de automatização adotados em atividades que não envolvam dados pessoais, não estão abrangidos pela disciplina da LGPD. Um caso particularmente interessante é o da pessoa jurídica. Os dados relativos a pessoas jurídicas não são dados pessoais, de modo que o tratamento automatizado de dados relacionados às pessoas jurídicas não estão no raio de incidência da norma da LGPD que assegura os direitos de revisão e de explicação—embora não fique excluída a hipótese de se buscar tais direitos, sobretudo em casos de assimetria negocial, por aplicação analógica do Código de Defesa do Consumidor, ou de alguma normativa protetiva específica, ou até mesmo por aplicação direta da Constituição, com base na ideia mais geral de proteção de dados como direito fundamental extensível também às pessoas jurídicas". (REIS; FURTADO, 2022)

[230] Em esclarecimento da definição, observam "(...) há muitos processos automatizados na indústria ou na pesquisa científica que, no entanto, não produzem 'decisões', no sentido empregado pela legislação brasileira. Em uma pesquisa científica sobre uma bactéria, por exemplo, pode-se usar processos automatizados para avaliar e prever aspectos ou comportamentos dessa forma de vida, sem que se possa falar, no entanto, em 'decisão automatizada', na acepção jurídica da expressão. O mesmo pode ocorrer numa fábrica de parafusos que automatize os processos de avaliação da qualidade de seus produtos: isso não gera decisões automatizadas, no sentido empregado pela LGPD". (REIS; FURTADO, 2022)

É importante questionar se a LGPD trouxe inovações ao ordenamento jurídico, uma vez que a Lei do Cadastro Positivo já previa a obrigação de fornecer informações sobre decisões automatizadas, levando em conta segredos comerciais e industriais. Além disso, é necessário esclarecer se a possibilidade de auditoria está limitada apenas a casos de recusa de explicação adequada. A Autoridade Nacional de Proteção de Dados (ANPD), criada pela LGPD, possui competência exclusiva para determinar auditorias, mas em tese elas se aplicam apenas à verificação de aspectos discriminatórios no tratamento automatizado de dados pessoais."

4.3 DADOS SENSÍVEIS E DECISÕES AUTOMATIZADAS POR INTELIGÊNCIA ARTIFICIAL

Na busca de resposta(s), é preciso ir além da ideia geral do regime proprietário, sendo necessário refletir sobre a questão: a quem pertence os dados pessoais?[231]. Afirmações como "os dados pessoais pertencem à pessoa natural, a quem os dados estão relacionados"; "os segredos comerciais pertencem à empresa que os mantém em segurança/confidencialidade" ou "as obras digitais pertencem ao respectivo autor e as bases de dados pertenceriam aos empreendedores que investiram na coleta e organização dos dados", não são aptas a esclarecer a questão.

As preocupações externadas no debate em torno da regulação da IA parecem corroborar a ideia de proteção do indivíduo e em certa medida relativizar a interpretação "patrimonialista" que a definição legal por hipótese propicie.

Por ocasião do debate em torno do marco legal da IA, Danilo DONEDA[232] expressa opinião no sentido de que *"a centralidade do elemento humano* [que] *deve ser enfatizada em todos os seus aspectos, em todos os pontos necessários"* com isso parecendo sinalizar que se essa tecnologia é tão necessária então os instrumentos e soluções regulatórias a ela concernentes

[231] O título provocativo é enunciado por Laura Schertel Mendes ao se propor a responder a respectiva questão, num dos tópicos de "Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.".

[232] Por ocasião da instalação da Comissão de Juristas, pelo Senado Federal, para elaboração de subsídios ao projeto de regulação da IA, Danilo Doneda (*in memoriam*) lembra que "a centralidade do elemento humano [que] deve ser enfatizada em todos os seus aspectos, em todos os pontos necessários. Nossa missão certamente será propor e pesquisar instrumentos e soluções regulatórias que não contradigam e não impeçam a aplicação da inteligência artificial, que pode ser, inclusive, necessária, mas que facilitem e incentivem a sua adoção, diminuindo riscos e garantindo a segurança jurídica (...)". (BRASIL, 2022, p. 18)

deverão viabilizar a sua efetiva aplicação, seja no sentido de mitigar os possíveis riscos, seja assegurando previsibilidade jurídica, com isso potencializando a confiança no livre fluxo de dados, condição essa reputada essencial ao desenvolvimento sustentável da IA.

Aparentemente alinhadas com essas expectativas estão as preocupações da Organização Mundial da Propriedade Intelectual (OMPI), em tese representativa dos atores globais hegemônicos[233] da comunidade interessada na propriedade intelectual.

Ao que se depreende, no entendimento dessa organização (GURRY, 2019), a regulação de dados não precisa necessariamente definir a atribuição da propriedade em relação aos dados, bastaria sim estabelecer a liberdade ou restringir o respectivo fluxo.

Eis a opinião de Francis Gurry expressa na Revista da OMPI, edição de outubro de 2019[234], *verbis*:

> No momento, nada me leva a crer no advento de um novo direito de propriedade registrável para dados. Se um novo direito surgir, será o resultado do posicionamento da sociedade quanto à coleta, ao armazenamento e ao uso ilícitos dos dados. Tudo o que estiver fora dessa esfera será considerado lícito. Uma vez instauradas, as restrições poderão ser consideradas a base de direitos excludentes do que normalmente consideramos propriedade. A título de ilustração, tomemos o código babilônico de Hamurabi, que data de 1754 a.C. Esse conjunto de leis não confere o direito de propriedade de ovelhas, simplesmente estipula que furtar a ovelha de um vizinho é ilegal e passível de punição. Desse modo, quando criamos restrições ao livre fluxo de dados no que diz respeito à coleta, ao armazenamento e ao uso, elas podem, a certa altura, equivaler a um direito de propriedade.

Para Laura Schertel MENDES[235] , há que se afastar eventual compreensão no sentido de que a regulação de proteção de dados vise atribuir um direito de propriedade.

---

[233] "A Organização Mundial da Propriedade Intelectual (OMPI; em inglês, *World Intellectual Property Organization*, WIPO) é uma entidade internacional de Direito Internacional Público com sede em Genebra (Suíça), integrante do Sistema das Nações Unidas. Criada em 1967, é uma das 16 agências especializadas da ONU e tem por propósito a *promoção da proteção da propriedade intelectual ao redor do mundo através da cooperação entre Estados*. O atual Diretor-Geral da OMPI é o australiano Francis Gurry. (...) Ainda que se alegue certa eqüidade entre os Estados-membros da OMPI pela regra do '*Um país, um voto*', na prática esta eqüidade não se verifica. Frequentemente os Estados e blocos mais ricos, particularmente os EUA e Europa, são quem, efetivamente, guiam a agenda da OMPI e têm seus interesses prevalecidos. Contribui para isso, ainda, o fato de a OMPI dar grande poder ao Secretariado para contornar, muitas vezes, os desejos dos Estados-membros". (ORGANIZAÇÃO..., 2023, g.n.)

[234] PROPRIEDADE..., 2019.

[235] MENDES, 2014.

Por definição, ensina a doutrinadora, o instituto da Proteção de Dados tem natureza multidimensional, objetiva equilibrar os direitos de proteção, de defesa e de participação do indivíduo nos processos comunicativos.

Em suma, o instituto presta-se a proteger a personalidade do indivíduo contra os riscos ocasionados pela coleta, processamento e circulação de dados pessoais, cuja exploração, ao que se sabe, tem base na mineração (*data mining*) [236] e poderá afetar as liberdades e direitos fundamentais do indivíduo, aspecto objeto de abordagem na seção seguinte.

SARTOR e LAGIOIA (2020, p. 84)[237], em referência ao contexto da União Europeia, apontam para a necessidade de adequada interpretação e aplicação de alguns princípios tradicionais de proteção de dados para os *dados sensíveis*, prudência essa necessária diante das demandas por possível harmonização regulatória e plena implantação da IA e *big data*[238].

[236] "A 'mineração de dados' (do inglês '*data mining*') consiste em uma grande gama de práticas que se valem de um conjunto de ferramentas para descoberta de informação e sua consequente transformação em conhecimento. Esse conjunto de técnicas também pode ser chamado de 'Descoberta de Conhecimento em Bases de Dados, ou '*Knowledge Discovery in Databases*' (KDD), e se trata da tentativa de solucionar problemas relacionados ao aumento exponencial da quantidade de dados disponíveis atualmente" (CAMILO; SILVA, 2009, p. 3). "A mineração de dados é motor da chamada economia digital, ou da mercantilização dos dados, em que os dados pessoais se transformam em mercadoria. Consolida-se, conforme Ciuriak (2018), uma economia orientada por dados como um modelo novo de negócios formado por: (I) assimetria informacional entre usuários e controladores de dados; (II) a industrialização do aprendizado nas inteligências artificiais; (III) economia monopolista, proliferando-se as chamadas *big techs*; (IV) novas formas de transação de ações; e (V) riscos sistêmicos devido às vulnerabilidades das infraestruturas de proteção de dados". (FORNASIER; KNEBEL; SILVA, 2020)

[237] "*It has been argued that the GDPR would be incompatible with AI and big data, given that the GDPR is based on principles – purpose limitation, data minimisation, the special treatment of 'sensitive data', the limitation on automated decisions – that are incompatible with the extensive use of AI, as applied to big data. As a consequence, the EU would be forced to either renounce application of the GDPR or lose the race against those information-based economies – such as the USA and China – that are able make full use of AI and big data* (ZRSKI, 2017, HILDEBRANDT, 2015) *Contrary to this opinion, this report shows that it is possible – and indeed likely – that the GDPR will be interpreted in such a way as to reconcile both desiderata: protecting data subjects and enabling useful applications of AI. It is true that the full deployment of the power of AI and big data requires collecting vast quantities of data concerning individuals and their social relations, and that it also requires processing of such data for purposes that were not fully determined at the time the data were collected. However, there are ways to understand and apply the data protection principles that are consistent with the beneficial uses of AI and big data*". (SARTOR; LAGIOIA, 2020).

[238] A *big data* envolve a coleta de grandes quantidades de dados sobre indivíduos e suas relações sociais e o processamento desses dados por vezes (ou via de regra) para fins que não foram totalmente determinados no momento da coleta (SARTOR; LAGIOIA, 2020)

A necessidade de especial atenção[239] em relação aos dados sensíveis[240] é prevista também no âmbito da LGPD, que não menciona, nem distingue, a forma ou técnica a ser empregada no tratamento dessa especial categoria de dados pessoais.

Num primeiro ponto, os autores ao início referenciados asseveram que as tecnologias de IA e *big data* possibilitam a "reidentificação" daqueles dados aparentemente não identificados e em tese não vinculados a um indivíduo específico e, nesse contexto atentam para o fato de que esse processo de reidentificação de dados sensíveis pode ter consequências graves para o titular dos dados.

À guisa de exemplo, mencionam caso em que registros médicos não identificados foram disponibilizados ao público e mediante posterior reidentificação foram divulgadas as condições médicas dos indivíduos envolvidos para conhecimento público (v. seção 5.2)[241].

O segundo aspecto apontado pelos autores concerne aos desafios relacionados com as inferências algorítmicas. Graças à IA e *big data* é possível vincular o comportamento

---

[239] Atenção especial também é conferida para o tratamento de dados de **crianças e adolescentes, aos quais se aplicam as regras específicas relativas ao consentimento, extensão e finalidade do tratamento.** V. LGPD: "Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei. § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo. § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis. § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança."

[240] Por **"dados sensíveis"** (LGPD: art. 5º, II) **entende-se a categoria particular de dado pessoal definida como aquele vinculado ao respectivo titular, pessoa natural, e relacionado a** origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, ou referente à saúde ou à vida sexual, dado genético ou biométrico.

[241] Sartor e Lagioia (2020) recorrem a Rocher *et al* (2019) para mencionar (nota 66 da publicação respectiva) as seguintes situações concretas: "[*N]umerous supposedly anonymous datasets have recently been released and reidentified. In 2016, journalists reidentified politicians in an anonymized browsing history dataset of 3 million German citizens, uncovering their medical information and their sexual preferences. A few months before, the Australian Department of Health publicly released de-identified medical records for 10% of the population only for researchers to reidentify them 6 weeks later. Before that, studies had shown that de- identified hospital discharge data could be reidentified using basic demographic attributes and that diagnostic codes, year of birth, gender, and ethnicity could uniquely identify patients in genomic studies data. Finally, researchers were able to uniquely identify individuals in anonymized taxi trajectories in NYC27, bike sharing trips in London, subway data in Riga, and mobile phone and credit card datasets*".

observável e as características conhecidas dos indivíduos – atividade online, compras, curtidas, movimentos – a dados sensíveis em tese não observáveis sobre eles, como suas atitudes psicológicas, seu estado de saúde, sua orientação sexual ou seu comportamento, preferências políticas.

De qualquer modo, dado os elevados níveis de riscos envolvidos no tratamento de dados pessoais sensíveis, percebe-se com relativa clareza que as avaliações, decisões ou inferências relacionadas a esses casos teriam o condão de expor os indivíduos envolvidos à discriminação ou manipulação e que nessas circunstâncias eventual inexistência de mecanismos de contestação das *decisões automatizadas* potenciaria a perpetuação dos erros de julgamento e decisões injustas, situação não compatível com as garantias constitucionais no País[242].

4.4 QUESTÕES DE JUSTIÇA E DISCRIMINAÇÃO CONECTADAS COM AS ETAPAS DO PROCESSO DECISÓRIO

Na opinião de alguns autores — como Kahneman (2012) — os sistemas de IA podem evitar falácias típicas da psicologia humana (viés da confirmação, heurística da representatividade, excesso de confiança, entre outros) e segundo disseminadas avaliações os sistemas algorítmicos poderão ter desempenho superior aos dos especialistas humanos.

Nesse aspecto, observam SARTOR e LAGIOIA (2020)[243], há quem sustente a possibilidade de que decisões algorítmicas possam ser equivocadas ou discriminatórias, e, em casos raros, os algoritmos de fato se envolvam em discriminação ilegal explícita (o chamado tratamento díspar) ao basear seu resultado em preditores (características) proibidos, como raça, etnia, gênero, opção política etc.

Conforme já salientado, os sistemas baseados em aprendizado supervisionado podem ser treinados em julgamentos humanos anteriores e podem, portanto, reproduzir os pontos fortes

[242] Note-se que, embora este estudo (focado nas possibilidades dialógicas) não considere as possíveis soluções no âmbito judicial, não pode ignorar que a Constituição Federal de 1988 positivou, em seu art. 5º, inciso XXXV, o princípio da inafastabilidade do controle jurisdicional, ao determinar que a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito.
[243] SARTOR, LAGIOIA, 2020, p. 32.

e fracos dos humanos que fizeram esses julgamentos, incluindo suas propensões ao erro e ao preconceito.

Note-se que um sistema de recrutamento treinado nas decisões de contratação anteriores aprenderá a emular a avaliação dos gerentes sobre quais candidatos seriam adequados, por vezes sem basear suas previsões diretamente em preditores relacionados ao desempenho de um candidato no trabalho.

Na hipótese de as decisões passadas terem sido influenciadas pelo preconceito, o sistema reproduzirá essa lógica. O preconceito assim embutido nos conjuntos de treinamento haverá de persistir inclusive nos casos em que as entradas (os preditores) dos sistemas automatizados não incluírem características discriminatórias proibidas, como etnia ou gênero.

A probabilidade de tal ocorrência estará presente quando existir uma correlação entre características discriminatórias e alguns preditores considerados pelo sistema[244].

Um conjunto de dados de treinamento pode se revelar tendencioso contra um determinado grupo, quando o resultado previsto (v.g., desempenho no trabalho) realiza aproximações por meio de um *proxy* [245]que tem um impacto diferente nesse grupo.

É o caso da predição relacionada com o desempenho futuro dos funcionários (alvo de interesse na contratação), se medido apenas pelo número de horas trabalhadas no escritório (SARTOR e LAGIOIA, 2020).

Esse critério poderá resultar na avaliação baseada em contratação anterior de mulheres – que eventualmente trabalhem menos horas que os homens, por conta dos encargos familiares –, contratações essas que seriam consideradas menos bem-sucedida do que a contratação de homens[246].

---

[244] "*[W]ith appropriate requirements in place, the use of algorithms will make it possible to more easily examine and interrogate the entire decision process, thereby making it far easier to know whether discrimination has occurred. By forcing a new level of specificity, the use of algorithms also highlights, and makes transparent, central trade-offs among competing values. Algorithms are not only a threat to be regulated; with the right safeguards in place, they have the potential to be a positive force for equity*". (KLEINBERG; MULLAINATHAN; SUNSTEIN, 2018, pp. 113–174 *apud* SARTOR; LAGIOIA, 2020, p. 22).

[245] "Um *proxy* é um serviço que age como um intermediário entre o usuário e a internet, recebe e repassa todas as suas requisições ao *site* que você está acessando". (GOGONI, 2019); "Em redes de computadores, um ***proxy*** (em português 'procurador', 'representante') é um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores". (WIKIPEDIA, 2023).

[246] SARTOR; LAGIOIA, 2020, p. 32.

Essa correlação (medida com base na *proxy* tendenciosa) levará os sistemas a prever desempenho inferior das candidatas do sexo feminino (SARTOR e LAGIOIA, 2020)[247].

Haverá casos em que os erros e discriminações decorram de vieses do sistema de aprendizado de máquina embutidos nos preditores.

Um sistema poderá utilizar um preditor favorável (característica de entrada) que se aplique apenas a membros de um determinado grupo (v.g., ter frequentado uma instituição de ensino superior socialmente seletiva). Outro exemplo de injustiça, no âmbito da tomada de julgamentos humanos tendenciosos, pode se basear em preditores desleais (v.g., cartas de recomendação) [248].

Enfim, a injustiça também pode derivar do conjunto de dados relacionados com a composição estatística de uma população. É o caso dos pedidos de fiança ou liberdade condicional, no qual o histórico criminal anterior desempenha papel relevante implicando no tratamento diferenciado de membros de um determinado grupo à sujeição de controles mais rígidos, em razão da atividade criminosa a que esteja associado, detectado e punido com mais frequência (poderá assim ocorrer que os membros desse grupo recebam uma avaliação menos favorável do que os membros de outros grupos que se comportaram da mesma maneira)[249].

Na perspectiva de Cathy O'Neil (2016), é difícil contestar a injustiça da tomada de decisão automatizada na medida que o pedido poderá ser desconsiderado ou rejeitado por interferir na operação do sistema, gerando custos adicionais e incertezas.

Na opinião da autora referenciada, as previsões dos sistemas de aprendizado de máquina são baseadas em correlações estatísticas, contra as quais pode ser difícil argumentar com base em circunstâncias individuais, mesmo quando exceções possam ser justificadas.

Mendes, Mattiuzzo e Fujimoto (2021) [250] classificam quatro tipos principais de discriminação algorítmica. O primeiro tipo é a discriminação por erro estatístico, que decorre

---

[247] *Idem*.

[248] Conforme destaca Bayamlioğlu (2018), sistemas baseados em aprendizado de máquina possuem uma dependência particular em relação aos dados, na medida em que as suas próprias regras são construídas com base em um processo de treinamento a partir de dados previamente classificados.

[249] Um exemplo oferecido por Sartor e Lagioia (2020) ilustra o preconceito sofrido por membros de um determinado grupo em razão da sua baixa representatividade como subconjunto do conjunto de treinamento, o que implica a redução da precisão das previsões para esse grupo (seria o caso de uma empresa que nomeou poucas mulheres no passado e que usa seus registros de contratações anteriores como seu conjunto de treinamento).

[250] MENDES; MATIUZZO; FUJIMOTO *in* DONEDA *et al*., 2021, pp. 421-448. (Omitem-se as referências internas feitas pelas autoras).

de erros cometidos pelos engenheiros ou cientistas de dados responsáveis pelo desenvolvimento do algoritmo. O segundo tipo é a discriminação pelo uso de dados sensíveis, que se baseia em informações legalmente protegidas. O terceiro tipo é a discriminação por generalização injusta, em que pessoas são equivocadamente classificadas em certos grupos devido a correlações abusivas. O último tipo é a discriminação que limita o exercício de direitos, em que a relação entre a informação utilizada pelo algoritmo e a realização de um direito é afetada de forma desproporcional.

As autoras acima referenciadas ainda destacam as diversas hipóteses de caracterização da discriminação ilícita. Da Constituição Federal, salientam que o Artigo 3º, IV e Art. 5º, XLI, prevê expressamente a proteção de grupos vulneráveis ao dispor sobre os princípios da igualdade e da proibição de discriminação que atente contra os direitos e liberdades fundamentais. Com base na Lei 7.716/1989, alertam para as discriminações algorítmicas vedadas (portanto passíveis de punição), materializadas nas diversas condutas tipificadas na lei[251]. No âmbito da LGPD, para além dos cuidados da regulação no tocante ao tratamento de dados sensíveis (LGPD: art. 5º, II)[252], tem-se no Artigo 6º, IX duas classes de discriminação conectadas com a finalidade do tratamento — a ilícita e a abusiva — , a primeira objeto de expressas definições "*in abstrato*" nas mencionadas leis; a segunda, a abusiva, com dificuldades

[251] Tipificações na Lei nº 7.716, de 1989: i - impedir ou obstar o acesso de alguém, devidamente habilitado, a qualquer cargo da Administração Direta ou Indireta, bem como das concessionárias de serviços público (art. 3º); ii - negar ou obstar emprego em empresa privada (art. 4º); iii - recusar ou impedir acesso a estabelecimento comercial, negando-se a servir, atender ou receber cliente ou comprador (art. 5º) iv - recusar, negar ou impedir a inscrição ou ingresso de aluno em estabelecimento de ensino público ou privado de qualquer grau (art. 6º) impedir o acesso ou recusar hospedagem em hotel, pensão, estalagem, ou qualquer estabelecimento similar (art. 7º) v - impedir o acesso ou recusar atendimento em restaurantes, bares, confeitarias, ou locais semelhantes abertos ao público, estabelecimentos esportivos, casas de diversões, ou clubes sociais abertos ao público, salões de cabeleireiros, barbearias, termas ou casas de massagem ou estabelecimento com as mesmas finalidades (art. 8º; art. 9º; art. 10); vi - impedir o acesso às entradas sociais em edifícios públicos ou residenciais e elevadores ou escada de acesso a eles (art. 11); vii - impedir o acesso ou uso de transportes públicos, como aviões, navios barcas, barcos, ônibus, trens, metrô ou qualquer outro meio de transporte concedido (art. 12); ix - impedir ou obstar o acesso de alguém ao serviço em qualquer ramo das Forças Armadas (art. 13); x - impedir ou obstar, por qualquer meio ou forma, o casamento ou convivência familiar e social (art. 14).

[252] Advertem as autoras: "A LGPD caracteriza de forma diferenciada alguns dados pessoais, determinando serem dados pessoais sensíveis os 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). Não existe na lei qualquer tipo de vedação geral ao uso de tais dados sensíveis para atividades de automação ou perfilhamento, mas é natural que seu uso para tais finalidades apresente riscos majorados. Assim, é necessário ter cuidado para avaliar se o uso de determinado dado sensível é ilícito ou abusivo, pois a análise sob a perspectiva da abusividade é residual em relação ao enquadramento como discriminação ilícita. Aquilo que a lei determinar que deve ser protegido de forma categórica e expressa deve ser enquadrado como ilícito; por outro lado, os casos não considerados como tal comportam presunção relativa de ilicitude, devendo ser analisados sob o prisma da abusividade". (MENDES; MATIUZZO; FUJIMOTO *apud* DONEDA *et al.*, 2021, p. 438)

interpretativas, porém sujeita à constatação, verificação e avaliação em casos concretos, alguns evidentes, outros nem tanto.[253]

Enfim, com base nessas considerações, cumpre rememorar que no Brasil as linhas gerais da disciplina jurídica do uso de dados jurídicos estão de fato contempladas na LGPD e que o arcabouço legal é complementado por normas setoriais, como aquelas relativas ao direito do consumidor etc.

Nos termos da LGPD (artigo 5º, X), qualquer[254] operação de tratamento destes dados pessoais — incluídas aí operações de coleta, armazenamento ou modificação (artigo 5º, X) — sujeita-se aos requisitos legais, dentre os quais a necessidade de uma base legal que autorize o seu processamento (artigo 7º), e da garantia de que os titulares dos dados processados têm acesso aos direitos nele assegurados (em especial, aqueles delineados nos artigos 18 a 22)[255].

Ademais, como asseverado em tópicos anteriores, salientou-se o entendimento de AGRAWAL, 2018, *apud* REIS e FURTADO, 202[256], no tocante à abrangência do processo decisório, cuja etapa inicial poderá incluir momentos anteriores à própria coleta dos dados, notadamente porque, na fase de treinamento, o modelo poderá ser alimentado mediante inputs de dados dos grupos sociais aos quais o indivíduo vier a ser futuramente associado, embora à época do treinamento, totalmente dissociados dos dados pessoais, objetos da decisão automatizada.

Na mesma linha, asseveram REIS e FURTADO (2022)[257] que os dados pessoais poderão integrar tanto os "dados de entrada" quanto os "dados de saída", estes últimos correspondentes ao "julgamento" (ou decisão automatizada propriamente dita). Isso implica dizer que na medida em que os dados correspondam a determinada pessoa natural eles

[253] Em qualquer caso, há que se verificar se as discriminações (sob qualquer forma vedada na LGPD) se enquadrariam numa das previsões do Código Civil (art. 186; art. 187 e art. 927), restando refletir sobre a ilicitude da alegação de confidencialidade de algoritmos discriminatórios ao manto do segredo dos negócios, passível de descortino por meio de auditoria, a cargo da autoridade nacional de proteção, nos termos do art. 20, § 2º, da LGPD, no contexto de recusa às informações relacionadas com os critérios e os procedimentos utilizados na decisão automatizada, incluída a de perfilização.

[254] O art. 4º da LGPD exclui do escopo da lei algumas categorias de tratamento de dados pessoais, como as operações ligadas a questões de segurança pública (art. 4º, III, "a"). Essas exclusões continuam enquadradas na definição de dados pessoais da LGPD e podem ser reguladas por lei posterior.

[255] MENDES, 2014.

[256] AGRAWAL; GANS; GOLDFARB, 2018, p. 74 *apud* REIS; FURTADO, 2022.

[257] Op. Cit. REIS, N. C. M.; FURTADO , G. R. Decisões automatizadas: definição, benefícios e riscos. civilistica.com, v. 11, n. 2, p. 1-44, 7 out. 2022. https://civilistica.emnuvens.com.br/redc/article/view/763, acesso em 31.01.2023

passariam a integrar o conceito de “dados pessoais” para os efeitos do direito de explicação e revisão estabelecidos na regulação protetiva (LGPD: Art. 20).

Enfim, é importante destacar que a LGPD se aplica às operações de tratamento de dados pessoais, incluindo a coleta, armazenamento e modificação, e também abrange o processo decisório automatizado. Além disso, os dados pessoais podem estar presentes tanto nos dados de entrada quanto nos dados de saída dos modelos de decisão automatizada, sujeitando-se aos direitos de explicação e revisão estabelecidos na LGPD.

Diante dessas considerações, é necessário abordar a questão da definição de perfis, que é compreendida como um aspecto especial da transparência e explicabilidade da decisão automatizada.

4.5 PERFIL, INFLUÊNCIA E MANIPULAÇÃO EM SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

A perfilização e as decisões automatizadas estão intimamente relacionadas, pois são partes integrantes do processo de tomada de decisão. A perfilização ocorre nas etapas iniciais do processo, podendo estar presente durante a fase de treinamento, enquanto as decisões automatizadas são o resultado pretendido no modelo. Ambas estão sujeitas à disciplina do Artigo 20 da LGPD (Lei Geral de Proteção de Dados), uma vez que envolvem o uso de dados pessoais, que incluem a definição de perfis pessoais, profissionais, de consumo, de crédito e aspectos da personalidade do titular[258].

Em tópico anterior, foram abordadas as etapas do processo decisório automatizado e a potencial imbricação dos dados pessoais na fase de treinamento de um modelo de IA usado nessa automação da decisão. É intuitivo que um modelo de IA dedicado à produção de uma decisão automatizada relacionada a um indivíduo ou grupo realizará avaliações iniciais, conhecidas como etapas de treinamento. Essas avaliações são baseadas em preditores obtidos a partir da análise de dados relacionados a pessoas naturais, com o objetivo de fazer previsões

[258] LGPD: “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.”

relacionadas a indivíduos específicos, que serão usadas para tomar decisões que podem afetar seus interesses e direitos.

Segundo Ajay Agrawal, Josua Gans e Avi Goldfarb[259] (citados por Reis e Furtado, 2022), a avaliação durante a perfilização pode ser baseada em critérios pré-definidos ou em critérios de decisão estabelecidos pelo próprio sistema. Além disso, os modelos conceituais que sustentam a avaliação podem ser influenciados por uma série de valores cognitivos e não-cognitivos. Mireille Hildebrandt (citada por Zanatta) também diferencia entre "perfilização orgânica", feita por seres vivos para monitorar e reconhecer padrões, "perfilização humana", que é a capacidade humana de construir estereótipos como pré-condição para a ação, e "perfilização automatizada", realizada por máquinas pré-programadas para identificar correlações inesperadas em grandes bancos de dados agregados[260].

É de fato levado em conta que a automação diminui os custos de coleta de informação sobre os indivíduos, armazenando-as e processando-as com o intuito de avaliar indivíduos e orientar decisões relacionadas a escolhas.

Sob outro prisma, a automação possibilita a utilização persistente de mecanismos abrangentes de avaliação e controle. Daí, em geral, tem-se que o problema decorrente do uso de sistemas automatizados de avaliação (predição, rotulagem, codificação etc.,) pode-se agravar, seja quando seu desempenho é pior, seja quando se afigure melhor do que os realizados diretamente por humanos.

Com apoio na IA, qualquer tipo de dados pessoais pode ser usado para analisar, prever e influenciar comportamento humano, e nisto reside o valor dos dados pessoais, transformados em "mercadoria" no âmbito desse processo[261].

---

[259] AGRAWAL; GANS; GOLDFARB, 2018, p. 74 *apud* REIS; FURTADO, 2022.

[260] Ao definir a perfilização automatizada como "um processo de descoberta de conhecimento em bases de dados", Hildebrandt salienta que a mineração de dados (*data mining*) é parte integrante desse processo. (HILDEBRANDT, 2008, p. 58 *apud* ZANATTA, 2019). **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. 10.13140/RG.2.2.33647.28328. disponível em https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais, acesso em 14.02.2023.

[261] Nesse aspecto, segundo ilustra Sartor e Lagioia (2020), até as informações que não foram coletadas ou foram descartadas como "exaustão de dados" sem valor – a exemplo das trilhas de atividades online – "agora se tornaram um recurso valioso". (SARTOR; LAGIOIA, 2020) The Impact of the General Data Protection (GDPR) on artificial intelligence. Página . https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)641530, acesso em 19.01.2023.

Por meio de tecnologias de IA e *big data*, aliadas a um conjunto de sensores onipresentes no dia a dia é possível rastrear qualquer atividade humana, sendo intuitivo que nesse cenário (e em muitos casos e contextos) os indivíduos estão expostos a vigilância e influência, a partir dos dados e informações disponíveis, presumivelmente reveladoras de suas características pessoais, que vão desde condições de saúde, local de residência, escolhas e eventos da vida pessoal, comportamento *online* e *offline,* dentre outros.

Ao correlacionar dados sobre os indivíduos com as rotulagens, codificações, classificações ou previsões correspondentes, a IA potencializa a criação de perfis. Implica dizer, abre-se o caminho para a inferência sobre informações relacionadas aos indivíduos ou grupos e para a adoção de avaliações e decisões a partir desses perfilamentos.

A partir dessas considerações, surge a indagação: qual o conceito de perfilização?

Do dicionário de língua inglesa, tem-se o termo *profiling* para significar "o ato ou processo de extrapolar informação sobre uma pessoa baseado em traços ou tendências conhecidas"[262].

Da etimologia italiana, tem-se o termo 'perfil' derivado do italiano 'profilo', de "profilare", originalmente significando traçar uma linha, especialmente o contorno de um objeto. [263] .

No entendimento de Sartor e Lagioia, perfilização(2020, p.22),[264] é o processo de expandir os dados disponíveis sobre indivíduos ou grupos, a fim de descrever ou antecipar seus traços e propensões. Bosco et al. (2015), citados pelos autores, definem perfilização como uma técnica parcialmente automatizada de tratamento de dados pessoais e/ou não pessoais que visa produzir conhecimento por meio da inferência de correlações, criando perfis que podem ser aplicados como base para a tomada de decisões[265].

---

[262] *Idem*.
[263] *Idem*.
[264] "*The term 'profile' derives from the Italian 'profilo', from 'profilare', originally meaning to draw a line, especially the contour of an object: that is precisely the idea behind profiling through data processing, which means to expand the available data of individuals of groups, so as to sketch describe or anticipate their traits and propensities*". (SARTOR; LAGIOIA, 2020) The Impact of the General Data Protection (GDPR) on artificial intelligence. Página . https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)641530, acesso em 19.01.2023, p. 22)
[265] "*Profiling is a technique of (partly) automated processing of personal and/or non- personal data, aimed at producing knowledge by inferring correlations from data in the form of profiles that can subsequently be applied as a basis for decision-making. A profile is a set of correlated data that represents a (individual or collective)*

Por outro lado, Reis e Furtado (2022) [266] estabelecem a distinção entre decisão e predição, sendo a perfilização entendida como uma decisão automatizada se for parte integrante do objetivo ou do resultado pretendido. A predição decorre de inferências estatísticas, enquanto a decisão implica tomar uma posição diante dos dados, não sendo apenas uma inferência estatística. A explicação fica mais clara nas palavras dos próprios Autores, de quem se transcreve o seguinte:

> (...) a perfilização está mais associada à predição e somente pode ser considerada a decisão automatizada se ela mesma for o objetivo do modelo ou algoritmo. Caso se queira, por exemplo, avaliar a capacidade de pagamento de alguém para efeito de concessão de um empréstimo, a perfilização será parte do tratamento de dados e da predição, mas a decisão não estará nisso, e sim na concessão ou não do empréstimo. A decisão é sempre uma tomada de posição diante dos dados, e não apenas uma inferência estatística. A predição, que decorre das inferências estatísticas, apontará o provável resultado da operação de empréstimo (digamos, há 80% de chance de o indivíduo pagar o empréstimo dentro do prazo); já a decisão estará em definir o titular dos dados como apto ou não para o empréstimo. Por exemplo, certa instituição financeira pode decidir pelo sim, com 80% de chance de pagamento, mas outra pode exigir um limiar de predição maior (digamos, 90%) para contratar o empréstimo. Portanto, a predição não é ainda a decisão; ela é o prenúncio do que provavelmente ocorrerá, caso a decisão seja tomada em um ou outro sentido, à luz dos dados tratados pelo modelo. A preferência por acolher essa probabilidade como um 'sim' ou um 'não' é que a decisão.

Ainda em relação à perfilização, considera-se oportuna a interessante observação de ZANATTA (2019)[267] no sentido de vislumbrar distinção entre o modelo regulatório adotado na União Europeia (RGPD) e a brasileira (LGPD); o primeiro, no sentido de adotar a regra da "proibição geral", contrária à da segunda de aparente autorização ampla.

Segue-se, portanto, ao exame para aferir se esses diferentes ordenamentos efetivamente almejaram propiciar graus semelhantes de proteção.

A legislação brasileira (LGPD) menciona a existência de vários tipos de perfis, como pessoais, profissionais, de consumo, de crédito e aspectos da personalidade. No entanto, isso não implica a existência de múltiplos conceitos relacionados à perfilização. A finalidade da lei está voltada para o uso e a repercussão dos dados pessoais na vida dos indivíduos aos quais eles

---

subject. Constructing profiles is the process of discovering unknown patterns between data in large data sets that can be used to create profiles. Applying profiles is the process of identifying and representing a specific individual or group as fitting a profile and of taking some form of decision based on this identification and representation". (BOSCO *et al.*, 2015, pp. 3-33 *apud* SARTOR; LAGIOIA, 2020)

[266] REIS; FURTADO, 2022.

[267] ZANATTA, 2019.

se referem. Mesmo os dados anonimizados serão considerados dados pessoais se forem usados na criação de perfis comportamentais, conforme estabelecido no Artigo 12, §2º da LGPD.

Nessa direção, a explicação adicional de Bruno BIONI (2019) [268]:

> Muitas vezes, processos de decisões automatizadas valem-se desses perfis que não necessariamente identificam uma pessoa em específico, mas um grupo – *grouping*. É pelo fato de ela estar catalogada, inserida, referenciada ou estratificada nesse grupo que uma série de decisões serão tomadas a seu respeito, ainda que sem significalizá-la diretamente. (...) As expressões "determinada pessoa" ou "identificada" (...) devem ser compreendidas com relação aos desdobramentos que o tratamento de dados pode ter sobre um indivíduo, ao contrário de significá-los com os olhos voltados para a base de dados em si, especificamente se o perfil comportamental pode ser ou não atribuído a uma pessoa em específico.

Com enfoque distinto, para a regulação da União Europeia, a noção de profiling (perfilização) não considera a construção de perfis de grupo, abrangendo apenas avaliações e decisões relacionadas a indivíduos, com base em dados pessoais. Por vias distintas, buscam-se idênticos níveis de proteção.

Com efeito, observe-se que enquanto na LGPD (Artigo 20) se menciona os diversos perfis (com sinalização em atrelamento ao grupamento populacional), a RGPD cuidou de estabelecer normativamente a definição de perfil (Art. 4º, nº4), prevendo ampla cobertura em relação a ela (Art. 22, nº1).

De fato, o Regulamento Europeu para a Proteção de Dados (GDPR: art. 4º, nº 4) associa (na tradução portuguesa) a "definição de perfil" como algo distinto de decisão automatizada (ao contrário, a LGPD permite leitura contrária); contudo, ao considerar a ampla proteção conferida no artigo 22, tal distinção não se confirma, em outros pontos.

Com efeito, o art. 4º, n. 4 do GDPR associa a perfilização com a análise e a predição, o que, no entendimento de REIS e FURTADO (2022), a distingue da decisão[269], sendo esta posterior àquela. Vale conferir o texto normativo.

> GDPR, art. 4º, nº 4: «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 econômica,

[268] BIONI, 2019, p. 80 *apud* ZANATTA, 2019.

[269] "O Regulamento Europeu para a Proteção de Dados (GDPR) define a perfilização (ou 'definição de perfil', na tradução portuguesa) como algo diferente da decisão automatizada, embora não seja totalmente fiel a essa distinção em outros pontos. Com efeito, o art. 4º, n. 4 do GDPR associa a perfilização com a análise e a predição, que são anteriores à decisão(...)" (REIS; FURTADO, 2022)

> saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

Verifica-se que, ao disciplinar a decisão automatizada, o art. 22, n. 1 do GDPR, não se limita à hipótese da definição de perfis, estabelecendo ampla proteção ao titular de dados contra decisões que produzam efeitos na sua esfera jurídica ou que similarmente o afete significativamente[270]. Confira-se:

> GDPR: Art. 22º (1º) - O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

De qualquer modo, acredita-se que a ideia a ser relevantemente fixada, neste particular, consiste em compreender que a perfilização é um passo integrante do processo decisório que, na hipótese discutida (LGPD: artigo 20), culmina na decisão automatizada; e, embora com esta não se confunda, é objeto de igual nível de proteção no âmbito da legislação brasileira (i.e., passível de revisão, senão no âmbito do próprio direito de explicação, implícito no §1º do referido artigo 20[271], com fundamento nos demais direitos informacionais como aqueles básicos estabelecidos no artigo 18)[272].

---

[270] Nesse particular, com atenção voltada ao Ordenamento, raciocina-se que – implícito no art. 20 da LGPD – há certa imbricação entre o ato de perfilar com a decisão automatizada, se os preditores do perfilamento, na hipótese, forem adotados no modelo decisório. Ademais, embora a perfilização seja em tese orientada pelos preditores inferidos a partir de dados (de treinamento) coletados de um grupo social específico, a adoção desses critérios de perfilização poderá ter implicações jurídicas notadamente se, no âmbito da decisão automatizada, os respectivos preditores orientarem a avaliação/decisão relacionada ao indivíduo, a quem se refere o processo decisório e nele identificado. Em casos tais, senão do próprio art. 20, a revisão poderá em princípio decorrer do direito de não ser indevidamente discriminado (espraiado no sistema jurídico brasileiro) e dos direitos básicos assegurados no art. 18 da LGPD: "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; (...) VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; (...)". Ademais, como já salientado, casos haverá em que os erros e as discriminações têm origem em vieses do sistema de aprendizado de máquina embutidos nos preditores; erros e discriminações esses não triviais e com impactos nos interesses e direitos de qualquer indivíduo; como forma de se atender às expectativas sociais de não discriminação positivadas aqui e ali ao longo do Ordenamento, surge o direito de revisão cujo procedimento (§ 1º ou § 2º do art. 20) viabiliza a explicitação dos critérios adotados num modelo preditor, eventualmente favorável (característica de entrada) a membros de um determinado grupo (*v.g.*, ter frequentado uma instituição de ensino superior socialmente seletiva), sem justificativas razoavelmente respaldadas nos critérios de justiça e equidade.

[271] LGPD: "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." (g.n.)

[272] V. nota anterior.

Mais do que conferir segurança jurídica aos setores da economia e para o tratamento de dados pelo Estado, a disciplina da proteção dos dados tornou-se fundamental para a manutenção da confiança nas estruturas de comunicação e informação desta Era Digital. A relevância do tema foi já ressaltada no STF por ocasião do julgamento da ADI 6387, cuja relatoria faz menção ao caso Cambridge Analytica, que "revelou como modelos de negócios são rentabilizados pela análise de dados e como alertou ao seu uso indevido (...)" [273]

A referência ao caso ilustra a percepção para os perigos envolvidos na criação de perfis, amplamente divulgado pela imprensa. Trata-se das tentativas de influenciar o comportamento eleitoral – nas eleições de 2016 nos Estados Unidos e possivelmente também no referendo do Brexit – com base no processamento massivo de dados pessoais (BAYER et al, 2019, *apud* SARTOR, LAGIOIA 2020, p. 29). Eis o relato.

Cerca de 320 mil eleitores registrados nos EUA teriam aceitado o convite para a realização de um teste de personalidade e político, respondendo a 120 perguntas disponibilizadas *online*, mediante recompensa de pequena quantia (dois a cinco dólares americanos) e sob a informação de que se tratava de pesquisa acadêmica.

O recebimento da recompensa estaria condicionado à autorização de acesso à sua página no Facebook, o que viabilizara, ao sistema, a conexão das respostas de cada indivíduo às informações incluídas em sua página no Facebook.

A partir do acesso à página de determinado candidato, a Cambridge Analytica coletou não apenas a página do Facebook dos examinandos, como também as páginas do Facebook de seus amigos, o que totalizou entre 30 e 50 milhões de pessoas. Os dados do Facebook também foram coletados de outras fontes (BAYER et al, 2019, *apud* SARTOR, LAGIOIA 2020, p. 29).

Após coletado esses dados, a Cambridge Analytica passou a tratar dois conjuntos de dados pessoais: ***(i***) os dados relacionados aos examinandos, consistentes na informação incluída em suas páginas de Facebook; (***ii***) as respectivas respostas ao questionário, os dados sobre seus amigos, com base nas informações em suas páginas do Facebook. Esses dados - sobre os participantes do teste – serviram como um conjunto de treinamento[274] e foram utilizados como

[273] ADI nº 6.387/DF, de relatoria da Ministra Rosa Weber, Plenário, julgada em 6 e 7 de maio de 2020.
[274] Informações usuais das páginas do *Facebook* de um indivíduo como curtidas, postagens, *links* etc., bem como as atitudes políticas, expressas nas respostas ao questionário.

valores alvos, ou preditores na construção de um modelo para traçar o perfil de seus amigos e demais contatos.

Os dados foram utilizados nos algoritmos de *machine learning* da Cambridge Analytica na construção do modelo correlacionando informações pessoais das respectivas páginas no Facebook com previsões sobre os traços psicológicos e as preferências políticas (ibid. op. cit. idem).

A partir desse modelo, a Cambridge Analytica aplicou os dados disponíveis na elaboração massiva de perfis, incluindo pessoas que não fizeram o teste, tudo com base em seus dados do Facebook e outros disponíveis, cruzando-os com as previsões fornecidas pelo modelo.

Assim, por exemplo, a predição relacionada a um participante do teste com um certo padrão de curtidas e postagens no Facebook que ensejasse sua classificação como detentor de personalidade neurótica, permitia que a mesma avaliação fosse estendida a um não participante do teste, cujo padrão se assemelhasse com seus dados do Facebook.

Numa etapa final, a partir do perfil de personalidade e político, foram identificados os eleitores mais sensíveis, ajustando-se a mensagem mais adequada à mudança de comportamento eleitoral, fator esse que, em determinados estados dos EUA, teria efeito devastador no resultado da eleição, disputada entre um e outro partido com pouca diferença de votos.

Portanto, esses eleitores foram alvos de anúncios políticos personalizados, acompanhados de outras mensagens destinadas a provocar a mudança de comportamento eleitoral tal como desejado (neste caso, explorou-se as emoções e preconceitos neles percebidos de sorte a minimizar a percepção quanto ao propósito das respectivas mensagens[275]).

A proteção dos dados pessoais é essencial para manter a confiança nas estruturas de comunicação e informação da Era Digital. O caso Cambridge Analytica é um exemplo que ilustra os perigos envolvidos na criação de perfis e na influência do comportamento eleitoral com base no processamento massivo de dados pessoais.

Em resumo, são inúmeras as questões implicadas com o tratamento de dados pessoais. Não interessa apenas aos indivíduos afetados compreender e identificar quais os procedimentos

[275] BAYER *et al.*, 2019 *apud* SARTOR; LAGIOIA, *op. cit.*, p. 29.

e quais resultados foram a partir dele alcançados. Interessa a todos que tenham corresponsabilidade democrática (HOFFMANN-RIEM, 2021, p. 87) que os sistemas de tratamento de dados sejam compreensíveis e controláveis. Nesse contexto e sob tal aspecto que nos tópicos seguintes se passa a analisar questões relevantemente relacionadas com a transparência e explicabilidade no âmbito da perfilização e das tomadas de decisões automatizadas.

CAPÍTULO 5 - TRANSPARÊNCIA E EXPLICABILIDADE DAS DECISÕES AUTOMATIZADAS

A transparência[276], assim como a privacidade, é fator com os quais todos haverão de conviver para sobreviver. Em defesa da transparência, sugiram os ideais de uma "sociedade transparente". No entanto, em relação à privacidade, é amplamente reconhecido que o seu significado mudou no contexto dos novos valores e interesses presentes na sociedade da informação (DONEDA, 2021).

Conforme apontado por Stefano Rodotà (1995), o paradigma "pessoa-informação-segredo" mudou para o paradigma "pessoa-informação-circulação-controle". No entanto, é importante ponderar a opinião de Karl Popper, que argumenta que qualquer inconveniência causada pela ciência é (ou pode ser) amplamente superada pelas vantagens[277].

Esses e outros aspectos são mencionados ao longo deste trabalho de forma dispersa. Portanto, além do debate filosófico, é importante apresentar o contexto do debate em torno da transparência, especialmente quando se trata da opacidade dos sistemas de IA. Compreender essas noções é fundamental para a análise jurídica da regulamentação focada na proteção dos direitos e interesses individuais, considerando também segredos comerciais, reconhecidamente importantes para incentivar a inovação e proteger informações confidenciais.

---

[276] Nesta seção, serão recorrentemente adotados conceitos em relação aos quais se fazem necessários esclarecimentos: no contexto do direito de explicação dos sistemas de IA nas decisões automatizadas, clareza, transparência e explicabilidade são conceitos diferentes, mas complementares. A clareza refere-se à qualidade da informação que é apresentada sobre o processo de tomada de decisão do sistema de IA. Em outras palavras, a clareza se refere à facilidade de compreensão do processo de tomada de decisão e das informações relevantes sobre o sistema. A transparência, por sua vez, refere-se à disponibilidade das informações relevantes para os interessados. Isso inclui a disponibilidade de informações sobre como o sistema foi construído, como ele opera e como toma decisões. A transparência permite que os interessados compreendam o funcionamento do sistema e possam verificar se o sistema está agindo de forma justa e não discriminatória. Finalmente, a explicabilidade se refere à capacidade do sistema de IA explicar as decisões que toma. Isso inclui a capacidade do sistema de IA de fornecer informações detalhadas sobre como chegou à determinada decisão, como as informações foram ponderadas e como foram levadas em conta as possíveis consequências das decisões. Portanto, a clareza, a transparência e a explicabilidade são conceitos diferentes, mas complementares, que devem ser considerados ao se avaliar o direito de explicação dos sistemas de IA nas decisões automatizadas. A clareza e a transparência permitem que os interessados entendam o funcionamento do sistema, enquanto a explicabilidade permite que o sistema forneça informações detalhadas sobre as decisões que toma.

[277] "Sob um determinado ponto de vista, a transparência é um fator ao qual adaptar-se é uma verdadeira questão de sobrevivência, e as alternativas de controle diante das novas características do fluxo informacionais poderiam parecer atos dignos de um *luddite* – os velhos ativistas receosos e contrários à tecnologia. Não se contam em poucos os entusiastas de um porvir no qual a transparência seja regra, que se destacam pelo pragmatismo de seu juízo segundo o qual efetivamente as vantagens de uma 'sociedade transparente' ultrapassariam suas inconveniências." (DONEDA *et al*, 2021, p. 342)

Além disso, a literatura aponta que a transparência por si só não garante a compreensão adequada dos resultados dos sistemas de IA. Segundo Talia Gillis (2022, apud Frazão et al, 2022), não é factível estabelecer uma relação de causa e efeito entre os inputs e outputs das decisões algorítmicas, dada a variedade de abordagens no aprendizado de máquina.

De acordo com as lições de Guidotti et al (2018), conforme citado por Sartor e Lagioia (2020) [278], existem várias abordagens complexas para fornecer explicações sobre o comportamento das redes neurais e outros sistemas opacos, conhecidos como "caixas pretas". Em algumas dessas abordagens, a explicação envolve observar os resultados das diferentes camadas da rede.

Nesse contexto, a literatura sugere a busca por um equilíbrio entre o desempenho e a explicabilidade, especialmente em domínios nos quais estão em jogo interesses humanos significativos. A explicação desempenha um papel fundamental nesses casos.

Sartor e Lagioia (2020) afirmam que, mesmo quando um sistema é considerado uma "caixa preta", ainda é possível realizar análises críticas do seu comportamento por meio da análise de sensibilidade. Por exemplo, ao verificar se a previsão de um sistema destinado a avaliar a capacidade de crédito muda quando modificamos o local de nascimento ou residência do requerente, podemos determinar se essa característica de entrada é relevante para a saída do sistema. Isso permite questionar se o sistema está discriminando indevidamente pessoas com base em sua etnia ou condição social, que podem estar relacionadas ao local de nascimento ou residência[279].

Guidotti et al (2018) [280] também destacam que pesquisas atuais sobre IA estão focadas no desenvolvimento de modelos compreensíveis para sistemas opacos, como redes neurais profundas, que sejam amigáveis aos especialistas humanos[281].

---

[278] GUIDOTTI *et al.*, 2018, pp. 1–4 *apud* SARTOR; LAGIOIA, 2020, p. 64.

[279] Em tradução livre: "(...) se a previsão de um sistema destinado a avaliar a qualidade de crédito muda se modificarmos o local de nascimento ou residência do solicitante, podemos determinar se esse recurso de entrada é relevante para a saída do sistema. Consequentemente, podemos nos perguntar se o sistema discriminou indevidamente as pessoas em função de sua etnia ou *status* social, que pode estar ligado ao local de nascimento ou residência." (SARTOR; LAGIOIA, 2020, p. 27)

[280] GUIDOTTI *et al.*, 2018, pp. 1–4. *apud* SARTOR; LAGIOIA, 2020, p. 64.

[281] Em tradução livre*:* "*Explicação do modelo*, ou seja, a explicação global de um sistema de IA opaco por meio de um modelo interpretável e transparente que captura totalmente a lógica do sistema opaco. Isso seria obtido, por

Isso envolve a explicação do modelo de forma global, através de um modelo interpretável e transparente que capture completamente a lógica do sistema opaco. Além disso, a inspeção do modelo permite entender algumas propriedades específicas ou predições do sistema opaco. Já a explicação do resultado refere-se à explicação de uma decisão específica em um exemplo particular.

Para os cientistas sociais (Miller e Wachter, 2017, apud Sartor e Lagioia, 2020) [282], não basta fornecer compreensibilidade apenas para especialistas, é necessário tornar as explicações acessíveis para os leigos. Para isso, eles propõem abordagens como explicação contrastiva, explicação seletiva, explicação causal e explicação social, que adotam uma abordagem interativa e conversacional[283].

Sartor e Lagioia (2020, p. 55) sugerem que as explicações fornecidas antes da inserção dos usuários nos algoritmos devem contemplar informações como os dados de entrada considerados pelo sistema, os valores-alvo que o sistema deve calcular e as consequências previstas da avaliação/decisão automatizada. Além disso, eles destacam a importância de especificar os propósitos gerais do sistema. No entanto, atualmente, é incomum encontrar aplicativos de IA que forneçam informações tão abrangentes, especialmente em relação à

---

exemplo, se fosse fornecida uma árvore de decisão ou um conjunto de regras, cuja ativação reproduzisse exatamente (ou quase exatamente) o funcionamento de uma rede neural;
Inspeção do modelo, ou seja, uma representação que possibilita a compreensão de algumas propriedades específicas de um modelo opaco ou de suas previsões. Pode dizer respeito aos padrões de ativação nas redes neurais do sistema, ou a sensibilidade do sistema a mudanças em seu input fatores (por exemplo, como uma mudança na renda ou idade do solicitante faz diferença na concessão de um pedido de empréstimo);
Explicação do resultado, ou seja, um relato do resultado de uma IA opaca em uma instância específica. Por exemplo, uma decisão especial relativa a um indivíduo pode ser explicada listando as escolhas que levam a essa conclusão em uma árvore de decisão (por exemplo, o empréstimo foi negado porque a renda do solicitante caiu abaixo de um certo limite, sua idade acima de um certo limite, e ele não tinha participação suficiente em nenhum imóvel disponível como garantia).” (GUIDOTTI *et al.*, 2018 *apud* SARTOR; LAGIOIA, 2020, p. 64)

[282] WACHTER; MITTELSTADT, 2017 *apud* SARTOR; LAGIOIA 2020.

[283] “(…) *the adoption of a certain decision (e.g., refusing a loan) rather than possible alternatives (granting the loan).Selective explanation: focusing on those factors that are most relevant according to human judgement.Causal explanation: focusing on causes, rather than on merely statistical correlations (e.g., a refusal of a loan can be causally explained by the financial situation of the applicant, not by the kind of Facebook activity that is common for unreliable borrowers).Social explanation: adopting an interactive and conversational approach in which information is tailored according to the recipient's beliefs and comprehension capacities Contrastive explanation: specifying what input values made a difference, determining* Em tradução livre: “*Explicação contrastiva*: especificando quais valores de entrada fizeram diferença, determinando a adoção de uma determinada decisão (por exemplo, recusar um empréstimo) ao invés de alternativas possíveis (conceder o empréstimo); *Explicação seletiva*: focando nos fatores que são mais relevantes de acordo com o julgamento humano;*Explicação causal*: foco nas causas, em vez de correlações meramente estatísticas (por exemplo, uma recusa de um empréstimo pode ser explicada causalmente pela situação financeira do solicitante, não pelo tipo de atividade do *Facebook* que é comum para mutuários não confiáveis); *Explicação social*: adotando uma abordagem interativa e conversacional em que a informação é adaptada de acordo com as crenças e capacidades de compreensão do destinatário.” (WACHTER; MITTELSTADT, 2017 *apud* SARTOR; LAGIOIA, 2020, p. 64.)

criação de perfis, que muitas vezes não fornecem informações precisas e relevantes aos usuários.

Sartor e Lagioia (2020) ainda argumentam que o acesso ao modelo algorítmico ou a possibilidade de submetê-lo a testes extensivos seria importante para permitir aos cidadãos uma espécie de "engenharia reversa" que possibilitaria a detecção de falhas e vieses. Essa abordagem democratizaria os controles, superando a complexidade dos aplicativos de IA e as restrições de acesso.

No entanto, mesmo com essas abordagens, é improvável que as informações fornecidas ao público em geral sejam suficientes para identificar problemas, disfunções e injustiças. Portanto, é encorajador saber que cientistas da computação estão envolvidos na pesquisa transdisciplinar da equidade algorítmica, buscando desenvolver técnicas e critérios para avaliar criticamente algoritmos e dados utilizados em softwares, com o objetivo de propor soluções que minimizem os riscos de discriminação algorítmica em várias aplicações dessa tecnologia[284].

5.1 PROTEÇÃO JURÍDICA E DECISÕES AUTOMATIZADAS POR SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Ao longo dos tópicos anteriores procurou-se identificar conceitualmente o processo decisório de um sistema de IA, exame esse que visou a mínima compreensão do funcionamento do “algoritmo de aprendizagem”, que agora sabemos serem basicamente decorrente de aplicação de técnicas de associações e correlações de informações a partir de padrões estatísticos presentes em grandes conjuntos de dados, sem prejuízo da possível incorporação de regras codificadas, tradutoras da visão de mundo do respectivo programador/desenvolvedor.

Analisou-se também os impactos e implicações das decisões automatizadas na vida de um indivíduo cujos dados pessoais tenham sido tratados. Isso inclui a criação de perfis com base em associações e correlações, que podem levar a suposições sobre a pertinência desse

[284] A revisão de literatura, nesse aspecto, é oferecida por Ricardo Silveira Ribeiro(2022) em trabalho no qual menciona o seguinte referencial de pesquisa: BAROCAS; HARDT; NARAYANAN, 2019; UOLAMWINI; GEBRU, 2018; CATON; HAAS, 2020; CORBETT-DAVIES *et al*, 2017; VERMA; RUBIN, 2018. (RIBEIRO, 2022)

indivíduo a determinado grupo. Essas decisões automatizadas têm o potencial de afetar a vida, os direitos e os interesses dos titulares de dados pessoais[285].

Apesar de termos adquirido noções preliminares sobre o fenômeno da IA, é importante considerar a perspectiva normativa. Sousa, Perone e Magrani (2021) argumentam que, assim como o GDPR, a LGPD se baseia em um sistema robusto de proteção dos direitos individuais. Isso se manifesta através dos princípios do acesso à informação, transparência, prevenção de danos, não discriminação, responsabilização e prestação de contas. Esses autores acreditam que esse conjunto de princípios garante ao titular de dados o controle sobre quais dados são processados, de que forma e para quais finalidades. Os agentes de tratamento de dados têm a obrigação de fornecer informações, ser transparentes, tomar precauções e serem responsáveis.

Portanto, concorda-se com esses autores e, neste trabalho, passamos a examinar o debate em torno da interpretação da base legal do direito de revisão e explicação no contexto das decisões automatizadas (Artigo 20 da LGPD). Isso inclui a análise dos outros direitos relacionados, como o direito de acesso e o direito de oposição, que, em princípio, se aplicam a qualquer tratamento de dados, independentemente de ser automatizado ou não.

5.2 DIREITOS DOS TITULARES NO TRATAMENTO DE DADOS AUTOMATIZADOS

De acordo com Danilo Doneda (2021), os estudos de Stefano Rodotà indicam uma mudança recente no conceito de privacidade. Anteriormente centrado no direito de "estar só",

[285] Em relação à construção de perfis (profissionais e comportamentais) por meio de sistemas de IA ou modelo de aprendizagem de máquina fixa-se aqui a ideia de que o uso de tais tecnologias pode ocasionar implicações significativas na vida de um indivíduo e na sociedade como um todo. Intui-se que em termos individuais, esses perfis podem ser usados por empresas para tomar decisões de contratação, promoção e demissão, bem como para personalizar a publicidade e oferecer produtos e serviços. Isso pode ter um impacto direto na vida financeira e profissional do indivíduo, podendo influenciar suas oportunidades de emprego e até mesmo seus salários. Além disso, oportuno mencionar, esses perfis também podem ser usados para fins de segurança, como em verificações de antecedentes criminais, que podem ter impacto na reputação de uma pessoa. A construção desses perfis considera padrões estatísticos daí gerando preditores sobre comportamento e personalidade. Do ponto de vista coletivo, a construção de perfis pode levar a um aumento da discriminação e desigualdade. Se os algoritmos de aprendizado de máquina forem treinados com dados enviesados, eles podem replicar e até mesmo amplificar e eternizar esses preconceitos. Além disso, esses perfis podem ser usados para segmentar e excluir grupos específicos da sociedade, aumentando a exclusão social e a polarização. O debate em curso aponta que a construção de perfis profissionais e comportamentais por meio de sistemas de IA ou modelo de aprendizagem de máquina deve ser regulamentada e transparente para garantir a proteção dos direitos e interesses dos indivíduos e da sociedade como um todo.

agora o foco está no controle da informação, especialmente quando se trata da proteção de dados pessoais.

Nos Estados Unidos, tal mutação se verificara no *direito de acesso* aos dados armazenados em órgãos públicos de instituições de proteção ao crédito, onde figurou como "núcleo duro" da concepção da *informational privacy;* o mesmo significado estaria presente na autodeterminação informativa estabelecida no Tribunal constitucional alemão, assim como na diretiva 95/46/CE da União Europeia[286].

Na América Latina, especialmente no Brasil, uma terceira via surgiu com a Constituição de 1988. Segundo Doneda, essa via é representada pelo *habeas data* (Art. 5º, LXXII), que se caracteriza como um modelo de proteção de dados pessoais com características próprias. Ele visa garantir ao cidadão o direito de conhecer as informações sobre si mesmo, sendo considerado um direito fundamental[287].

No entanto, o *habeas data*, restrito ao direito de acesso e retificação, mostrou-se insuficiente para garantir o direito à informação, que enfrenta desafios multifuncionais requeridos para a proteção da personalidade. Reconhecer esse direito fundamental se tornou necessário diante da diversidade de novos problemas surgidos na sociedade da informação, onde a tecnologia desempenha um papel significativo[288].

Ao traçar a genealogia do direito à explicação das decisões automatizadas, na perspectiva do ordenamento brasileiro, Renato Leite MONTEIRO (2021) menciona dispositivos infraconstitucionais relacionados com o direito de acesso à informação, como a Lei de Defesa do Consumidor (Lei 8078/1990) e Lei do Cadastro Positivo (Lei 12.414/2011), nos quais o poder judiciário[289] recorreu nas últimas décadas para estabelecer limites à prática de *credit scoring* e formação de bancos de dados sobre histórico de crédito (no ponto em que se veda a utilização de dados não relacionadas com a finalidade de análise de risco de crédito do consumidor) ou dos demais dados sensíveis, entendidos como aqueles pertinentes à "origem

[286] DONEDA, 2021, p. 177.
[287] "(i) trata-se de uma ação que visa a assegurar um direito de acesso e retificação de dados pessoais, ainda que não expresso literalmente; (ii) as duas consequências positivas possíveis da ação seriam constringir o coato a revelar a informação sobre o impetrante e, no caso da sua inexatidão, proceder à sua retificação". (DONEDA, 2021, p. 286)
[288] *Idem*.
[289] TEPEDINO; FRAZÃO; OLIVA, 2020, p. 86 *apud* MONTEIRO, 2021.

racial e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas"[290]

Dessa forma, no âmbito infraconstitucional, o Código de Defesa do Consumidor (CDC) assegura o direito de acesso à informação pessoal no contexto das relações de consumo, garantindo implicitamente o direito à correção e ao cancelamento justificado dos dados[291].

Já na Lei do Cadastro Positivo (Lei 12.414, de 2011), destaca-se a previsão no seu artigo 5º, no tocante aos direitos de:

> Lei 12.414, de 2011. Art. 5º "IV — conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial"; "V — ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento"; "VI — solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados"; e "VII — ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados."

O debate tende a avançar para o plano processual, a extrapolar o âmbito das regras abstratamente estabelecidas em âmbito infraconstitucional.

Conforme defendido por Laura Schertel Mendes, o direito de acesso é um corolário do direito geral à informação e serve para que o indivíduo possa proteger sua personalidade. Esse direito consiste em receber informações completas sobre os dados registrados sobre si mesmo, incluindo onde e quando foram armazenados ou coletados, quem os detém e o respectivo conteúdo[292].

Em ressalva, a autora também menciona, com base em Hans Peter BULL (2005), que embora previsto na maioria das legislações o direito de acesso está sujeito a variações e

---

[290] A propósito, assim definido no art. 5º, II, da LGPD: "dado pessoal sensível: 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;".

[291] "Ana Paula Gambogi Carvalho sustenta o sentido de que até mesmo o pedido do consumidor para incluir dados a seu respeito no cadastro seria pertinente por meio da ação de habeas data". (CARVALHO *in* DONEDA *et al*, 2021, p. 338). No tocante ao CDC, para ilustrar a citação, transcreve-se o artigo 43: "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas."

[292] MENDES, 2014.

limitações (ao acesso), as quais em geral seriam classificáveis em dois grupos: ***(i)*** o interesse público, sob diversas manifestações e ***(ii***) os direitos e interesses privados[293].

Em relação à proteção de dados pessoais, a natureza instrumental do direito de acesso parece estar bem salientada nas lições da professora, das quais se transcreve o seguinte trecho:

> (...) a proteção de dados pessoais depende da garantia de direitos ao titular que possibilitem o efetivo controle da circulação de seus dados pessoais. Isso exige que o titular tenha livre acesso aos seus dados (direito de acesso), possa corrigir dados equivocados e desatualizados (direito de retificação) e que ele possa cancelar dados que foram indevidamente armazenados (direito de cancelamento)[294];

Outras indicações no tocante à instrumentalidade do direito de acesso são observadas na literatura, especialmente no trabalho de MONTEIRO (2021), para quem, embora necessário, o direito de acesso não se afigura suficiente para assegurar a concretização dos demais dele dependentes. Confira-se:

> Apenas o direito de acesso permite ao titular dos dados exercer outros direitos, como a retificação, apagamento e, de certa forma, também o direito à revisão de decisões automatizadas e a efetividade de uma explicação. Mas, por outro lado, o acesso por si só não serve como forma suficiente para que o titular dos dados possua controle sobre fluxos e procedimentos que afetam a sua personalidade, pois o mero fornecimento desses dados provavelmente não permitirá ao titular ter um conhecimento efetivo sobre a forma, como e para o que eles são tratados[295].

A conexão do direito de acesso com a proteção de dados pessoais parece ganhar especial relevância em razão da estatura de direito fundamental a esta conferida pela Emenda Constitucional nº 115, de 2022, que alterou a Constituição Federal "para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais", ao acrescentar o Inciso LXXIX ao artigo 5º[296] .

Raciocina-se que, ao inserir a proteção dos dados pessoais no rol de direitos fundamentais, os demais direitos, mesmo os de "caráter instrumental", adquirem relevância no Sistema Jurídico. Essa leitura é baseada na doutrina de Gilmar Mendes, que afirma que os direitos fundamentais não apenas proíbem a intervenção, mas também exigem proteção

---

[293] BULL, 2005 *apud* MENDES, 2014.
[294] MENDES, 2014.
[295] MONTEIRO, 2021.
[296] Constituição Federal, art. 5º: "LXXIX - *é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais*)."

adequada. Portanto, há não apenas a proibição do excesso, mas também a proibição de proteção insuficiente, conforme expresso por Canaris[297].

Sob a perspectiva mais ampliada, observa-se que haveria conexão do direito à proteção dos dados pessoais com o direito de personalidade.

Cíntia Rosa Pereira de Lima (2020) destaca a doutrina de Danilo Doneda (2021), que considera a privacidade como um aspecto relacional, determinando a forma como a personalidade de uma pessoa se relaciona com outras pessoas e com o mundo exterior. Da mesma forma, o direito à proteção de dados é um direito de personalidade, uma vez que se relaciona ao desenvolvimento do ser humano.[298].

Ao estabelecer a conexão com os direitos fundamentais, seja como um direito autônomo à proteção dos dados pessoais ou como um direito de personalidade específico (autodeterminação informacional), é importante refletir sobre a eficácia desses direitos no âmbito privado, considerando as lições de Menezes Cordeiro (2009,p. 273) citadas por Lima e Ramiro (2022, [n.p]). Os direitos de personalidade são chamados assim porque concedem ao indivíduo o controle sobre uma parte de sua própria esfera de personalidade. Eles se distinguem dos demais direitos por se referirem especificamente à pessoa. Os direitos de personalidade são direitos privados especiais, diferentes do direito geral da personalidade, que consiste na pretensão geral, concedida pela ordem jurídica, de ser reconhecido como pessoa. O direito de personalidade é um direito subjetivo que deve ser respeitado por todos[299].

Com essa breve incursão, cumpre examinar o direito de acesso sob a perspectiva da regulação protetiva de dados pessoais, no Brasil inserida junto aos demais direitos elencados na LGPD (arts. 17 a 22 da LGPD), com os quais, como dito, se relaciona: ***i)*** o direito de obter a confirmação da existência de tratamento; ***ii)*** direito de acesso aos dados; ***iii)*** direito de correção dos dados incompletos, inexatos ou desatualizados***; iv)*** direito à anonimização dos dados pessoais; ***v)*** direito ao bloqueio ou eliminação dos dados desnecessários, excessivos ou decorrentes de tratamento ilícito; ***vi)*** direito à portabilidade dos dados pessoais; ***vii)*** direito à informação sobre o compartilhamento de seus dados pessoais pelo controlador; ***viii)*** informações sobre não fornecimento do consentimento e quais as consequências da negativa;

[297] MENDES, 2012, p. 477.
[298] Nesse ponto, para Cintia Rosa Pereira de Lima, destacam-se a distinção e a eficácia, no âmbito privado, dos direitos de personalidade (o geral e os específicos). (CORDEIRO, 2009, p. 373 *apud* LIMA, 2020)
[299] *Idem*.

ix) direito à revogação do consentimento; ***x)*** direito à revisão das decisões tomadas com base em tratamento automatizado de dados pessoais, dentre outros[300].

Pois bem, no Brasil, a leitura sistemática da LGPD com os "microssistemas" presentes no Ordenamento parece indicar claramente que o direito de acesso resta assegurado sob os diversos prismas de leitura acima enunciados.

Entretanto, convém estender a análise para abordar as polêmicas relacionadas com as possíveis limitações do direito de acesso. Ademais, como já sinalizado, a exemplo das demais legislações, no direito brasileiro, o direito de acesso está em tese sujeito a variações e limitações, cabendo examiná-lo sob essas perspectivas[301].

Ao abordar especificamente o direito a explicação, MONTEIRO (2021) lembra que "os segredos de negócios, previstos no ordenamento Europeu como 'direitos de terceiros' e na LGPD como 'segredo comercial e industrial', aparecem como limitações ao direito à explicação"[302]. Argumenta que, "se os segredos de negócios em tese configuram em limitação ao direito de explicação, por consequência, igualmente se afigurará como limitação ao direito de acesso a determinadas informações".

Portanto, nesse aspecto, opina MONTEIRO (2021), com base em MAHIEU et al, que embora o direito de acesso tenha sido claramente estabelecido na regulação e em que pese a relativa facilidade com que o cidadão possa executá-la (ausência de rigor na definição dos requisitos formais da solicitação), ainda seria insuficientemente claro o alcance prático ou facilidade com que se daria o exercício de tal direito de acesso[303]. Ademais, aparentemente as organizações estão expressamente autorizadas — com fundamento no segredo de negócios — a estabelecer limitações de acesso à informação de muitas maneiras diferentes, seja com base em estratégias corporativas, seja mediante barreiras técnicas[304].

---

[300] Nas lições de Cíntia Rosa Pereira de Lima, todos esses direitos – segundo ensinamentos de Stefano Rodotà – decorrem da autodeterminação informacional, considerada como um dos fundamentos da proteção de dados pessoais (art. 2º, II, da LGPD), direito funcionalmente destinado ao controle das informações que digam respeito ao titular a quem os dados se referem.

[301] Em tópico anterior, já se mencionou o entendimento de Laura Schertel Mendes, baseado em Hans Peter Bull, quanto às variações a que se sujeita o direito de acesso, o qual também poderá sofrer limitações classificáveis em dois grupos: o interesse público, sob diversas manifestações, e os direitos e interesses privados. (BULL, 2005 *apud* MENDES, 2014)

[302] MONTEIRO, 2021, p. 15.

[303] MAHIEU; ASGHARI; VAN EETEN, 2017 *apud* MONTEIRO, 2021, p. 15.

[304] MONTEIRO, *op. cit.*, p. 280.

Em exame realizado sob o prisma da RGPD (art. 15), SARTOR e LAGIOIA (2020, p. 69) destacam que em decorrência dos princípios da transparência e da responsabilização os titulares teriam direito de acesso aos seus dados pessoais bem como às demais informações sobre o tratamento.

Sustentam que o artigo 15.º, n.º 1, alínea f, da RGPD, aborda a tomada de decisão automatizada estabelecendo que o responsável pelo tratamento deverá fornecer, se e quando solicitado pelo titular dos dados, as mesmas informações que deveriam ter sido fornecidas antes de iniciar o tratamento de acordo com o 13.º, n.º 2, alínea f e 14.º (2)(g). Eles entendem que a informação obrigatória concerne à "existência de tomadas de decisão automatizadas" e "informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas de tal tratamento para o titular dos dados".

Além disso, argumentam que é importante ter em conta o "considerando 63", que trata explicitamente do direito de acesso à informação. Em primeiro lugar, o direito de acesso inclui o direito do titular dos dados de saber, sempre que possível, a lógica envolvida em qualquer tratamento automatizado de dados pessoais e, pelo menos quando baseado na definição de perfis, as consequências desse tratamento. No entanto, isso não deve afetar negativamente os direitos ou liberdades de terceiros, incluindo segredos comerciais, propriedade intelectual e, em particular, os direitos autorais que protegem o software[305].

No entanto, eles ressaltam que o considerando 63 estabelece que a limitação não deve resultar na negação completa do direito à informação[306].

Em suma, segundo esses autores, há ainda ampla discussão sobre se o artigo 15.º deve ser lido como concedendo aos titulares dos dados o direito de obter uma explicação individualizada de avaliações e decisões automatizadas.

Haveria, no entender de SARTOR e LAGIOIA (2020), ambiguidades tanto na redação do artigo 15.º quanto no considerando 63 a ele relacionado, os quais não especificaram se a obrigação de fornecer informações sobre a "lógica envolvida" diz respeito apenas ao fornecimento de informações gerais sobre os métodos adotados no sistema, ou informações específicas sobre como esses métodos foram aplicados ao titular dos dados[307].

---

[305] SARTOR; LAGIOIA, 2020, p. 69.
[306] *Idem*.
[307] *Idem*.

Em relação à perspectiva da regulação brasileira, MONTEIRO (2021, p. 280 et seq.) argumenta que ainda que as obrigações de transparência passiva e ativa possam em tese assegurar aos titulares dos dados o direito de acesso à integralidade dos dados pessoais utilizados no processo decisório automatizado, dadas as limitações cognitivas do indivíduo, o simples fornecimento desses dados, por si só, certamente poderá não permitir ao titular pleno conhecimento sobre como seus dados são tratados, muito menos em contexto de sistemas complexos automatizados como o de IA[308].

Portanto, em remate, firma-se aqui a ideia de que o direito de acesso em si, ainda que corroborado pelos demais direitos conferidos ao titular pode não ser suficiente para lhe assegurar efetivo controle sobre o fluxo de dados e a autodeterminação informativa. Assim, é preciso prosseguir no exame do debate.

5.2.1 Direito de oposição ao tratamento de dados

Conforme aponta a doutrina, o exame do direito de oposição, previsto no artigo 18, §2º da LGPD[309], padece das mesmas dificuldades interpretativas enfrentadas no âmbito do direito de acesso, sobretudo porque sua leitura é conjugada com os permissivos do legítimo interesse e os da dispensa de consentimento.

Contudo, esses últimos teriam sido relativizados em face do direito de oposição, este aplicável em tese em caso de descumprimento dos requisitos legalmente estabelecidos para o tratamento[310].

Dado que a Lei Geral de Proteção de Dados (LGPD) foi inspirada no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, é importante analisar o artigo 21 correspondente, que estabelece claramente duas questões[311]: (1) o titular dos dados não está

[308] MONTEIRO, 2021, p. 280.

[309] LGPD: "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: (...)
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei."

[310] O comentário de Bruno Bioni (2021), em relação ao direito de oposição disposto no art. 18 da LGPD, "houve atecnicidade na redação da lei, haja vista que as outras bases legais não são exceções ('dispensa') ao consentimento. Provavelmente, isso se deve em razão do fato de que, ao longo das diversas versões do anteprojeto da lei, o consentimento foi tratado como regra".

[311] RGPD (versão portuguesa): "**Artigo 21º Direito de oposição** 1.O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6º nº 1, alínea e) ou f), ou no artigo 6º, nº 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e

sujeito a decisões automatizadas, como o perfilamento; e (2) o titular dos dados tem o direito de se opor ao processamento de seus dados para fins de marketing direto. No entanto, é importante destacar que, no contexto do RGPD (Artigo 7º, parágrafo 3), o direito de oposição não se aplica diretamente a um tratamento baseado no consentimento, no qual o regulamento permite a retirada do consentimento como meio suficiente para interromper o processamento.

De acordo com Sartor e Lagioia (2020, p. 59), o direito de oposição permite que os titulares de dados se oponham ao processamento de seus dados. Alguns pontos importantes a serem observados são: (I) o titular dos dados pode alegar uma situação pessoal/particular para fundamentar essa oposição; (II) o responsável pelo tratamento dos dados só pode continuar o processamento se puder demonstrar motivos legítimos e convincentes que sobrepujem os interesses e liberdades do titular dos dados; (III) geralmente, o direito de oposição não se sobrepõe ao interesse público exercido por uma autoridade legítima, a menos que haja bases legais específicas; (IV) o direito de oposição em relação à criação de perfis e ao marketing direto não requer qualquer justificativa pessoal por parte do titular dos dados, e cabe ao responsável pelo tratamento facilitar o exercício desse direito de forma simples, intuitiva e padronizada; (V) o direito de oposição em relação ao processamento para fins de pesquisa e estatística diz respeito à oposição à inclusão de dados pessoais relacionados ao titular como dados de entrada para o tratamento. Em teoria, os resultados das pesquisas e estatísticas não devem consistir em dados pessoais. No entanto, em princípio, o direito de oposição não se sobrepõe ao tratamento realizado por motivos de interesse público. Essa exceção é prevista no artigo 89º, que permite a oposição, a menos que haja algum interesse público relevante para pesquisa científica, histórica ou estatística. Nesse caso, o eventual apagamento de dados pessoais não prejudicaria seriamente os objetivos do tratamento para fins de arquivo, pesquisa

liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial. 2.Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta. 3.Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim. 4.O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se referem os nº 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações. 5.No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas. 6.Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89º, nº 1, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público."

ou estatística, especialmente em contextos de tratamento massivo de dados (como o big data) usado para treinamento do sistema ou definição de modelos algorítmicos[312].

No que concerne a este alinhamento da LGPD com o espírito da RGPD, ensina a professora Cintia Rosas Pereira de Lima (2020, [n.p.]) :

> (...) a LGPD assegura ao titular o direito de rever as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses (art. 20), para tanto, o controlador deve fornecer, sempre que solicitadas, informações claras e adequadas sobre os critérios e os procedimentos utilizados para a decisão automatizada (§1º do art. 20 da LGPD)". Ocorre que nem sempre essa cautela é adotada pelo controlador, e os titulares dos dados desconhecem a realização de tais práticas, por isso, nesse ponto é crucial que a ANPD realize auditorias para verificar essas práticas e adequação destas com os dispositivos legais nos termos do § 2º do art. 2º da LGPD.

Na doutrina nacional, Cíntia Rosa Pereira de Lima (2020, [n.p.]) categoriza tanto o direito de oposição quanto o direito de "não sujeição" (de revisão) à decisão automatizada, sob o procedimento estabelecido no artigo 20 da LGPD. Isso se aplica não apenas a decisões automatizadas, mas também ao caso do perfilamento, como previsto no Regulamento Geral de Proteção de Dados da União Europeia (RGPD: artigos 20º e 21º) [313]. A professora ensina que a LGPD assegura ao titular o direito de revisar as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses (art. 20), e o controlador deve fornecer informações claras e adequadas sobre os critérios e procedimentos utilizados para a decisão automatizada, quando solicitadas (§1º do art. 20 da LGPD).

No entanto, muitas vezes essa cautela não é adotada pelo controlador, e os titulares dos dados desconhecem a realização dessas práticas. Nesse ponto, é crucial que a ANPD realize auditorias para verificar essas práticas e a conformidade com os dispositivos legais, conforme estabelecido no § 2º do art. 2º da LGPD.

Para Bruno BIONI (2021, p. 173 *et seq.*), o chamado direito de oposição guarda semelhança com a hipótese de revogação do consentimento, na medida em que, a despeito das

---

[312] SARTOR; LAGIOIA, 2020, p. 59.

[313] Tema abordado em tópico anterior, ao que se anota a observação de Cintia Rosa Pereira de Lima (2020), no sentido de que o termo deriva da expressão *online profiling* e que em relação a ela, Frederik Borgesius explicaria que esse processo "seria construído com base no monitoramento do comportamento do usuário na internet com objetivo de enviar publicidade direcionada aos interesses detectados com base neste monitoramento (*direct marketing*)" e que, para Eli Parisier, "haveria riscos nesta prática na medida em que ocorre a doutrinação do indivíduo com base nesse perfil, segundo o diagnóstico de que se cria um 'filtro invisível' (uma bolha) afetando na própria interação deste indivíduo com outras pessoas e no acesso à informação". Além disso, acrescenta a autora, "há um risco à privacidade na medida em que o histórico do comportamento do indivíduo é vasculhado sem que se tenha conhecimento para poder consentir ou não".

bases legais autorizativas (art. 7º) [314] , a LGPD viabiliza ao titular dos dados – no caso de descumprimento - meios para obstruir o tratamento, mesmo porque, ao que se depreende, os permissivos das respectivas bases legais (art. 18) [315] estão condicionados à regularidade do tratamento dos dados pessoais.

No entanto, de acordo com o autor, diferentemente da revogação do consentimento, que é um direito potestativo sem limitações pré-estabelecidas, o exercício do direito de oposição encontra limitações e está condicionado à violação das normas, o que impede uma interpretação inicial apressada de que o exercício desses dois direitos de objeção teria alcances distintos[316].

Portanto, o exercício do direito de oposição não depende apenas da vontade do titular, pois pressupõe uma violação das disposições da LGPD.

Além disso, segundo Bioni, não se deve permitir uma assimetria normativa indesejada entre essas bases legais como resultado do exercício do direito de oposição. O objetivo é

---

[314] "Bases legais" para o tratamento. LGPD: "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 terceiros; 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 terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. 1º (Revogado). § 2º (Revogado). § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei."

[315] LGPD, art. 18: "§ 2.º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei" (g.n.). Afirma Bioni que, nesse ponto, "houve atecnicidade na redação da lei, haja vista que as outras bases legais não são exceções ("dispensa") ao consentimento. Provavelmente, isso se deve em razão do fato de que, ao longo das diversas versões do anteprojeto da lei, o consentimento foi tratado como regra".

[316] Entendido como um direito subjetivo que confere ao titular a possibilidade de constituir, modificar ou extinguir uma situação subjetiva com uma declaração de vontade, sem que a outra parte possa se opor. Cf: CHIOVENDA, 2000 *apud* BIONI, 2021.

equalizar todas as bases legais, de modo que seja buscada uma interpretação que coloque em pé de igualdade as hipóteses de legitimação para o tratamento de dados pessoais, especialmente o consentimento perante o legítimo interesse[317].

Bioni também argumenta que a LGPD não detalha adequadamente o direito de oposição, especialmente em relação à base legal do legítimo interesse, embora reconheça a existência de uma "dialética normativa que coteja a autodeterminação informacional perante os demais fundamentos da LGPD[318].

Em que pesem as polêmicas no âmbito hermenêutico, alinhamo-nos ao argumento de Ana FRAZÃO, Ângelo Prata CARVALHO e Giovanna MILANEZ (2022, p. 598), no sentido de que o direito de oposição integra o conjunto de direitos acionáveis no âmbito do procedimento estabelecido no artigo 20, relacionado com o direito de revisão (e de explicação) de decisões automatizadas. Transcreve-se[319]:

> É no contexto dos desafios inerentes à nova economia que o art. 20 da LGPD pretende criar uma espécie de devido processo legal para proteger os cidadãos contra a "tirania" dos julgamentos automatizados. Para tal fim, foi criado um verdadeiro bloco de direitos, cujos principais desdobramentos são os seguintes: 1. O direito de acesso e informação em relação a respeito dos critérios e procedimentos utilizados para a decisão automatizada; 2. O direito de oposição quanto à decisão automatizada e de manifestar o seu ponto de vista; 3. O direito de obtenção da revisão da decisão automatizada; e 4. O direito de petição à autoridade nacional para a realização de auditoria, em caso da não prestação das informações. Como se pode observar, tais direitos decorrem não apenas da autodeterminação informativa do cidadão e do controle que a lei lhe atribui sobre os seus dados pessoais, mas também de importantes princípios.

---

[317] Neste particular, Bruno Bioni assevera que "a forma pela qual foi costurado o legítimo interesse na LGPD também confere uma posição jurídica ao titular de objeção ao tratamento de seus dados lastreado em tal base legal. Nesse sentido, a expressão 'legítima expectativa' tem igualmente uma conotação subjetiva, vinculada ao que o próprio titular deseja e espera que seja feito com seus dados. Caso contrário, a última fase do LAI, relativa ao dever de transparência, não funcionalizaria um dos fundamentos da lei, que é a autodeterminação informacional (LGPD: art. 2 §2º). Em poucas palavras, se na medida em que é dada transparência acerca do tratamento de dados com base no legítimo interesse e o titular a ele se opõe, caso o agente de tratamento de dados não o acate, estará violando uma das normas da Lei Geral de Proteção de Dados Pessoais. Trata-se de uma interpretação sistemática entre os arts. 10, II e § 2.º, e 18, § 2.º. No entanto, deve-se observar que esse direito não é absoluto. Se por um lado a posição jurídica de processar dados sem o consentimento prévio não pode ser abusada a ponto de lhe retirar por completo a sua capacidade de autodeterminação informacional, por outro lado, tal direito de objeção também deve ser contornado pela figura do abuso de direito".

[318] De fato, a LGPD: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

[319] FRAZÃO; CARVALHO; MILANEZ, 2022, p. 598.

5.2.2 Direito de revisão e de explicação de decisões automatizadas

Em tópicos anteriores, ilustrou-se o cenário sob o qual os sistemas de IA possuem acesso a quantidades massivas de informações sobre indivíduos (inclusive sobre pessoas de seu contato, ou não, com perfis semelhantes a eles) e da potencialidade de, com base nessas novas tecnologias associadas, utilizar-se de tais informações para induzir comportamentos e/ou mesmo à guisa de preditores (enquanto dados de entrada) servir de apoio para a tomada de decisões automatizadas, por vezes potencialmente danosas a direitos desses indivíduos (ou grupos de indivíduos) a cujos dados pessoais a tomada de decisão se relaciona.

A esse propósito, autores como CITRON e PASQUALE (2014) ressaltam que a disseminação de sistemas automatizados (a exemplo de pontuação de crédito) nesta *Era Informacional* implica na necessidade do escrutínio de seu funcionamento, o que se daria mediante institucionalização de procedimentos regulares de verificação (desses sistemas) daquilo que concerne à sua atuação direta nos diversos contextos da vida de um indivíduo, ampliando ou limitando as suas oportunidades.

Conforme salientado por FLORID et al (2018) [320], no contexto em que uma avaliação ou decisão foi tomada com respeito a seus dados, os cidadãos basicamente querem saber como e por que uma determinada resposta algorítmica foi dada ou uma decisão foi tomada, para ao fim e ao cabo "entender e responsabilizar os processos de tomada de decisão da IA".

Em outras palavras, diante da possibilidade de materialização (e perpetuação) de uma injustiça algorítmica, para além da expectativa de manutenção de controle sobre o tratamento de dados pessoais, surge a necessidade de entender (e possivelmente contestar) as razões das avaliações e decisões que afetam as pessoas a quem os dados se referem, assim como se potencializa as preocupações relacionadas com a transparência/explicabilidade algorítmica.

Portanto, é defensável a ideia de que é necessário sujeitar os sistemas automatizados a determinados requisitos de justiça na mesma medida dos seus impactos na vida dos indivíduos (CITRON, PASQUALE, 2014)[321].

[320] FLORIDI *et al*, 2018 *apud* SARTOR; LAGIOIA, 2020, p. 48.
[321] CITRON; PASQUALE, 2014 *apud* MONTEIRO, 2021.

No que concerne à quebra de confiança na organização que utiliza os sistemas de IA[322] BALKIN (2017) a atribui à quebra de expectativa dos indivíduos aos quais os dados utilizados se relacionam. Argumenta que, "afinal, as pessoas têm o interesse de não serem enganadas ou manipuladas, assim como possuem forte interesse em poder confiar nessas tecnologias", quiçá também acreditando que os lucros dos agentes (que as utilizam) não provenham das suas limitações cognitivas em relação ao uso que fazem de seus dados pessoais[323].

Por outro ponto de vista, Sartor e Lagioia (2020) afirmam que é possível identificar, de forma indireta, o interesse dos cidadãos em uma competição algorítmica justa. Entre suas expectativas normais, está a de não estarem sujeitos a abusos de poder de mercado resultantes do controle exclusivo sobre grandes quantidades de dados e tecnologias[324].

Estes autores argumentam que a falta de concorrência pode afetar negativamente os consumidores, privando-os de alternativas e limitando suas escolhas. No entanto, essa preocupação afeta diretamente os concorrentes em si[325]. Eles também apontam que a falta de concorrência permite que as empresas líderes obtenham enormes lucros, aumentando seu poder de mercado. Isso pode ser usado para influenciar a opinião pública e a política, por exemplo, através da compra "preventiva" de potenciais concorrentes.

Para esses autores, portanto, ao examinar o direito de revisão e explicação no contexto de decisões automatizadas por sistemas de IA, é importante considerar a extensão coletiva desses direitos, uma vez que eles podem entrar em conflito com a proteção conferida aos segredos comerciais. Além disso, argumentam, ao analisar as possíveis relações entre esses

---

[322] A regulação do fluxo de dados "se traduz em demanda da sociedade da informação e não foi puro acaso a inserção da proteção de dados pessoais, essa agora entendida como resultado da evolução da concepção individualística da privacidade, apoiando-se atualmente no prestígio da boa-fé e na manutenção da confiança dos indivíduos nesse ecossistema de tratamento de dados". Em reforço a essa linha interpretativa, coteje-se o objetivo declarado nas estratégias nacionais em torno da construção de um marco regulatório para a IA, especialmente a brasileira consubstanciada na EBIA 2021. (EBIA, 2021)

[323] Avaliação baseada em BALKIN, 2017 *apud* SARTOR, LAGIOIA, 2020, p. 48.

[324] "(...) *citizens have an indirect interest in fair algorithmic competition, i.e., in not being subject to market-power abuses resulting from exclusive control over masses of data and technologies. This is of direct concern to competitors, but the lack of competition may negatively affect consumers, too, by depriving them of valuable options and restricting their sphere of action*". (SARTOR; LAGIOIA, *op. cit*., p. 49)

[325] Como se vê, embora a problemática concorrencial não integre diretamente o escopo deste trabalho, a questão tangencia os desafios dialógicos entre o segredo de negócios e o tratamento de dados pessoais, da qual se ocupa este estudo. Como visto, a Lei nº 9.279, de 1996, ao tratar da tutela aos segredos de negócios, opta pela criminalização de sua revelação indevida, pretendendo, de forma oblíqua, proteger a lealdade na concorrência em geral. Especificamente, ressalve-se que, embora mencionada como um dos fundamentos na LGPD (art. 2º II), a regulação nos domínios dos abusos de poder no mercado não é nela tratada substantivamente e, sim, na Lei Antitruste (Lei nº 12.529, de 2011), que estrutura o Sistema Brasileiro de Defesa da Concorrência e dispõe sobre a prevenção e a repressão às infrações contra a ordem econômica.

interesses protegidos, é necessário determinar se existe uma relação de transcendência ou prevalência de um direito sobre o outro[326].

Em suma, mais do que a busca de respostas, foi escopo deste tópico refletir sobre os seguintes pontos relacionados com a disciplina legal da decisão automatizada (LGPD: art. 20): ***(i)*** se, de fato, aludido permissivo legal aplica-se a todo e qualquer tipo de decisões automatizadas; (***ii)*** se, efetivamente, no âmbito das decisões automatizadas, resta assegurado um direito "absoluto" à explicação; e ***(iii)*** se foram estabelecidas e quais seriam as salvaguardas ao mister de equilibrar simetricamente os respectivos interesses em causa[327].

5.3 INTERPRETANDO O ARTIGO 20 DA LGPD

Dada a complexidade decorrente da imbricação entre o tema do segredo de negócios com a questão da explicabilidade das decisões automatizadas e que tal complexidade é agravada no contexto da utilização de sistemas de IA, é necessário algumas digressões nos parênteses adiante.

Com base na reflexão de BOBBIO[328] sobre o papel dos mistérios e dos segredos na democracia, no cotejo das prescrições normativas (LGPD: art. 20) — e com base no entendimento dos comentaristas referenciados —, busca-se discernir o que "é bom, útil e oportuno" que o titular saiba em relação à decisão automatizada para assim poder distinguir os impedimentos factuais de acesso ao conhecimento das possíveis razões jurídicas (como a proteção do segredo) e mesmo das limitações cognitivas atribuíveis a ele próprio[329]. Essas

[326] Esse contexto, em tese, afastaria a pertinência de possível concertação entre tais atores, para fins conciliatórios, senão na renúncia ou parcial disposição de algum de seus direitos em proveito da outra.

[327] Substancialmente, esses pontos foram objetos de exame no artigo "O direito à explicação: entre a experiência europeia e a sua positivação na LGPD". (DONEDA *et al*, 2021)

[328] "O segredo não é por si mesmo um bem ou um mal. É bom quando impede que se conheça aquilo que é bom, útil ou oportuno que se ignore; é mau quando impede que se saiba aquilo que seria bom, útil e oportuno que se soubesse. O mistério, ao contrário, diz respeito àquilo que, ainda que fosse bom, útil e oportuno que se conhecesse, não consegue ser conhecido, ou por dificuldades de acesso às fontes ou pela intervenção de um poder superior ou mesmo somente pela insuficiência de nossas capacidades cognitivas (...)

O segredo é um artifício institucional. O mistério, ao contrário, ao menos enquanto não for dissipado, é um limite ao nosso conhecimento, que somente pode ser batido mediante trabalho intenso no mesmo plano do conhecimento, no desvelamento daquilo que está oculto. Um evento pode deixar de ser secreto mediante um decreto. Nenhum decreto pode fazer com que algo deixe de ser misterioso". (BOBBIO, 2015, p. 78, g.n.)

[329] Ao discorrer sobre o segredo de negócios, nos âmbitos do direito de explicação, Frazão *et al* (2022) destacam que, sem os esclarecimentos "por parte dos agentes de tratamento, estar-se-á admitindo que julgamentos

distinções também visam afastar qualquer caráter misterioso ou místico atribuído à tecnologia envolvida nos desenvolvimentos da IA, que poderiam, hipoteticamente, escapar dos alinhamentos do inciso II, do §4º do art. 18 da LGPD[330].

Como mencionado anteriormente, enquanto pairam dúvidas em relação ao sentido e alcance de vários preceitos da LGPD, há pouca controvérsia quanto à existência do direito de explicação no contexto das decisões exclusivamente automatizadas, principalmente porque tal prerrogativa não é uma novidade no ordenamento jurídico, uma vez que já estava prevista em leis setoriais anteriores à LGPD, como a Lei de Cadastro Positivo (Lei 12.414/2011: Art. 5º) [331] e o Código de Defesa do Consumidor (Lei 8.078/1990)[332].

Com a edição da LGPD, aplicável a qualquer hipótese de tratamento de dados pessoais nela definidos, ampliou-se a aplicabilidade do procedimento de revisão das decisões automatizadas, a partir da regra no caput do Art.20, este complementado pelo seu §1º, no sentido de estabelecer a obrigação do controlador de – sempre que solicitado – fornecer ao titular dos dados, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, "observados os segredos comercial e industrial" [333].

Naturalmente, a disposição do artigo 20, de natureza procedimental, não implica a exclusão dos demais direitos conferidos ao titular dos dados pessoais (LGPD: Art. 17 ao Art.

---

algorítmicos continuem sendo verdadeiras caixas-pretas, o que é inadmissível com uma sociedade que pretenda ser minimamente democrática" e que para além da violação aos princípios e direitos um ambiente de opacidade seria "(...) um grande e poderoso incentivo para utilizações abusivas e para discriminações ilícitas (...).".

[330] LGPD, art. 18: "§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência." (g.n.)

[331] Lei nº 12.414, de 2011: "Art. 5º São direitos do cadastrado: (...) VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e (...)"

[332] O art. 43 CDC disciplina os arquivos de consumo e estabelece o direito de acesso do consumidor aos cadastros e aos bancos de dados, às informações a seu respeito e às respectivas fontes; também, determina o dever de clareza dos arquivos, bem como o direito de retificação de informações incorretas e que o consumidor:
"Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas."

[333] Lei nº 13.709, de 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. § 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."

22, entre outros), os quais, em princípio, podem ser exercidos no contexto do direito de revisão em relação a uma tomada de decisão automatizada ou avaliação destinada a definir o seu perfil pessoal, profissional, de consumo, crédito ou aspectos de sua personalidade[334].

Confira-se:

> LGPD: 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. G.n.
>
> § 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.

A discussão sobre a existência de um "direito à explicação" aparentemente teve origem no debate sobre a regulação da União Europeia (RGPD), que também serviu de inspiração para a legislação nacional. Existe um consenso relativo em ambos os contextos de que esse direito deriva de outros direitos ou, no mínimo, viabiliza o exercício de outras prerrogativas conferidas ao indivíduo. Isso inclui o princípio da transparência, o direito de acesso à informação e, principalmente, o direito de solicitar revisão de decisões automatizadas[335].

Segundo FRAZÃO et al. (2022, p. 660-661), a complexidade interpretativa dessa questão pode resultar dos esforços da LGPD em conciliar os vários interesses protegidos, especialmente por meio do procedimento estabelecido no artigo 20. Esse conjunto de regras pode, na prática, garantir a salvaguarda dos interesses e direitos de todas as partes envolvidas, inclusive os relacionados ao dever de manter segredos comerciais.

Nesse aspecto, considere-se a avaliação de CASEY et al (2018) – focada na regulação europeia – quanto ao fato de que, embora o direito à explicação não implique em uma abertura

---

[334] A regra da proibição geral às decisões automatizadas está presente na RGPD, que as autoriza pela via da exceção, o que não ocorre na lei brasileira (LGPD). “Em vez de proibir e criar salvaguardas para lidar com exceções a LGPD, cria um amplo direito de 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 da sua personalidade. Nesse sentido, permite maior flexibilidade no uso dessas técnicas”. (SOUZA; PERRONE; MAGRANI *apud* DONEDA *et al.*, p. 281)

[335] SOUZA; PERRONE; MAGRANI *apud* DONEDA *et al.*, 2021, p. 262.

completa da "caixa preta"[336], é preciso balancear os respectivos mecanismos "*ex post*" a um sistema de avaliação de riscos "*ex ante",* como forma de se atender as orientações de autoridades locais (europeias) no tocante aos interesses de *stakeholders* relevantes envolvidos, interesses concernentes à compreensão do processamento geral dos sistemas envolvidos, com vistas ao desenvolvimento de práticas de documentação e de justificação de determinadas características desses sistemas de tomada de decisão automatizadas.

Na defesa da avaliação "balanceada" que fazem do direito à explicação dos sistemas algorítmicos, esses autores ainda argumentam - *apud* MONTEIRO (2021, p.55)[337] – que eventual atenção excessiva na transparência desses sistemas implicaria em deslocar desmedidamente o peso sobre os indivíduos ("*falácia de transparência*"), que teriam que envidar esforços na interpretação dessas informações, cuja compreensão nem sempre seria viável.

Portanto, alinhado a CASEY et al. (2018), acredita-se que o conjunto de informações técnicas, em si complexas e de difícil entendimento para o cidadão médio (não especialista), seria inútil ou irrelevante para o exame dos efeitos/resultados das decisões automatizadas sobre os direitos e liberdades individuais. Além disso, essas informações seriam pouco esclarecedoras sobre a finalidade efetiva do tratamento dos dados pessoais considerados.

Além disso, ao ler o artigo 20 da LGPD, observa-se que o direito de revisão se aplica a decisões tomadas exclusivamente com base no tratamento automatizado de dados pessoais, afetando os interesses do titular desses dados. Isso inclui decisões que visam definir perfis pessoais, profissionais, de consumo e de crédito, bem como aspectos da personalidade.

---

[336] PASQUALE, 2015.

[337] Para estender a análise neste ponto, considere-se ainda o posicionamento de Casey *et al*, na resenha de Renato Leite Monteiro, nos seguintes termos: "(...) as vantagens de mudar o foco do debate sobre o direito à explicação seriam as seguintes: o primeiro é que o foco na transparência interna de sistemas pode colocar um peso excessivo sobre os indivíduos, que devem buscar e interpretar as informações (o que se convencionou denominar 'falácia da transparência'). A provisão de explicações básicas diante de demandas individuais pode, ainda, dissimular as razões de empresas cujos sistemas de tratamento de dados sejam enviesados de outras formas. Além disso, em muitos casos, especialmente de sistemas de *machine learning* altamente complexos, o custo para obter uma explicação pode ser muito alto e superar o benefício dessa explicação a nível individual; por fim, o que é considerado mais importante é que auditorias de sistema do tipo vislumbrado pelos DPIAs já têm um histórico positivo na detecção e combate de discriminação em algoritmos opacos e têm a vantagem de permitir a interação com entidades externas, muitas vezes com mais recursos e conhecimento do que indivíduos isolados". Em prosseguimento ao exame da questão, Renato L. Monteiro, destaca que debate inconcluso no âmbito dos atores da academia e das organizações da sociedade civil cujas proposições até agora giram em torno dos modelos de relatórios de impacto, de auditorias, de testes e de outras medidas de mitigação de riscos das decisões automatizadas.

A partir do entendimento do caput do Art. 20 da LGPD, podemos inferir que a prescrição normativa subsequente (LGPD: Art. 20, §1º) impõe ao controlador a obrigação de fornecer informações claras (facilitando a compreensão) e adequadas (relacionadas à finalidade pretendida, ao exercício de outros direitos, especialmente o direito de revisão). Essas informações devem abranger os critérios e procedimentos utilizados para as decisões automatizadas, observando os segredos comerciais e industriais.

Portanto, no contexto das decisões automatizadas, é preciso considerar que as dificuldades de entendimento e explicação derivadas da opacidade algorítmica podem decorrer de um ato de vontade (opções de design inerentes à arquitetura do modelo computacional adotado) como também de injunções legais.

Nesse sentido, para além das dificuldades interpretativas tem-se os esforços das legislações nacionais e internacionais de proteção de dados na tentativa de **equacionar os interesses envolvidos**, de um lado assegurando os direitos à transparência, à explicação e a de não ficar sujeito a decisões automatizadas; de outro, de igualmente assegurar tutela de direitos, em tese legítimos, conferidos aos controladores/desenvolvedores da tecnologia, a exemplo dos segredos de negócios (MONTEIRO, 2021) [338].

A consideração de que a tecnologia contemporânea é complexa e opaca é resultado de um longo processo de desenvolvimento técnico. Isso nos leva a reconhecer que explicações simplistas, fornecidas apenas para cumprir o princípio da transparência, podem não ser suficientes para avaliar a problemática em questão, que diz respeito à explicabilidade dos modelos utilizados em processos de tomada de decisão automatizados, e também para mitigar os potenciais riscos aos quais os cidadãos estão expostos.

Embora o direito à explicação esteja respaldado por um amplo conjunto de direitos garantidos na LGPD (Art. 20, Art. 18, Art. 6, etc.), é importante ressaltar que sua implementação prática encontra obstáculos não apenas nos limites impostos pelo segredo de negócios, mas também na crescente complexidade dos algoritmos e na consequente opacidade natural desses sistemas.

Neste ponto, a LGPD se assemelha à RGPD, que — ao estabelecer nos artigos 13º[339] e

[338] MONTEIRO, 2021.

[339] RGPD: "**Artigo 13º - Informações a facultar quando os dados pessoais são recolhidos junto do titular - 1 - Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe,**

14º [340]as obrigações do controlador de prestar informações —, parece viabilizar concretude ao

aquando da recolha desses dados pessoais, as seguintes informações: (a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante; (b) Os contactos do encarregado da proteção de dados, se for caso disso; (c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; (d) Se o tratamento dos dados se basear no artigo 6.o, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro; (e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; (f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.o, ou no artigo 49.º, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas. **2 - Para além das informações referidas no n.º 1, o responsável pelo tratamento fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente**: (a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo; (b) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratamento no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados; (c) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.o, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; (d) O direito de apresentar reclamação a uma autoridade de controlo; (e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados; (f) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.o, n.[os] 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados. **3 - Quando o responsável pelo tratamento de dados pessoais tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do n.º 2. 4- Os n.[os] 1, 2 e 3 não se aplicam quando e na medida em que o titular dos dados já tiver conhecimento das informações**."

[340] RGPD: "**Artigo 14º - Informações a facultar quando os dados pessoais não são recolhidos junto do titular – 1 - Quando os dados pessoais não forem recolhidos junto do titular, o responsável pelo tratamento fornece-lhe as seguintes informações**: (a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante; (b) Os contactos do encarregado da proteção de dados, se for caso disso; (c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; (d) As categorias dos dados pessoais em questão; (e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; (f) se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas; **2 - Para além das informações referidas no n.º 1, o responsável pelo tratamento fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente:** (a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo; (b) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro; (c) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratamento no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados; (d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.º, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; (e) O direito de apresentar reclamação a uma autoridade de controlo; (f) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público; (g)A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.º, n.[os] 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados. **3 - O responsável pelo tratamento comunica as informações referidas nos n.[os] 1 e 2: (a)** Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados; (b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou (c) Se estiver prevista a divulgação dos dados pessoais

princípio da transparência mesmo antes da tomada da decisão automatizada, cuja revisão seria fundada no respectivo artigo 22º (nº 1)[341] .

No âmbito da legislação nacional, é possível inferir da leitura restrita ao artigo 20 da LGPD[342] que a divulgação de informações claras e adequadas (§1º) tem como objetivo permitir que o titular dos dados exerça o direito de revisar decisões totalmente automatizadas que o afetem em seus interesses. O controlador é advertido de que a recusa com base na proteção dos segredos comerciais pode levá-lo a ser auditado pela autoridade nacional para verificar a existência de discriminação no tratamento (§2º).

No entanto, como já observado em relação aos direitos de acesso e oposição, a LGPD (Art. 18, I, II e III)[343] concede ao titular o direito de confirmar a existência de tratamento, acessar seus dados e solicitar a correção de informações incompletas, imprecisas ou desatualizadas. Isso inclui a possibilidade de solicitar a anonimização, o bloqueio ou a exclusão de dados considerados desnecessários, excessivos ou tratados em desacordo com a LGPD.

---

a outro destinatário, o mais tardar aquando da primeira divulgação desses dados. **4 - Quando o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados pessoais tenham sido obtidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes referidas no n.º 2**. - **5 - Os n.os 1 a 4 não se aplicam quando e na medida em que: (a)** O titular dos dados já tenha conhecimento das informações; (b) Se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, sob reserva das condições e garantias previstas no artigo 89.º, n.º 1, e na medida em que a obrigação referida no n.º 1 do presente artigo seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento. Nesses casos, o responsável pelo tratamento toma as medidas adequadas para defender os direitos, liberdades e interesses legítimos do titular dos dados, inclusive através da divulgação da informação ao público; (c) A obtenção ou divulgação dos dados estejam expressamente prevista no direito da União ou do Estado-Membro ao qual o responsável pelo tratamento estiver sujeito, prevendo medidas adequadas para proteger os legítimos interesses do titular dos dados; ou (d) Os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade."

[341] RGPD: "Art. 22º (...) 1º O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar."

[342] LGPD: "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 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."

[343] LGPD: "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;"

Essas obrigações teoricamente se aplicam, por extensão, a outros agentes de tratamento com os quais os dados tenham sido compartilhados (Art. 18 §6º)[344].

Vale lembrar que o tratamento de dados está sujeito aos requisitos e condicionantes específicos, como o da exigência de prévio consentimento, quando e se aplicável (Art. 7º-I e §6º; Art. 8º; Art.9º §1º; Art. 11-I); da verificação da legitimidade dos interesses do controlador, neste caso, subordinados aos direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (Art. 7º IX).

Nessa linha, importa considerar a restrição imposta em relação ao tratamento irregular (LGPD: art. 44)[345] ou realizado de forma ilícita (Código Civil: artigos 186; 187 e 927)[346], circunstâncias cujas ocorrências atrairiam os efeitos jurídicos estabelecidos no ordenamento, inclusive no tocante à imputação de responsabilidades.

Naturalmente, sem danos (ou ameaça de dano) a direito ou interesse protegido, não há que cogitar em imputação de responsabilidade, não há o que reparar ou assegurar, tampouco se impõe o direito de revisão a que alude o Artigo 20 da LGPD.

Portanto, uma vez que o propósito final do direito de revisão (e explicação) é a proteção de um interesse, como enfatizado por REIS e FURTADO (2021), é com base nesse interesse que se pode avaliar a necessidade e a utilidade dos mecanismos jurídicos de proteção contra decisões automatizadas[347].

---

[344] LGPD, art. 18: "§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional."

[345] LGPD: "Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."

[346] Código Civil: "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."
"Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes."
"Art. 927. Aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem."

[347] Em apoio à argumentação, esses autores rememoram ao instituto do direito subjetivo, na construção doutrinária. (ANDRADE, 1992, p. 8 *apud* REIS; FURTADO, 2022)

Nesse sentido, os autores referenciados argumentam que "*se algum interesse juridicamente protegido for violado ou ameaçado pela decisão automatizada, há, quando menos, o direito de questionar em juízo o ato da máquina, por força da garantia do direito de ação (CF, art. 5º, XXXV)"*[348].

Além disso, os autores afirmam que é possível "inovar" os demais direitos consagrados na Lei Geral de Proteção de Dados (LGPD), observando outros preceitos, inclusive, se aplicáveis, as normas do Código de Defesa do Consumidor (Lei 8078/90), do Código Civil, da Lei do Cadastro Positivo (Lei 12.414/2011), da Lei de Acesso à Informação (Lei 12.527/2011) ou qualquer outra legislação, inclusive tratados. Mesmo que, a princípio, essas normas tenham sido concebidas para relações no mundo analógico, elas podem ser aplicadas por analogia ao contexto digital, conforme estabelecido no art. 64 da LGPD[349].

Portanto, é possível afirmar que, embora a LGPD não tenha estabelecido limitações expressas à automatização do processo decisório e, consequentemente, autorizando explicitamente a decisão automatizada, também é correto sustentar que a decisão automatizada está sujeita aos requisitos estabelecidos para o tratamento de dados. A falta de observância desses requisitos configura uma irregularidade[350], podendo, em alguns casos, configurar uma ilicitude[351] se houver dano ou violação de qualquer um dos direitos conferidos ao titular dos dados pessoais, incluindo o direito de revisão e explicação dos dados pessoais considerados na tomada de decisão automatizada ou no perfilamento[352].

Ao analisar o procedimento estabelecido no artigo 20 da LGPD, percebe-se uma ampliação das questões discutíveis no âmbito do processo informacional nele estabelecido.

---

[348] Constituição Federal, art. 5º: "XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;"

[349] REIS; FURTADO, 2022. Em relação ao art. 64 da LGPD mencionado pelos autores: "Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte."

[350] Preceitua a LGPD: "O tratamento de dados pessoais realizados será irregular, quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano".

[351] A violação de direitos de outrem, do qual decorra dano, configura ato ilícito, conforme prescreve o Código Civil: "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."

[352] O qual, como dito, não se restringem aos de revisão (*i.e.*, de não se sujeitar a uma decisão totalmente automatizada) e de explicação, entendido como obter informações claras e adequadas quanto aos critérios e procedimentos adotados na decisão automatizada, o que inclui a relacionada à formação de perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (normalmente, inserida como "dados de entrada", ou nela utilizada, à guisa de preditores).

Nesse ponto, destaca-se que qualquer tomada de decisão (ou avaliação, ou criação de perfis) amparada no tratamento de dados pessoais, que afete potencialmente ou concretamente os interesses do titular dos dados, está teoricamente contemplada nesse procedimento instrumentalizador do processo informacional.

Resumindo, embora não se analisem profundamente as situações de ilicitude e irregularidade resultantes da violação das regras e princípios aplicáveis ao tratamento de dados pessoais, neste tópico fica claro que a existência dessas proibições normativas limita a permissão geral para decisões automatizadas. Fora desses limites, tais decisões serão consideradas proibidas, pois violariam a regulação de proteção de dados (LGPD). Além disso, o sistema jurídico, em princípio, não protege atos ilícitos nem atos praticados de forma irregular[353].

5.4 PROCESSO TECNOLÓGICO E PROCESSO INFORMACIONAL

O reconhecimento da existência de um devido processo "tecnológico" sinaliza a pressuposição de que vários interesses legítimos estão em jogo e é nesse quadro que situamos a proposição de autores nacionais, como Bruno BIONI (2019), quanto à aplicabilidade, ao cenário em questão, de um devido processo informacional, não restrito à aplicação limitada de privacidade, mas com o propósito de assegurar justa simetria entre os indivíduos de uma sociedade[354].

A partir dessa digressão, é de se salientar que as decisões automatizadas gradativamente ganham espaço no cotidiano da sociedade, e o reconhecimento do fenômeno revela-se tanto na percepção da presença dos algoritmos e sistemas de IA na vida dos indivíduos, como dos seus

[353] A guisa de ilustração, embora não se analise o ato em si, tampouco o objeto de direito passível de afastamento da tutela (o segredo de negócios, por hipótese), anota-se a classificação sugerida por Braga Neto (2010, p. 175 et.seq.), em relação à eficácia do ato ilícito: "ilícito indenizante: é todo ato ilícito cujo efeito é o dever de indenizar. Não importa o ato que está como pressuposto normativo. Se o efeito é reparar, *in natura* ou *in pecunia*, o ato ilícito praticado, estaremos diante de um ilícito indenizante; ilícito caducificante: é todo ato ilícito cujo efeito é a perda de um direito. Também aqui não importa os dados de fatos aos quais o legislador imputou tal eficácia. Importa, para os termos presentes, que se tenha a perda de um direito como efeito de um ato ilícito. Sendo assim teremos o ilícito caducificante (...)".
[354] BIONI; MARTINS, 2020.

significativos impactos, muito deles aptos a gerar insegurança e desconfiança em relação ao devido respeito neles contemplados aos direitos e liberdades estabelecidos no Ordenamento.

Ademais, a maior presença das decisões automatizadas no cotidiano, acompanhada de pouca transparência no tocante ao seu funcionamento, potencializam a complexidade do trabalho de identificação de práticas abusivas, discriminatórias ou, ainda, monopolísticas, que podem causar impactos tanto individuais quanto coletivos.

Acredita-se que a simetria desempenharia um papel protetor nesse aspecto. Além dos direitos individuais relacionados à proteção de dados pessoais, há também o interesse coletivo no uso da tecnologia como um todo. A confiança em suas várias aplicações deve ser preservada, embora não se possa descartar a possibilidade de que em alguns setores seu uso seja proibido ou restrito desde o início.

Nesse sentido convergem as preocupações em torno dos potenciais riscos imanentes ao desenvolvimento de uma IA de propósito geral[355], conforme se viu em seções anteriores (.v. seção 3.1)

Aparentemente corroborando com tal ideia, Renato Leite MONTEIRO (2021) destaca que a economia digital se baseia na confiança, um fato reconhecido tanto em instâncias nacionais quanto internacionais. Exemplos disso são a decisão da Corte Constitucional alemã sobre a Lei do Recenseamento (*Vokszahlungesetzt*) de 1983 e o *Affaire Safari*, que resultou na Lei de Informática de Liberdades francesa em 1978, além das diretrizes da OCDE sobre o tratamento de dados pessoais[356].

Seguindo esse contexto histórico de debate, o autor argumenta que a Lei Geral de Proteção de Dados (LGPD) possui um caráter abrangente, uma vez que, ao enfatizar a proteção do direito à personalidade (art. 1º), também considera a inovação econômico-tecnológica (art. 2º) como seu fundamento.

Com base em interpretação do art. 20 da LGPD, o autor referenciado argumenta que, no bojo do denominado Direito à Explicação, o dispositivo em específico oferece um direito amplo

[355] Em relação à inteligência artificial de propósito geral, autoaprimorável, a humanidade pode se encontrar em uma condição de inferioridade semelhante à dos animais em relação aos humanos. Alguns cientistas e tecnólogos importantes (como Stephen Hawking, Elon Musk e Bill Gates) defenderam a necessidade de antecipar esse risco existencial (PARKIN, 2015 *apud* SARTOR; LAGIOIA, 2020, p. 5)
[356] MONTEIRO, 2021, pp. 91-92.

ao devido processo informacional mediante o qual se assegura a simetria entre os titulares de dados e os processadores[357].

Essa correção da assimetria também poderia ser aplicada à regulação da União Europeia (RGPD). No entanto, uma análise realizada por SARTOR e LAGIOIA (2020) indica que são necessários esforços interpretativos na aplicação do RGPD, pois segundo esses autores, ele é ambíguo e insuficientemente claro na solução do problema da assimetria informacional em desfavor do titular dos dados, especialmente em relação ao consentimento e ao direito à explicação.

Ainda no entendimento desses autores, a prerrogativa de mínima compreensibilidade — presente no direito de explicação — poderá permanecer subutilizada pelos titulares dos dados, uma vez que estes podem não ter um conhecimento suficiente para mínima compreensão das tecnologias e dos padrões normativos aplicáveis.

Ademais, sublinham, mesmo quando a explicação venha a sinalizar potenciais "defeitos" (v.g., mau funcionamento e aplicações inadequadas de IA e tecnologias de *big data*) na tomada de decisão automatizada, poderá ocorrer que os titulares dos dados não consigam obter uma nova decisão mais satisfatória[358].

Todavia, em posicionamento conciliatório, SARTOR e LAGIOIA (2020) sustentam que embora o GDPR seja pródigo em cláusulas vagas e padrões abertos - inclusive no que dizem

---

[357] Idem.

[358] "(…) *we should be cautioned against over emphasising a right to individualised explanations as a general remedy to the biases, malfunctions, and inappropriate applications of AI and big data technologies. A parallel may be drawn between consent and individualised explanation, as both rely on the data subject's informed initiative. It has often been observed that consent provides no effective protection, given the disparity in knowledge and power between controllers and data subjects, and also the limited time and energy available to the latter, and their inability to pool their interests and resources and coordinate their activities. The same may also apply to the right to an explanation, which is likely to remain underused by the data subjects, given that they may lack a sufficient understanding of technologies and applicable normative standards. Moreover, even when an explanation elicits potential defects, the data subjects may be unable to obtain a new, more satisfactory decision*". Em trad. Livre: Devemos ser cautelosos em enfatizar demais um direito a explicações individualizadas como um remédio geral para os vieses, falhas e aplicações inadequadas de tecnologias de IA e big data. Pode-se estabelecer um paralelo entre consentimento e explicação individualizada, pois ambos dependem da iniciativa informada do sujeito de dados. Frequentemente, observa-se que o consentimento não oferece uma proteção efetiva, dada a disparidade de conhecimento e poder entre controladores e sujeitos de dados, bem como o tempo e energia limitados disponíveis para estes últimos, e sua incapacidade de reunir seus interesses e recursos e coordenar suas atividades. O mesmo pode ser aplicado ao direito a uma explicação, que provavelmente continuará sendo subutilizado pelos sujeitos de dados, pois eles podem não possuir uma compreensão suficiente das tecnologias e padrões normativos aplicáveis. Além disso, mesmo quando uma explicação revela possíveis defeitos, os sujeitos de dados podem ser incapazes de obter uma nova decisão mais satisfatória". (SARTOR, LAGIOIA, 2021).

respeito às questões aqui abordadas[359] -, em muitos casos, muitas vezes é necessário interpretar esses padrões indefinidos do RGPD de acordo com o equilíbrio entre os vários interesses envolvidos.

Segundo os autores, na avaliação desses interesses, deve-se considerar as justificativas ou interesses relacionados a uma determinada atividade de processamento, juntamente com as medidas adotadas em relação a ela. Em outras palavras, é necessário ponderar se os interesses do controlador em processar os dados e adotar certas medidas são ou não superados pelos interesses dos titulares dos dados em não serem sujeitos ao processamento ou em serem protegidos por medidas preventivas, adicionais ou mais rigorosas[360].

De qualquer sorte, é preciso prosseguir e, nesse caminhar, tem-se o entendimento de FRAZÃO, CARVALHO e MILANEZ (2022)[361], para quem — como já sinalizado em seção anterior — o direito de revisão e explicação a que alude o artigo 20 da LGPD tem evidentes conexões com as garantias constitucionais do contraditório e do devido processo legal, garantias essas que, ao entendimento desses autores, aplicam-se, na medida do possível, às relações privadas.

Isso implica dizer que, no bojo do devido processo, as garantias constitucionais são atendidas quando são asseguradas às partes interessadas a defesa de um ato por elas consideradas de direito. Nessa perspectiva, os autores asseveram:

> O problema agrava-se pelo fato de que as decisões algorítmicas são caracterizadas por grande opacidade, sendo verdadeiras caixas pretas, sem transparência ou accountability. Dessa maneira, nada assegura que decisões totalmente automatizadas possam ter a objetividade que delas se espera; na verdade, tais decisões podem ser bastante enviesadas e ainda refletirem diversos tipos de preconceitos. Se o processo de impugnação e revisão das decisões algorítmicas não for capaz de contornar essas

[359] Menciona os seguintes: a identificabilidade do titular dos dados (artigo 4.º, n.º 1), a liberdade de consentimento (artigo 4.º, n.º 11), a compatibilidade do tratamento posterior com o original (artigo 5.º, n.º 1, alínea c), a necessidade dos dados relativamente à sua finalidade (artigo 5.º, n.º 1, alínea c), a legitimidade dos interesses do responsável pelo tratamento e a sua importância não preponderante (artigo 6.º, n.º 1, f), a pertinência da informação sobre a lógica envolvida na tomada de decisão automatizada (artigos 13.º, n.º 2, alínea f) e 14.º, n.º 2, alínea g), a adequação das medidas de salvaguarda a adoptar para a tomada de decisão automatizada (artigo 22.º, n.º 2), e a adequação das medidas técnicas e organizativas para a proteção de dados desde a concepção e por defeito (artigo 25.º).

[360] No original: "*In various cases, the interpretation of undefined GDPR standards requires balancing competing interests: it requires determination of whether a certain processing activity, and the measures adopted are justified on balance, i.e., whether the controller's interests in processing the data and in (not) adopting certain measures are outweighed by the data subjects' interests in not being subject to the processing or in being protected by additional or stricter measures*." (SARTOR; LAGIOIA, 2020, p. 86). Para além dessas considerações, os autores parecem preconizar que esse posicionamento está alinhado com a estratégia da União Europeia no enfretamento do desafio de desenvolver uma IA centrada no ser humano, em conformidade com entendimentos refletidos no Livro Branco da Comissão Europeia. (PARLAMENTO EUROPEU, 2020, pp. 7-8; 76 e ss.)

[361] FRAZÃO; CARVALHO; MILANEZ, 2022, p. 334.

> dificuldades, certamente que não será idôneo para resguardar os direitos dos titulares de dados". [362]

Renato Leite MONTEIRO (2021), em sua tese de doutorado na Faculdade de Direito da USP, defende uma proposição semelhante. Ele afirma que garantir apenas o acesso aos dados e informações que serviram de base para a tomada de decisão não é suficiente para compreender como o processo funciona e como esses elementos são valorizados, articulados e utilizados na tomada de decisões automatizadas. Portanto, é necessário garantir que o titular compreenda como uma decisão automatizada específica foi alcançada, além de fornecer acesso aos elementos (dados e informações) que embasaram a decisão. Do ponto de vista do devido processo legal, o direito do titular de compreender as razões, os fundamentos e o raciocínio por trás de uma decisão que o afeta é essencial. Isso é garantido, por exemplo, por meio dos deveres atribuídos ao juiz de motivar explicitamente sua decisão judicial, informando quais provas e argumentos foram aceitos, como eles foram avaliados, os motivos pelos quais outros argumentos e provas não foram aceitos e a lógica que levou à decisão. No contexto do devido processo legal, a compreensão estaria intimamente relacionada ao requisito de motivação das decisões judiciais[363].

De um lado, parece evidente, portanto, que a LGPD proporciona ao controlador oportunidade para apresentar objeções factuais e jurídicas às requisições de informações apresentadas pelo titular de dados, inclusive relacionadas com o segredo de negócios, se aplicável (LGPD: Art. 18, §4, incisos I e II e Art. 20, §2º).

De outra parte, sob a perspectiva do titular, sem dúvida, a lei lhe assegura, dentre outros direitos e garantias[364], as seguintes prerrogativas: **(a)** a confirmação da existência de tratamento de dados pessoais (Art. 18-I); **(b**) de acesso aos dados pessoais (Art. 18-II); **(c)** de correção de

---

[362] FRAZÃO; CARVALHO; MILANEZ, 2022, pp. 588-589.
[363] MONTEIRO, 2021.
[364] Naturalmente, a correção da notória assimetria informacional, imanente no ecossistema digital, em desfavor do indivíduo, para além da estrutura normativa da LGPD, deverá ser objeto de consideração por parte da autoridade reguladora/fiscalizadora (ANPD) por ocasião da edição de normas regulamentadoras, sendo certo que, em princípio, caberá ao controlador – ou agente de tratamento, por hipótese detentor do segredo de negócios – o ônus da prova no tocante às suas objeções às requisições de informações estabelecidas em benefício do titular dos dados. Também não ignora que o titular poderá postular suas pretensões nas esferas administrativas (por petição dirigida à autoridade nacional ou órgãos de proteção do consumidor) ou judiciais. LGPD, art. 18, § 1º e § 8º, art. 22 e art. 64): "Art. 18. (...) § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. (...) § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor"; "Art. 22. 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."; "Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.".

dados pessoais incompletos, inexatos ou desatualizados (Art. 18-III); (**d**) de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (Art.18 -IV); **(e) d**e revogação do consentimento ou eliminação de dados tratados sem o seu consentimento (Art. 18,-IX e VI); **(f)** de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os seus interesses (Art. 20 caput); **(g)** de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos de negócio (Art. 20 §1º).

Com efeito, segundo FRAZÃO et al. (2022)[365] o artigo 20 da LGPD não só estabelece o devido processo em face dos efeitos das decisões automatizadas, como também viabiliza a tutela (proteção) de um bloco de direitos, nos quais se vê incluído, para além do direito de oposição (já objeto de exame no item 5.2.1, retro), o direito de revisão e o de explicação propriamente ditos.

Portanto, neste ponto, nosso entendimento alinha-se ao das doutrinas referenciadas, sobretudo quanto à dimensão procedimental dos direitos do titular, previstos no Capítulo III da LGPD. Com base nesses direitos, podemos observar com certa clareza que a LGPD, ao estabelecer o procedimento descrito nos artigos 18 e 20, busca garantir uma abordagem equilibrada para todas as partes, contribuindo para a materialização dos princípios do contraditório e da ampla defesa no contexto do processamento de dados pessoais.

5.4.1 A questão da revisão humana

As indicações de falta de consenso no tocante à obrigatoriedade da participação humana[366] no processo de revisão e de explicação na tomada de decisões automatizadas

[365] "É no contexto dos desafios inerentes à nova economia que o art. 20 da LGPD pretende criar uma espécie de devido processo legal para proteger os cidadãos contra a 'tirania' dos julgamentos automatizados. Para tal fim, foi criado um verdadeiro bloco de direitos, cujos principais desdobramentos são os seguintes: 1. O direito de acesso e informação em relação a respeito dos critérios e procedimentos utilizados para a decisão automatizada; 2. O direito de oposição quanto à decisão automatizada e de manifestar o seu ponto de vista; 3. O direito de obtenção da revisão da decisão automatizada; e 4. O direito de petição à autoridade nacional para a realização de auditoria, em caso da não prestação das informações. Como se pode observar, tais direitos decorrem não apenas da autodeterminação informativa do cidadão e do controle que a lei lhe atribui sobre os seus dados pessoais, mas também de importantes princípios." (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 598).

[366] "O texto inicialmente aprovado em 2018 trazia a previsão do direito do titular dos dados de solicitar revisão de decisões automatizadas (tomadas unicamente com base em tratamento automatizado), *por pessoa natural*, todavia, tal previsão foi excluída pelo Presidente da República por intermédio da Medida Provisória 869/2018. Seguiu-se o procedimento de aprovação da medida provisória e sua conversão em lei e o Congresso emendou o artigo para incluir o § 3º, para novamente estabelecer que a revisão mencionada no *caput do* art. *20* deveria ser realizada por *pessoa natural*, o que restou vetado em sanção presidencial da nova lei (Lei 13.853/2019)". (MONTEIRO, 2021, p. 188) Entretanto, a discussão pública em torno da supervisão humana nos processos decisórios automatizados segue seu curso agora no bojo do Projeto de Lei que pretende dispor sobre o uso e

revelam não só a complexidade das questões relacionadas com o uso de aplicações de IA nas tomadas de decisões cotidianas como também sinaliza a magnitude dos impactos dessas decisões nas vidas dos indivíduos por elas afetados.

Este estudo considera o contexto europeu (RGPD), que também enfrenta polêmicas semelhantes. No entanto, nesse caso, não parecem existir dúvidas relevantes sobre a existência de um regime que protege o indivíduo e garante a explicação das decisões automatizadas.

Ao examinar o debate em torno do RGPD, SARTOR e LAGIOIA (2020) asseveram que a questão quanto à obrigatoriedade ou não de intervenção humana na tomada de decisão automatizada tem origem na ambiguidade do artigo 22, que estabelece salvaguardas mínimas aplicáveis visando assegurar o direito do titular de "expressar seu ponto de vista e o de contestar a decisão", porém omite-se no tocante à obrigatoriedade de que tais informações sejam "específicas", com isso parecendo pretender excluir a obrigação legal do controlador de prestar explicações individuais, abrindo margem a dúvidas no tocante à previsão do "Considerando 71")[367].

Na visão dos autores referenciados, é possível interpretar que o legislador europeu pretendia não onerar indevidamente os controladores, ao utilizar no texto normativo as expressões vagas como "pelo menos", possivelmente pressupondo que "uma explicação seria legalmente requerida, sempre que viável, ou seja, sempre que for compatível com tecnologias,

---

desenvolvimento da Inteligência Artificial no País. Vide proposição de texto do respectivo artigo 3º: "*Art.* 3º *O desenvolvimento, implementação e uso de sistemas de inteligência artificial observarão a boa-fé e os seguintes princípios: I- crescimento inclusivo, desenvolvimento sustentável e bem-estar; II- autodeterminação e liberdade de decisão e de escolha; III* ***participação humana no ciclo da inteligência artificial e supervisão humana efetiva****; IV- não discriminação; V - justiça, equidade e inclusão; VI - transparência, explicabilidade, inteligibilidade e auditabilidade; VI - confiabilidade e robustez dos sistemas de inteligência artificial e segurança da informação; VII - devido processo legal, contestabilidade e contraditório; VIII - rastreabilidade das decisões durante o ciclo de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica; IX - prestação de contas, responsabilização e reparação integral de danos; X - prevenção, precaução e mitigação de riscos sistêmicos derivados de usos intencionais ou não intencionais e efeitos não previstos de sistemas de inteligência artificial; e XI não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas dos sistemas de inteligência artificial*." (g.n.)

[367] O Artigo 22(3) do GDPR estabelece a seguinte Medidas de salvaguarda: "*Nos casos previstos no artigo 22.º, n.º 2, alíneas a) e c) – ou seja, quando a decisão automatizada é necessária para contratar ou expressamente consentida – o artigo 22.º, n.º 3, exige medidas de salvaguarda adequadas: o responsável pelo tratamento deve implementar as medidas adequadas para salvaguardar os direitos e liberdades e interesses legítimos do titular dos dados, pelo menos o direito de obter intervenção humana por parte do responsável pelo tratamento, de expressar o seu ponto de vista e de contestar a decisão*." De acordo com o Grupo de Trabalho do Artigo 29, algumas dessas medidas dizem respeito à redução de riscos. Exemplos são verificações de garantia de qualidade, auditoria algorítmica, minimização de dados e anonimização ou pseudonimização e mecanismos de certificação. Essas medidas devem garantir que os requisitos estabelecidos no Considerando (71) – no que diz respeito à aceitabilidade, precisão e confiabilidade – são respeitados. (SARTOR; LAGIOIA, 2020, p. 61)

custos e práticas de negócios". Em suma, no entendimento desses autores, o legislador europeu enfrentava dúvidas no tocante a se as explicações individualizadas deveriam ser transformadas em uma exigência legal.

De qualquer modo, afirmam os autores que do ponto de vista prático essa incongruência não é considerada significativa, uma vez que a obrigação de prestação de informação já estaria prevista nos artigos 13.º, 14.º e 15.º do RGPD.

Além disso, segundo esses especialistas, alguns comentaristas sugerem que a visão de que os titulares dos dados têm direito a explicações individualizadas sob o RGPD poderia eventualmente ser estabelecida pelas autoridades de proteção ou pelos tribunais, uma vez que a efetiva explicação individualizada pode ser uma condição prévia para permitir que os titulares dos dados contestem efetivamente as decisões automatizadas (Sartor, Lagioia, 2020, p. 61 et seq.)[368].

Sob a perspectiva do Ordenamento, FRAZÃO, CARVALHO e MILANEZ (2022) avaliam que o texto do artigo 20 da LGPD precisa ser interpretado à luz da Constituição Federal, como também em coerência com os princípios da LGPD, de modo que haveria bons fundamentos para se exigir a presença da pessoa natural, mesmo que a lei seja omissa no tocante à expressa "obrigatoriedade" de intervenção humana nas decisões automatizadas.[369]

5.4.2 Auditoria e medidas preventivas, em razão do risco da atividade

A literatura (v.g., MULHOLLAND, FRAJHOF , 2019, p. 272)[370] salienta a falta de clareza no âmbito da regulação brasileira a respeito da realização de auditorias e medidas preventivas em razão do risco da atividade.

Autores como FREIRE DE SÀ e MACENA DE LIMA (2021)[371] sustentam que caberá à autoridade nacional (LGPD artigos 55-A a 55-L) a tarefa de suprir as incertezas e lacunas presentes na regulação, inclusive no que se refere à possível discricionariedade na realização de auditoria para fins de verificação de aspectos discriminatórios no tratamento automatizado de dados pessoais (Artigo 20§2º).

---

[368] SARTOR; LAGIOIA, 2020, p. 61 *et* seq.
[369] FRAZÃO; CARVALHO; MILANEZ, 2022, p. 597.
[370] MULHOLLAND; FRAJHOF *apud* FRAZÃO; MULHOLLAND, 2019. p. 272.
[371] SÁ; LIMA, 2021, p. 227.

SOUSA, PERRONE e MAGRANI (2021, p. 267)[372] vão além, opinando no sentido de que a auditoria dos mecanismos de tratamento de dados automatizados situa-se no plano da competência da autoridade de proteção de dados, não se figurando propriamente num direito individual, uma vez que, para além da proteção dos direitos individuais[373], o escopo protetivo da auditoria atinge dimensões mais amplas de direitos, como direitos coletivos ou direitos individuais homogêneos.

Nesse sentido, com apoio em KAMINSKI (2018, p.25)[374] , explicam que tanto a LGPD quanto o GDPR possuem essa dimensão sistêmica de proteção, mediante disposições (LGPD: Art. 6º VIII)[375] que indicam que os controladores devem por iniciativa própria "adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais", o que inclui — a depender das circunstâncias — a realização de estudos de impacto e alguma forma de auditoria e análise.

Ao se referir à competência da autoridade de proteção, os autores também destacam o dever de zelar pela proteção de dados por meio de mecanismos de controle e fiscalização, dentre as quais, portanto, a de realizar auditorias[376].

No que concerne à realização de estudos de impactos, a sinalização do artigo 38 da LGPD[377] não oferece clareza no tocante ao nível de obrigatoriedade atribuída aos controladores

---

[372] SOUZA; PERONE; MAGRANI *apud* DONEDA *et al.*, 2021, p. 267.

[373] Naturalmente, no espírito do devido processo, parece sustentável que, embora situe-se no âmbito da competência da autoridade de proteção de dados que poderia de oficio determinar a realização da auditoria, nada indica que tal diligência não possa ser requerida pela parte interessada (na medida em que se afigurar necessário tal meio de prova, na hipótese de afetada em seus direitos ou interesses por uma decisão automatizada, a partir do tratamento de dados pessoais de sua titularidade).

[374] Segundo os autores, Margot Kaminski "dá a dimensão sistêmica da transparência como parte de um regime europeu de responsabilidade e prestação de contas em decisões automatizadas ('*accountability*')". (SOUZA; PERONE; MAGRANI *apud* DONEDA *et al.*, 2021, p. 267)

[375] LGPD: "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;"

[376] LGPD, art. 55-J, incluído pela Lei 13.853, de 2019: "Art. 55-J. Compete à ANPD: (...) 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; (...) 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".

[377] LGPD: "Art. 38. 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. 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."

em relação à referida medida, uma vez que o art. 4º §3º da LGPD[378] sugere que a exigência desse relatório depende da iniciativa da autoridade nacional[379].

Diante da dúvida, cumpre rememorar o alerta que faz DONEDA (2022.p.533)[380] no tocante à especial atenção que merece a atuação da autoridade de proteção dados, a considerar os moldes com que elas, em sua maioria foram instituídas.

Afinal, obtempera o Autor, a simples atuação do indivíduo na proteção de seus interesses — no âmbito do controle individual — não enseja a tutela adequada do direito fundamental assegurado no Ordenamento, diante "*da crescente complexidade dos mecanismos de tratamento de dados e a dificuldade em se estabelecer nexos causais entre este tratamento e os efeitos por ele causados à pessoa*" e mesmo pela potencialidade de excluir o indivíduo do acesso a serviços essenciais presentes estruturalmente na sociedade digital, caso decida resistir, no exercício de sua vontade autônoma[381].

[378] LGPD, art. 4º: "§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais."
[379] A regulação prescreve importantes vetores de governança e compliance, conforme se vê na LGPD, art. 50, § 2º, I, "d", no ponto em que se requer a adoção de políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade. Enfim, para além dos poderes-deveres atribuídos à autoridade parece induvidoso que as expectativas dos cidadãos em relação ao tratamento de seus dados é que os agentes de tratamento demonstrem esforços consistentes nesse sentido.
[380] DONEDA, 2021, pp. 333-334.
[381] *Idem.*

CAPÍTULO 6 – DIÁLOGO ENTRE A PROTEÇÃO DE DADOS, SEGREDO DE NEGÓCIO E A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL

Conforme já se observou, a interdisciplinaridade e a transversalidade[382] deste estudo emergem diretamente de disposições expressas na Lei Geral de Proteção de Dados (LGPD ou Lei 13.709/2018)[383] e na Lei de Propriedade Intelectual (LPI ou Lei 9.279/1996)[384].

A primeira assentando o tratamento de dados pessoais nos pilares da transparência e no respeito à autodeterminação informativa do indivíduo, salvaguardando, contudo, a observância do segredo de negócios, quando devido.

A segunda, ao proteger o segredo de negócios, sujeita a sua tutela ao interesse social e ao desenvolvimento econômico do País (BALMES, 2008).

Com isso, denota-se a necessidade desses diálogos transversais, com vistas à

---

[382] Esta seção tem por escopo integrar os três temas examinados individualmente em seções específicas deste trabalho (segredo de negócios, proteção de dados e IA).

[383] LGPD: "Art. 10. (...) § 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. (...)
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: (...) 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; [...] Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: (...) II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. (...)
§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento. [...] Art. 38. 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. (...)
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. (...) III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; [...] Art. 55-J. Compete à ANPD: (...) 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. 2.º desta Lei; (...) X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial."

[384] Lei nº 9279, de 1996: "Art. 2º A proteção dos direitos relativos à propriedade industrial, considerado o seu interesse social e o desenvolvimento tecnológico e econômico do País, efetua-se mediante (...)"
"Art. 206. Na hipótese de serem reveladas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, sejam segredo de indústria ou de comércio, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades."

compatibilização entre uma e outra proteção.

Como demonstrado nas seções anteriores, em muitos casos, a proteção do segredo de negócios pode ser usada como justificativa para não fornecer informações importantes e necessárias para garantir a transparência e explicabilidade das decisões tomadas por sistemas automatizados, especialmente aqueles que utilizam técnicas de IA. Essa proteção do segredo de negócios pode levantar questionamentos sobre sua compatibilidade com as leis gerais de proteção de dados pessoais, pois pode impedir que as pessoas entendam por que e como uma decisão foi tomada.

A falta de definição regulatória nesse contexto pode abalar a previsibilidade e a estabilidade do mercado, pois uma regulamentação voltada para o uso da IA busca afastar a falta de confiança gerada pelos efeitos negativos que ela pode ter na sociedade como um todo[385].

No âmbito doutrinário, é relevante mencionar os estudos de Diana Liebenau (2016), citados por Carneiro e Almada (2019), que destacam possíveis conexões entre as teorias de proteção de dados pessoais e propriedade intelectual, especificamente as três teorias de privacidade: controle, acesso limitado e integridade contextual. Essas teorias analisam a distribuição e o controle da informação, o papel social da privacidade e a importância do contexto em que a informação é utilizada.

Giulia Schneider (2017, p. 227 et. Seq.), também mencionada por Carneiro e Almada (2019), discute a evolução gradual dos papéis da propriedade intelectual e da proteção de dados, especialmente no contexto da União Europeia. Segundo Schneider, as leis de proteção de dados, como o GDPR, ampliaram os deveres de transparência das empresas em relação à geração e processamento de dados pessoais, afastando-se do tradicional controle e restrição de acesso presentes nesses domínios.

Essas visões sugerem um movimento contrário ao papel central da propriedade intelectual, em que o foco agora está no controle e sigilo de informações sensíveis, em vez da divulgação do conhecimento para obtenção de patentes. Empresas europeias priorizam os "segredos comerciais" em vez de patentes, devido aos custos vantajosos e ao enfoque na inovação (CARNEIRO e ALMADA, 2019).

[385] Em relação à imprescindibilidade do fator confiança no âmbito do mercado, v. CAIRU (1874) *apud* FORGIONI, 2005, nota 8.

Com esse pano de fundo, esta seção explora as discussões internacionais sobre o equilíbrio entre a proteção dos segredos comerciais e a privacidade dos dados pessoais, com base na experiência europeia com a implementação do GDPR, que pode ser comparada à LGPD no Brasil. Também se destaca a harmonização da estratégia brasileira com os padrões mundiais para o desenvolvimento de uma IA robusta, transparente e confiável. Analisando essas perspectivas regulatórias, busca-se explorar o debate público em torno da criação de uma legislação sobre IA no País, que tem como objetivo promover a confiança no fluxo de informações por meio do uso responsável e ético dessas novas tecnologias. Na sequência, examinam-se os respectivos lugares comuns que por hipótese sinalizem as possibilidades de interações equilibradas e "dialógicas" entre as proteções jurídicas em estudo, por hipótese viabilizadas pela garantia de transparência e explicabilidade das decisões automatizadas.

6.1 SEGREDO DE NEGÓCIOS VS. PROTEÇÃO DOS DADOS PESSOAIS: EM BUSCA DO EQUILÍBRIO

Em referência à Diretiva dos segredos comerciais no âmbito da União Europeia, Francesco Banterle (2016) [386] explica que em diferentes países da União Europeia existem regimes variados de proteção jurídica para os segredos comerciais. Cada Estado-Membro tem a prerrogativa de adotar diferentes modelos de proteção, resultando em uma diversidade de níveis de proteção.

O autor destaca que na Suécia, os segredos comerciais são regulamentados por legislação específica, enquanto na Itália e Portugal são considerados tipos de direitos de propriedade intelectual. Na França, a proteção é apenas parcial, enquanto na Áustria, Alemanha, Polônia e Espanha baseia-se em leis de concorrência desleal. Na Holanda e Luxemburgo, a regulação é feita com base na lei de responsabilidade civil, enquanto no Reino Unido, Irlanda e Malta prevalece o regime de quebra de confiança.

A virtual "dependência" do direito contratual e a abordagem de propriedade estaria presente na maioria dos respectivos Estados-Membros.

[386] BANTERLE, 2016.

Entretanto, ao que se vê, o objetivo da Diretiva foi buscar uma harmonização parcial mediante definição de um padrão mínimo de proteção, reservando aos Estados-Membros autonomia para estabelecerem a proteção de forma mais abrangente, segundo suas leis nacionais, não visando instituir um regime de segredos comerciais no âmbito da EU (Banterle, 2016).

No entanto, parece que a Diretiva dos segredos comerciais (Diretiva EU 2016/943) não conseguiu atingir seu objetivo de harmonização normativa, especialmente porque o Regulamento Geral de Proteção de Dados Pessoais (UE 2016/679) agora levanta a questão sobre a prevalência dos direitos de segredo comercial em relação à proteção de dados pessoais.

Em que pese a aparente confusão, os mecanismos da RGPD apontam por uma solução caso a caso, a cargo de uma autoridade nacional de proteção de dados em cuja competência estaria o cumprimento da linha regulatória no sentido de que "se o direito de acesso afetar negativamente os segredos comerciais, esse direito pode ser reduzido, porém nunca totalmente negado". Nesse sentido é a diretriz explicitamente enunciada no "considerando 41" da Diretiva 95/46/CE e confirmada no "Considerando nº 63 do Regulamento Geral de Proteção de Dados Pessoais (U.E) 943/2016/RGPD) [387].

6.1.1 A extensão do conceito de dados pessoais e os limites da tutela do segredo de negócios: uma zona cinzenta

A discussão parece centrar-se no conceito "expansionista" de informações comerciais sugerida pela Diretiva dos Segredos Comerciais, em contraste com a mesma indeterminação conferida em relação aos dados pessoais.

[387] O Considerando 41, da Diretiva 95/46 foi contemplado no Considerando 63 do Regulamento (U.E) 946/2016: "Os titulares de dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude. Aqui se inclui o seu direito de acederem a dados sobre a sua saúde, por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados. Por conseguinte, cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências. Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. Esse direito não deverá prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software. Todavia, essas considerações não deverão resultar na recusa de prestação de todas as informações ao titular dos dados. Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido". (g.n.)

Embora não objeto de definição especificamente relacionada com "informações comerciais", a diretiva esclarece que o escopo da proteção de segredos comerciais refere-se a 'dados comerciais' como informações - e nelas inclui os planos de negócios, pesquisas e estratégias de mercado e informações sobre clientes e fornecedores. Isso pode causar controvérsia, pois parece haver uma sobreposição com o conceito de dados pessoais delineado no Regulamento Geral de Proteção de Dados (RGPD).

Por um lado, a doutrina, como a defendida por SOUSA e SILVA (2014) , relaciona o conceito de “Informações” adotado na Diretiva de Segredos com os “dados organizados”. Por outro lado, também reconhece que a definição oferecida na Diretiva de Segredos Comerciais é explícita em incluir as listas de clientes no conceito de informações protegidas e confidenciais. Isso implicaria proteção para os conjuntos de dados internos contendo “dados de pesquisa” e consequentemente não seria viável distingui-los daquelas informações que possam relacionar/incluir/referir a dados pessoais[388], presente na definição de dados pessoais.

Nesta perspectiva de conceito “estendido” de informações comerciais, é possível cobrir quase todos os tipos de dados comerciais, inclusive os dados pessoais de clientes ou não clientes (SOUSA e SILVA, 2014).

Uma linha de debate diz respeito à viabilidade de as normas de proteção de dados pessoais terem sido incorporadas no âmbito da diretiva dos segredos comerciais. Nesse aspecto, dado que a Diretiva dos Segredos Comerciais tende a atribuir controle sobre os dados pessoais ao detentor ou controlador e não necessariamente ao respectivo titular (pessoa natural), surge a opinião de Francesco Banterle (2016) [389] sobre a possível inclusão da proteção de dados pessoais na Diretiva dos Segredos Comerciais.

Gianclaudio Malgieri (2016, p. 102-116) argumenta que a discussão certamente tomaria um rumo diferente se considerássemos sua opinião[390] de que, se apenas dados específicos do cliente forem divulgados sem outras informações, como avaliação do agente sobre o cliente e alternativas de marketing de negócios, seria uma questão técnica e não jurídica. Se for tecnicamente viável "descontextualizar" (separar dados pessoais e segredos comerciais), então

[388] Cf. Banterle (2016), tais menções constam expressamente no Anexo 21 do Relatório de Impacto da Diretiva de Segredo Comerciais.
[389] BANTERLE, 2016.
[390] MALGIERI, 2016, pp. 102–116.

não seria razoável afirmar que o acesso aos dados pessoais afetaria negativamente o segredo comercial[391].

Ao analisar a questão à luz da LGPD (Art. 18 e Art. 44), parece razoável concluir que em termos práticos é responsabilidade do "controlador" (possível detentor dos segredos de negócios) garantir a segurança e integridade dos dados pessoais objetos de tratamento, em benefício do titular respectivo. Trata-se, aparentemente, de uma possível confusão semântica.

Em todo caso, com o objetivo de enriquecer o debate, é relevante mencionar a diversidade de "visões políticas" adotadas pelos Estados-membros da União Europeia, o que pode indicar uma sobreposição conceitual em relação ao objeto protegido em ambas as regulamentações de proteção.

Com base em Gianclaudio MALGIERI[392], observa-se que a inclusão do artigo 24 na lei italiana 196/2003[393] foi justificada pela busca de equilíbrio entre o direito à privacidade e o direito de acesso a informações "específicas". Segundo a lei italiana, o consentimento do titular dos dados pode ser dispensado em situações em que outro interesse, como o processamento para fins comerciais, deve prevalecer sobre a proteção de dados. Essa disposição também considerou o direito de oposição do titular de dados, previsto no artigo 14(a) da Diretiva (UE) 95/46, incorporado na legislação italiana. No entanto, a ideia predominante era reduzir os conflitos entre os titulares e os responsáveis pelo tratamento, com a suposição de que os primeiros não exerceriam seus direitos de proteção de dados se não tivessem conhecimento do tratamento. A lei também ressaltou a necessidade de que o processamento desses dados ocorra de acordo com a legislação de segredo comercial e industrial.

A proteção de dados no Reino Unido e na Irlanda foi menos permissiva em relação à lei italiana. De acordo com Gianclaudio MALGIERI (2016) [394], a Lei de Proteção de Dados de 1998 no Reino Unido previa que mesmo que o titular tivesse o direito de ser informado pela controladora de dados sobre a lógica envolvida na tomada de decisão automatizada, essa solicitação poderia não ser atendida se a informação fosse um segredo comercial. Na Irlanda, a

[391] Entende-se aqui que o autor denomina que "descontextualização" corresponda a uma operação de filtragem ou clivagem de dados.
[392] "*Art. 24 (Casi nei quali puo` essere effettuato il trattamento senza consenso) Il consenso non e` richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:* (...) *d) riguarda dati relativi allo svolgimento di attivita` economiche, trattati nel rispetto della vigente normativa in material di segreto aziendale e industriale*.". (MALGIERI, 2016, pp. 102–116).
[393] A legislação em referência vigia em 2016, e já era alvo de críticas pelos estudiosos como Misserini.
[394] MALGIERI, 2016, pp. 102–116.

Seção 4(12) do "*Data Protection Act*" de 1988 (alterado em 2003) explicitamente enfatizou a desnecessidade de informar a lógica envolvida na tomada de decisão automatizada se isso afetasse adversamente os segredos comerciais ou a propriedade intelectual, especialmente no caso de computadores cujo design protegesse os direitos autorais de software.

MALGIERI também menciona a possibilidade de estender a proteção de dados para pessoas jurídicas[395]. Alguns estudiosos propuseram a expressão "*vie prive e des affaires*" para sugerir a definição de uma estrutura fragmentada de proteção da privacidade comercial[396]. Na Irlanda, porém, os estudiosos consideram que o direito constitucional à privacidade não se estende às entidades corporativas, sendo exclusivo para garantir a autonomia dos indivíduos, e não das entidades corporativas. Dessa forma, na Irlanda, o segredo comercial, baseado na tese da privacidade, não encontra respaldo no direito constitucional.

Além disso, a tese da proteção dos segredos comerciais, baseada na analogia da Quarta Emenda nos Estados Unidos[397], tem orientado diversos julgados da Suprema Corte norte-americana. De acordo com Malgieri (2016), o debate teórico está relacionado à viabilidade de proteger os segredos comerciais sob a proteção da "propriedade" e da personalidade, devido à confusão entre segredos comerciais, segredos econômicos e segredos de personalidade. Segundo o entendimento de Posner (1992), a analogia da Quarta Emenda poderia levar a um relaxamento das medidas tradicionais de proteção do sigilo, por acreditar-se que isso estaria tutelado pelo direito à privacidade. No entanto, nos EUA, o debate continua em aberto.

---

[395] *CA Limoges, 4 Mars 1988, Juris Data, n. 1988-040911*: "*os tribunais locais aceitaram uma espécie de 'vida privada «das pessoas colectivas: para além de algumas decisões vagas sobre a aceitabilidade da existência dos direitos das pessoas colectivas, a Cour d'Appel de Limoges em 1988 declarou que uma associação tinha uma« vida secreta »que devia ser protegida de cada forma de intrusão.Mais recentemente, o Cour d'Appel de Aix-en-Provence em 2001 reconheceu que as pessoas coletivas podem ser sujeitas a ataques na sua vida privada e que «as pessoas coletivas têm direitos, que não são iguais, mas são semelhantes aos direitos da personalidade, como o direito a um nome, o direito de manter em segredo sua vida interior, o direito à reputação, etc*." (MALGIERI, 2016).

[396] *Cour d'Appel Nimes, 13 July 2010, n. 07/05143; CA Rennes, 4 May 2010, n. 08/08588; CA Bordeaux, 9 December 2009, n. 08/02995; CA Pau, 19 January 2009, 07/01962. J-C Saint-Pau, Droit au respect de la vie prive´e, De´finition conceptuelle du droit subjectif, J.-Cl. Civil Code, Art. 9, Fasc. 10, n8 44: 'il; semble certain qu'une information d'entreprise (par exemple, une note de service) est une information prote´ge´e au titre du droit au respect de la vie prive´e'*. (MALGIERI, 2016)

[397] *Kewanee Oil Co. v Bicron Corp, 416 U.S. 470, 487 (1974).; Soldal v Cook County, 506 U.S. 56 (1992); Frank W. Winne & Son, Inc. v Palmer, 1991 U.S. Dist.; Tennant Co. v. Advance Mach. Co., 1984, Tennant Co. v Advance Mach. Co., 355 N.W.2d 720, 725 (Minn. Ct. App. 1984); PJ Courture, 'Independent Derivation and Reverse Engineering' in Trade Secret Protection and Litigation (PLI Patents, Copyrights, Trademarks & Literary Property Course Handbook Series No. 340, 1992)* (MALGIERI, 2016).

À semelhança com a Quarta Emenda (EUA), a Convenção Europeia de Direitos Humanos (Art. 8, 1) assegura que "todos tem direito ao respeito pela vida privada e familiar, pelo lar e pela correspondência"[398].

O Tribunal Europeu dos Direitos do Homem tem aceitado a tese; todavia resiste em lhe dar uma interpretação geral. Com base numa interpretação dinâmica da Convenção decidiu-se avaliar a questão "caso a caso" (a possibilidade de incluir o direito de respeitar a sede social de uma empresa, filiais ou instalações comerciais, com base no referido artigo 8º)[399]. Entretanto, é possível elencar afirmações do Tribunal e do próprio Tribunal de Justiça da União Europeia (TJUE), como as seguintes:

> (I) não haveria razões para excluir da noção de vida privada as atividades de natureza profissional ou empresarial, porque, é no curso de suas vidas profissionais que a maioria das pessoas teriam oportunidade significativa de desenvolver relações com o mundo exterior[400].
>
> (II) A noção de vida privada não pode ser entendida como significando que as atividades profissionais e comerciais de pessoas físicas ou jurídicas estão excluídas[401]

É evidente, portanto, que o debate, tanto na UE quanto nos EUA, gira em torno do princípio constitucional de "vida privada". A discussão ainda continua sobre se a atual legislação de proteção de dados (RGPD) protege explicitamente as empresas.

Nesse aspecto, não há dúvida de que a regulamentação de proteção de dados (tanto no âmbito da RGPD europeia quanto da LGPD brasileira) é direcionada à pessoa natural e não à pessoa jurídica[402]. Vale ressaltar que uma das interfaces entre as leis de proteção de dados pessoais (RGPD na União Europeia e LGPD no Brasil) e a proteção de segredos comerciais (Diretiva de Segredos Comerciais na UE e LPI no Brasil) deriva da extensão conceitual dos "dados pessoais".

Além disso, é importante reafirmar que o conceito de dados pessoais abrange qualquer informação relativa a um indivíduo (por definição, "identificado ou identificável"), excluindo

---

398 *Idem.*
399 *Idem.*
400 *ECHR, 16 December 1992, Niemietz v Germany, § 29, RTDH 1993, 470, note of P Lambert and F Rigaux*. (MALGIERI, 2016)
401 *CJEU, 14 February 2008, C-450/06, Varec SA v Belgium, § 48, Contrats Marche´s publ. 2008, n8 4, comm. 80, obs. J-P Pietri.* (MALGIERI, 2016)
402 RGPD: "Considerando (14) A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva." (g.n.)

dados anônimos que teoricamente não estão sujeitos às leis de proteção de dados. Também é necessário considerar todos os meios razoavelmente prováveis de serem usados (inclusive por terceiros) para identificar um indivíduo, direta ou indiretamente, a fim de determinar se uma pessoa é identificável. Mesmo que uma informação não identifique diretamente um indivíduo, isso pode ser possível por meio do enriquecimento de dados[403].

6.1.2 Proteção dos bancos de dados

Nas seções anteriores (voltado para o quadro europeu) parece que ao fim e ao cabo a "protagonista" do debate pode ter sido a lista de lista de clientes, cuja "segregação" (e consequente "apropriação") sempre foi considerada legítima no âmbito dos segredos comerciais.

Para complicar o contexto deste tópico, consideremos o debate particularmente voltado à proteção especial dos bancos de dados (tutela *sui generis*). Na União Europeia, a fonte legal é a Diretiva 96/9-CE e tem por base o reconhecimento do direito em questão é justificado pelo investimento realizado na obtenção, verificação ou apresentação do conteúdo de uma base de dados, ainda que não envolva o aspecto "criativo", requisitado no direito de autor.

Portanto, para sustentar que o conjunto de dados de informações do cliente deva ser protegido pelo direito "sui generis" do banco de dados, predomina o argumento de fundo "lockeano" no sentido de que investimentos e esforços foram/são necessários para as atividades de criação de um banco de dados e ao processamento sistemático desses dados.

Veja-se a transcrição dos "considerandos" da Diretiva 96/9 (CE):

> (40) Considerando que o objectivo deste direito sui generis consiste em garantir a protecção de um investimento na obtenção, verificação ou apresentação do conteúdo de uma base de dados durante o prazo limitado do direito; que esse investimento pode consistir na utilização de meios financeiros e/ou de ocupação do tempo, de esforços e de energia;
>
> (41) Considerando que o objectivo do direito sui generis consiste em conceder ao fabricante de uma base de dados a possibilidade de impedir a extracção e/ou a reutilização não autorizada da totalidade ou de uma parte substancial do conteúdo da base de dados; que é o fabricante de uma base de dados que toma a iniciativa e assume

[403] Article 29 Working Party (2013, p. 30): Opina no sentido de que o anonimato completo é difícil e as tecnologias modernas permitem a reidentificação dos indivíduos. Uma solução apropriada diferente pode, no entanto, envolver "anonimização parcial" ou pseudonimização (ou seja, onde os dados só podem ser vinculados ao indivíduo se ele possuir uma "chave" de decodificação), quando o anonimato completo não for praticamente viável. Se a anonimização parcial ou a desidentificação são suficientes, depende do contexto. Para esse fim, pode ser necessário complementar as técnicas de anonimato com outras salvaguardas para garantir uma proteção adequada, que inclui minimização dos dados, medidas organizacionais e técnicas adequadas.

> o risco de efectuar os investimentos; que isso exclui da noção de fabricante nomeadamente os subempreiteiros;
>
> (49) Considerando que, não obstante o direito de proibir a extracção e/ou a reutilização da totalidade ou de uma parte substancial de uma base de dados, se deverá prever que o fabricante de uma base de dados ou o titular do direito não possa impedir o utilizador legítimo de extrair e reutilizar partes não substanciais da base; que, no entanto, esse mesmo utilizador não pode prejudicar injustificadamente os legítimos interesses do titular do direito sui generis, nem o titular de um direito de autor ou de qualquer direito conexo sobre obras ou prestações contidas nessa base;
>
> (52) Considerando que os Estados-membros nos quais estão em vigor normas específicas que estabelecem um direito semelhante ao direito sui generis previsto na presente directiva, devem poder manter, em relação ao novo direito, as excepções tradicionalmente previstas por essa mesma legislação;
>
> (58) Considerando que, para além da protecção que a presente directiva assegura à base de dados através do direito de autor, e ao seu conteúdo através do direito sui generis de impedir a extracção e/ou a reutilização não autorizadas, devem continuar a aplicar-se as outras disposições legais relevantes existentes nos Estados-membros no que se refere ao fornecimento de produtos e serviços de bases de dados;
>
> Artigo 13º
>
> Aplicação de outras disposições legais
>
> O disposto na presente directiva não prejudica as disposições relativas nomeadamente ao direito de autor, aos direitos conexos ou a quaisquer outros direitos ou obrigações que subsistam sobre os dados, obras ou outros elementos incorporados numa base de dados, as patentes, marcas, desenhos e modelos, protecção dos tesouros nacionais, a legislação sobre acordos, as decisões ou prácticas concertadas entre empresas e concorrência desleal, o segredo comercial, a segurança, a confidencialidade, a protecção dos dados pessoais e da vida privada, o acesso aos documentos públicos ou

Aparentemente, na União Europeia, a incidência da Diretiva 96/9 EC dá azo ao debate no tocante à viabilidade inclusão dos dados individuais (caracterizados nos dados pessoais de um titular identificado ou identificável) no conceito de "conjunto de dados" ali objetos de proteção. Nessa Diretiva, resta certa a natureza *sui generis* desse direito de proteção, o qual não se confunde com o direito de autor.

Para SILVEIRA ([s.d.]), nos casos (União Europeia e EUA), a proteção se aplica ao "arranjo" dos dados, não extensiva para os elementos individuais do banco de dados.

Nos EUA, o banco de dados é protegido pela lei de direitos autorais (*copyright*)[404], sendo admitida a proteção de compilações, desde que selecionados, organizados de forma a constituir uma obra original.

[404] Proteção, em tese, seria de 70 anos.

Em se tratando de banco de dados não originais, com base em TSYVER [n.d.] [405], assinalam que a recomendação é que se busque proteção por meio de contratos. Trazem à colação o julgado *Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340*, 1991, para demonstrar, a título de exemplo, que uma compilação de dados de lista telefônica, embora possa representar uma coleção de fatos, uma vez que seria compilada sem qualquer criatividade ou originalidade, não se beneficia da proteção autoral, segundo a lei estadunidenses.

Em outros julgados, esses esforços teriam sido objeto de proteção (na hipótese a compilação de fatos seria protegida na medida em que demandara "grande esforço" do criador), sendo tal modalidade de proteção chamada de *"Sweat of thebrow" Protection*[406].

Contudo, sob a perspectiva do Ordenamento, predomina o entendimento de que tal proteção só se aplicaria a dados não originais, qual seja, banco de dados não relacionados com atividade intelectual de autor, mas que, todavia, demandaram investimentos consideráveis na sua formação. Em nome da teoria do esforço, na União Europeia, tal investimento é protegido mediante atribuição de uma propriedade sui generis, por 15 anos, em relação ao conjunto de informações ou dados livres, ou fatos, compilados. A Lei Brasileira [407] (como a Norte-Americana) não oferece proteção do banco de dados aos dados subjacentes (MILAGRE e SEGUNDO, 2015).

E se os dados - subjacentes a dados públicos - revelarem informações pessoais ou protegidas, a quem seria atribuído o controle sobre estes dados?

Em relação às bases de dados de dados pessoais tratados para fins comerciais, não é evidente se o investimento requerido reside na criação ou recolha. A rigor técnico, os controladores de dados não criam dados pessoais, apenas os reúnem e os organizam (Banterle, 2016)[408].

---

[405] TYSVER, [s.d.].
[406] ENGELFRIET, [s.d.].
[407] Lei 9610/1998

[408] Como observa Francesco Banterle (2016), "os contatos pessoais são fornecidos diretamente pelos clientes. Portanto, listas de clientes e grupos de e-mail (dados processados para fins de marketing direto) são dados "coletados" em vez de "criado" pelo controlador de dados. Além disso, a coleta de dados do cliente frequentemente requer a verificação das informações coletadas e um programa para processar e tornar as informações acessíveis para marketing. Mais importante ainda, conforme confirmado pelos tribunais nacionais, o processamento de dados para marketing requer a coleta do consentimento dos usuários e o fornecimento de mecanismos de cancelamento de assinatura, que são formalidades relacionadas à obtenção, verificação e atualização de dados".

Quanto à análise comportamental (*profiling*) seria preciso superar diversas dúvidas. Trata-se de um processo automatizado. Inexiste informação e é o software que analisa o comportamento dos clientes e gera dados de perfil. Regra geral, segundo o autor, dois aspectos podem ser considerados na análise comportamental: ***(i)*** como o cliente interage com um serviço; e ***(ii)*** históricos de compras dos clientes. A interação do cliente não faz parte da atividade principal do titular do banco de dados. São – em verdade - criados pelos clientes e capturados pelo controlador de dados. Os dados de compra (histórico) dos clientes podem ser originados da atividade principal do controlador de dados (não há investimento na criação de tais dados). Vislumbra que o investimento ocorra na criação de um software de análise. Em qualquer caso, a configuração de um sistema de criação de perfil requer: ***(i)*** atualização metódica dos dados de acordo com o comportamento dos clientes ou preferências de privacidade; ***(ii)*** que a apresentação desses dados permita/viabilize a sua exploração em atividades de marketing. (Banterle, 2016).

É de se notar que uma compilação não é protegida pelo direito autoral brasileiro somente pelo fato de ser "compilação" (MILAGRE e SEGUNDO, 2015). É preciso que seus fatos e dados sejam organizados de tal modo que a obra constitua uma autoria original. Diversamente, como se viu, a Europa protege os bancos de dados não originais, se houve esforço em sua compilação, pelo direito "*sui generis*".

Se os dados pessoais são protegidos na forma da Lei Geral de Proteção de Dados (13.709/2018) questão que se abre é se com base na teoria do esforço, o empenho das "plataformas" em agrupar dados pessoais ensejaria a elas especial modalidade de apropriação aos dados subjacentes. Aparentemente não, a considerar os termos estritos da Lei dos direitos de autor (9.610/98)[409].

[409] Lei nº 9.610, de 1998: "Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como: (...) XII - os programas de computador; XIII - as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de seu conteúdo, constituam uma criação intelectual. § 1º Os programas de computador são objeto de legislação específica, observadas as disposições desta Lei que lhes sejam aplicáveis. § 2º A proteção concedida no inciso XIII não abarca os dados ou materiais em si mesmos e se entende sem prejuízo de quaisquer direitos autorais que subsistam a respeito dos dados ou materiais contidos nas obras. § 3º No domínio das ciências, a proteção recairá sobre a forma literária ou artística, não abrangendo o seu conteúdo científico ou técnico, sem prejuízo dos direitos que protegem os demais campos da propriedade imaterial." (g.n.)

6.1.3 A quem pertencem os dados pessoais – a questão proprietária[410].

Modo geral, o pensamento jurídico no Brasil, que é em parte influenciado pelos tratados e doutrina internacionais, segue a mesma inclinação "patrimonialista" majoritária no âmbito da propriedade intelectual[411].

Contudo, em relação ao segredo de negócios, é interessante observar, com base em ARAUJO (2015)[412], que desde Visconde de CAIRU (1874)[413] a tutela jurídica preconizava tão somente a legitimidade da guarda do sigilo em relação às transações confidenciais, cujo ônus era atribuído ao próprio comerciante. Não chegava a ponto de advogar a respectiva tutela ao abrigo dos direitos da personalidade da pessoa jurídica, senão da necessidade de proteção em face da concorrência desleal[414].

No debate contemporâneo, entretanto, parece haver uma aproximação entre a confidencialidade dos negócios empresariais e os dados pessoais[415]. Teorias como a dos círculos concêntricos, a analogia com a Quarta Emenda nos Estados Unidos e o Artigo 108 da Convenção Europeia de Direitos Humanos são invocadas para demonstrar uma possível conexão entre os direitos fundamentais, viabilizando a proteção dos segredos tanto no âmbito da privacidade quanto no dos direitos de personalidade (ver seção 6.1).

Nesse sentido, Vaneska Donato Araújo (2015, passim)[416] aponta que diversos autores nacionais[417] argumentam que a proteção do segredo comercial no Brasil poderia ser respaldada pelo direito à intimidade da pessoa jurídica. No entanto, a autora contrapõe essa ideia com a noção de especialidade do direito autoral, defendida por Giselda Hironaka e Silmara Chinelato,

---

[410] Danilo Doneda (2021, p. 303) analisa criticamente o modelo proprietário de proteção e oferece, de forma detalhada, as diversas modalidades de tutela dos dados pessoais, dentre as quais menciona os modelos preconizados por Adolfo Di Majo: a tutela proprietária, a tutela dos direitos da pessoa, a tutela aquiliana e a tutela das leis de proteção, este nos moldes germânicos.

[411] DI MAJO, *op. cit.*, p. 240 *apud* DONEDA, 2021, p. 338.

[412] ARAUJO, 2015.

[413] Reimpressão fac-símile pelo Serviço de Documentação do Ministério da Justiça e Negócios Interiores, Rio de Janeiro, 1963, *apud* ARAUJO, 2015.

[414] Nesse sentido estrito foram os acordos comerciais firmados no século posterior: *Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio*, tratado internacional, integrante do conjunto de acordos assinados em 1994, que encerrou a Rodada Uruguai e criou a Organização Mundial do Comércio.

[415] À guisa de especulação, essa imbricação parecia decorrer da inexistência de expressa previsão constitucional para a proteção dos dados pessoais suprida com a edição da Emenda à Constituição nº 115, de 2022, que acrescentou ao art. 5º o inciso LXXIX ("é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"). Até então, tanto o segredo de negócios quanto a proteção de dados pessoais teriam, em tese, amparo nos mesmos dispositivos constitucionais relacionados à inviolabilidade da intimidade e do sigilo (incisos X e XII do art. 5º da Constituição Federal)

[416] *Idem*.

[417] Por todos, mencione-se PEREIRA, [s.d.], p. 13; SZNIAWSKI, 1989, pp. 81-92; SIMÃO FILHO *apud* MARTINS; FERREIRA JUNIOR, 2005, p. 337-365.

que distinguem os elementos de natureza patrimonial e moral[418], considerando estes últimos como direitos de personalidade efetivamente reconhecidos. Araújo argumenta que a pessoa jurídica pode ser beneficiária do direito autoral, já que investe recursos na organização, seleção e instrução da obra, mas limitando-se aos aspectos patrimoniais. Além disso, a pessoa jurídica poderia ser considerada a criadora da obra, embora não pudesse reivindicar a paternidade da mesma com base no conceito de direito de personalidade[419]. No que diz respeito ao segredo comercial e industrial, Araújo enfatiza que sua proteção é essencialmente patrimonial e não visa preservar uma suposta intimidade, mas sim viabilizar o desenvolvimento dos negócios por meio da proteção contra a concorrência desleal. Nesse aspecto, ela concorda com a linha de pensamento dos autores mencionados.

Para Laura Schertel Mendes (2014)[420], a regulação de proteção de dados pessoais não pode ser compreendida como atributiva de um direito de propriedade, pois tendo natureza multidimensional teria por objetivo equilibrar os direitos de proteção, de defesa e de participação do indivíduo nos processos comunicativos, prestando-se a proteger a personalidade do indivíduo contra os riscos ocasionados pela coleta, processamento e circulação de dados pessoais.

No entanto, uma interpretação que considere os dados pessoais como bens negociáveis levantaria preocupações éticas, uma vez que as informações relacionadas ao indivíduo no meio digital refletem sua identidade. Isso remete às construções teóricas da sociologia, filosofia e ciência política, que relacionam a identidade individual com o papel de cidadão, sendo responsável e com liberdade suficiente para formar opiniões e preferências sobre si mesmo[421].

De qualquer modo, apesar das objeções e críticas à referida linha de pensamento (MOROZOV, 2018; ZUBOFF, 2019), não se pode ignorar as implicações políticas (e portanto

---

[418] Em seus aspectos morais, o direito autoral é aquele gerado da relação do autor com sua criação, estando, por isso, estreitamente vinculado à pessoa do autor, como fosse uma projeção de sua personalidade. Em razão disso, incide ao direito moral o atributo de um direito "personalíssimo", da irrenunciabilidade, impenhorabilidade, ao lado dos direitos específicos do direito ao "inédito", à paternidade, à integridade, à modificação e arrependimento (Lei nº 9.610, de 1998).

[419] Neste particular, Vaneska Donato Araújo (2015) recorre a Rolf Serick (1966) para afirmar que "(...) igualmente, o direito moral tem natureza diversa do direito de tutela ao nome. Este último é imanente a um sujeito humano e por isso constitui um verdadeiro e próprio direito da personalidade. O direito a paternidade espiritual é, ao contrário, uma relação do autor com a própria obra, que vem a ser apenas por meio da atividade criativa; não se trata assim, de um verdadeiro e próprio direito da personalidade". Nesse raciocínio, a autora pontua que o abandono da rígida divisão entre direitos públicos e privados propiciaria melhor visão no tocante aos direitos fundamentais do ser humano, como tal apto a vincular não apenas o Estado como também os particulares.

[420] MENDES, 2014.

[421] SPIEKERMANN, S.; ACQUISTI, A.; BÖHME, R.; HUI, K (2015)

com repercussão jurídica) decorrentes dos interesses econômicos envolvidos na promoção e exploração comercial de um mercado de dados pessoais a partir de demanda por sua categorização como importante ativo com potencial de agregação de valor para empresas e para os consumidores.

Outra questão relevante, a nosso ver primordial – porém não enfrentada neste tópico - refere-se à anonimização e sua relação com o "estado da técnica". Restaria de fato viabilizada a anonimização num contexto do avanço da tecnologia nos moldes observados nos "v's da *big data*? Teria a regulação "se traído"[422] ao aparentemente fugir da definição de estado da técnica positivada no Artigo 11 da Lei de 9.279/96[423] ou a ideia subjacente (ao incluir o termo "identificável" na definição de "dados pessoais") teria sido a de estabelecer uma barreira de acesso ao tratamento de dados pessoais à elite tecnológica[424], justamente aqueles "*players*" que dominam e segregam o estado da técnica (da desanonimização) por intermédio do mecanismo do segredo comercial?

Em suma, a resolução desses conflitos mencionados dependerá de um posicionamento enfático das autoridades nacionais, que devem se manter atualizadas em relação a essas e outras tensões entre a proteção da confidencialidade da tecnologia e a proteção de dados pessoais. As respostas para essas questões vão além do escopo deste trabalho e certamente serão objeto de pesquisas futuras.

6.2 PERSPECTIVAS REGULATÓRIAS DA PROTEÇÃO DE SEGREDO DE NEGÓCIOS, DADOS PESSOAIS E DECISÕES AUTOMATIZADAS POR SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

[422] LGPD, art. 12: "§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios." (g.n.)

[423] Lei nº 9.279, de 1996, art. 11: "§ 1º O estado da técnica é constituído por tudo aquilo tornado acessível ao público antes da data de depósito do pedido de patente, por descrição escrita ou oral, por uso ou qualquer outro meio, no Brasil ou no exterior, ressalvado o disposto nos arts. 12, 16 e 17." (g.n.)

[424] "Em todo o mundo a economia do conhecimento permanece restrita a vanguardas insulares: manufatura avançada, serviços intensivos em conhecimento (frequentemente associados com a manufatura avançada) e agricultura científica de precisão. Mesmo onde tenha perdido qualquer conexão privilegiada com a indústria, permaneceu, em cada setor, uma franja" (UNGER, 2018, p. 36).

Existem aparentes tensões entre as proteções jurídicas conferidas ao segredo de negócios e aos dados pessoais. Nas seções anteriores, foi demonstrado que as controvérsias em torno da transparência e explicabilidade das decisões automatizadas ainda não foram completamente resolvidas.

Essa falta de clareza na regulamentação precisa ser aprimorada, pois além de impedir a participação do país na corrida tecnológica do século XXI, é necessário lidar com os riscos significativos decorrentes da inteligência artificial, do uso de big data e do aprendizado de máquina.

No âmbito da LGPD, MONTEIRO (2021) destaca a preocupação concernente às insuficiências da norma para garantir a proteção dos dados pessoais razão por que propõe medidas para solucioná-las[425].

Nem mesmo o Regulamento Geral de Proteção de Dados (RGPD) escapa das polêmicas. Nesse aspecto, ZARSKY (2017)[426] e HILDEBRANDT (2015)[427], *apud* SARTOR e LAGIOIA (2020)[428], argumentam que o GDPR seria incompatível com IA e *big data*, uma vez que o GDPR se baseia em princípios – como o da limitação de finalidade, da minimização de dados, do tratamento especial de "dados sensíveis", das limitação de decisões automatizadas – que são incompatíveis com o uso extensivo de IA, de aplicação da *big data*, de sorte que a UE não poderia, com base na GDPR, avançar na corrida tecnológica, nesses domínios liderada pelos EUA e a China.

SARTOR e LAGIOIA (2020), por seu turno, contrapõem (p. 76) à opinião desses autores por eles referenciados para sustentar que é possível – e que também é provável – que o GDPR possa ser interpretado de forma a conciliar ambos os desideratos: proteger os titulares dos dados e permitir aplicações úteis de IA. Contudo, reconhecem (p. 79) que existem vários

[425] Em breve síntese, a proposição de MONTEIRO (2021, p. 314 *et seq*.) ampara-se na ideia de desenvolvimento de um "*framework* de explicabilidade a partir da cláusula geral do devido processo informacional, na forma de uma 'caixa de ferramentas', composta por diferentes instrumentos técnico-jurídicos, que podem ser combinados para a construção de um modelo de explicação em uma determinada situação concreta".
[426] ZARSKY, 2017, pp. 995-1020.
[427] HILDEBRANDT, 2015.
[428] SARTOR; LAGIOIA, 2020.

problemas de incertezas em relação à proteção de dados relacionados à IA não respondidos explicitamente no GDPR[429].

Uma visão ampliada poderia se extrair do argumento de Rodrigo Leme FREITAS (2021, p. 404 e 405)[430] no sentido de que – dada a crise que assola a temática do acesso-controle aos dados (e aos conhecimentos) no âmbito da propriedade intelectual – a compreensão prospectiva acerca da adequação paradigmática das "conjecturas possíveis que circulam no âmbito tecnológico-econômico-político-jurídico" passa pelo entendimento do papel da convergência tecnológica nesses domínios (pano de fundo desta pesquisa, v. Seções 2 e 3, retro).

Portanto, assumindo (com base em FREITAS, 2021) que convergência tecnológica e convergência regulatória são temas imbricados, nesta seção especula-se sobre os possíveis desdobramentos do debate público no País, o que se faz necessariamente a partir da experiência internacional.

Além disso, a maioria dos países democráticos parece empenhada na harmonização, compartilhando das mesmas preocupações éticas e jurídicas, no que toca à transparência e explicabilidade dos sistemas computacionais de IA utilizados em decisões automatizadas.

---

[429] Dado esse cenário, Sartor e Lagioia (2020) concluem que "os controladores envolvidos no processamento baseado em IA devem endossar os valores do GDPR e adotar uma abordagem responsável e orientada para o risco, e devem ser capazes de fazê-lo de maneira compatível com as tecnologias disponíveis e com rentabilidade econômica (ou a realização sustentável de interesses públicos). No entanto, dada a complexidade do assunto e as lacunas, imprecisões e ambiguidades presentes no GDPR, os controladores não devem ser deixados sozinhos neste exercício. As instituições precisam promover um amplo debate social sobre aplicações de IA e devem fornecer indicações de alto nível. As autoridades de proteção de dados precisam engajar ativamente um diálogo com todas as partes interessadas, incluindo controladores, processadores e sociedade civil, para desenvolver respostas apropriadas, com base em valores compartilhados e tecnologias eficazes. A aplicação consistente dos princípios de proteção de dados, quando combinada com a capacidade de usar a tecnologia de IA de forma eficiente, pode contribuir para o sucesso dos aplicativos de IA, gerando confiança e prevenindo riscos". [No original: "*In conclusion, controllers engaging in AI-based processing should endorse the values of the GDPR and adopt a responsible and risk-oriented approach, and they should be able to do so in a way that is compatible with the available technologies and with economic profitability (or the sustainable achievement of public interests). However, given the complexity of the matter and the gaps, vagueness and ambiguities present in the GDPR, controllers should not be left alone in this exercise. Institutions need to promote a broad social debate on AI applications and should provide high level indications. Data protection authorities need to actively engage a dialogue with all stakeholders, including controllers, processors, and civil society, to develop appropriate responses, based on shared values and effective technologies. Consistent application of data protection principles, when combined with the ability to use AI technology efficiently, can contribute to the success of AI)applications, by generating trust and preventing risk*s"].

[430] Na obra, resultante de sua tese de doutorado na Faculdade de Direito da USP, aprovada "com distinção", o autor levanta e enfrenta os grandes desafios – em parte relacionados com a convergência regulatória – a serem enfrentados nesses domínios, no âmbito das adequações dos sistemas jurídicos nacionais frente às diversas crises globalmente presentes neste início de século XXI.

De acordo com os cientistas políticos Bennett e Raab (2006) [431], citados por Mendes (2014) [432], a proteção de dados pessoais deu origem a um setor autônomo de política pública, reconhecendo a importância do controle do fluxo de informações pessoais na sociedade atual. Esse setor autônomo é caracterizado pela existência de instrumentos legais próprios, organismos regulatórios específicos, uma rede de especialistas e juristas, um grupo robusto de jornalistas e ativistas dispostos a expor abusos e violações, uma comunidade acadêmica crescente especializada no tema e uma rede internacional para o intercâmbio de experiências e ideias.

Estudos posteriores, protagonizados por esses autores, enfocam a análise da convergência regulatória no campo da proteção de dados, considerando quatro perspectivas: determinismo tecnológico, emulação, harmonização e penetração[433].

O determinismo tecnológico sugere que as inovações tecnológicas inevitavelmente mudam a sociedade, levando as leis e políticas a se adaptarem a essas mudanças. No entanto, argumenta-se que essa abordagem é problemática, pois as tecnologias frequentemente refletem os valores e interesses de seus criadores e usuários, e não são necessariamente neutras em relação à privacidade e proteção de dados pessoais. A emulação envolve a criação de leis e políticas com base nas práticas de outros países ou regiões. Embora possa ser útil para estabelecer padrões globais de proteção de dados, a emulação também pode resultar em uma competição para a adoção de padrões cada vez mais fracos. A harmonização consiste na criação de leis e políticas comuns em nível internacional, mas é difícil alcançar esse objetivo devido às diferentes tradições jurídicas, culturais e políticas dos países. Por fim, a penetração envolve a criação de padrões de proteção de dados em nível internacional por meio de negociação e persuasão, sem a necessidade de um acordo legal formal. Embora possa ser útil para criar padrões globais de proteção de dados, também pode levar à adoção de padrões mínimos inadequados para proteger adequadamente os dados pessoais[434].

---

[431] BENNETT; RAAB, 2006, p. XXI *apud* MENDES, 2014.
[432] MENDES, 2014.
[433] BENNETT; RAAB, 2018.
[434] Mendes e Bioni (2019, pp. 157-180) abordam esses quatro elementos de análise nos seguintes termos*:* "*a) determinismo tecnológico: ainda que países tivessem aspectos culturais socioeconômicos e jurídicos distintos, acabaram por enfrentar problemas e desafios comuns que os aproximaram a adotar soluções regulatórias similares; b) emulação: a criação de normas sobre a matéria que acabaram por serem adaptadas ou copiadas por regulações posteriores. Nesse sentido, as Fair Information Practice Pinciples foram gestadas no contexto estadunidense, mas acabaram cruzando o Atlântico e influenciando toda a jornada europeia; c) harmonização: por questões de interesse econômicos e de relações exteriores, percebeu-se a necessidade da articulação de padrões normativos para que não fosse inviabilizada a integração entre diferentes países e blocos econômicos*

De acordo com Mendes e Bioni (2019) [435], a formulação de diretrizes e convenções internacionais pela OCDE nas décadas de 1980 influenciou as leis de proteção de dados ao redor do mundo. Em relação à comparação entre o Regulamento Geral de Proteção de Dados da União Europeia (RGPD) e a Lei Geral de Proteção de Dados brasileira (LGPD), os autores avaliam que, embora tenham abordagens legislativas distintas, é possível observar equivalências normativas entre elas, como o princípio da accountability e as ferramentas de corregulação.

Por outro lado, Marília Machado Muchiuti (2022) [436], com base em Anu Bradford (2019) [437], analisa o conteúdo da LGPD em comparação com o RGPD e sugere que essa aproximação pode ser explicada pelo "Efeito Bruxelas", no qual a União Europeia exporta normas facilitadas por mercados, empresas privadas e dinâmicas de influência. Muchiuti argumenta que o processo de difusão de normas no sistema internacional desafia as visões tradicionais desse sistema normativo, aproximando as perspectivas e literaturas das Relações Internacionais e do Direito de forma holística e integrada

Estendendo o campo de visão, GRUSIN (2015, *apud* CANTARINI, [2022])[438], sugere que as preocupações globais com os impactos humanístico-sociais das novas tecnologias - e especialmente aquelas decorrentes da utilização da inteligência artificial (IA) - dão azo à percepção de que as diretrizes éticas e questões legais caminham *pari-passu* com o tema da governança dos algoritmos, a ponto de deslocar a centralidade da *autorregulação* rumo a uma *autorregulação regulada*[439].

De acordo com FLORIDI (2021) [440] e MENDES e FONSECA (2021) [441], o modelo regulatório da IA está em desenvolvimento no Brasil, ainda que esteja em fase inicial ou incipiente, na nossa opinião.

---

sob o argumento de normas conflitantes; d) penetração: a ação de atores políticos no processo de construção de regimes jurídicos que forçou essa agenda de padronização".

[435] MENDES; BIONI, 2019, pp. 157-180.

[436] MUCHIUTI, 2022.

[437] BRADFORD, 2020.

[438] GRUSIN, 2015, pp. vii-xxxi.

[439] Dada a limitação de várias ordens, este trabalho não se estende na conceituação desses modelos regulatórios, embora os mencionem, assim como os vê implicitamente acolhidos na LGPD. Entre outros, v. FLORIDI, 2021; MENDES; FONSECA *apud* DONEDA *et al*., 2021, pp. 73-95.

[440] FLORIDI, 2021.

[441] MENDES; FONSECA *apud* DONEDA et al., 2021.

Embora a LGPD já apresente sinais de autorregulação regulada (art. 46 e art. 50) [442] a lei brasileira de proteção de dados parece não abordar adequadamente os procedimentos necessários para implementar os consensos estabelecidos em torno dos "Princípios de Práticas Justas de Informação (FIPPs)" [443], embora tenha incorporado esses princípios, em conformidade com o GDPR (MENDES e FONSECA, 2019) [444].

Nesse contexto, é possível especular que uma das possíveis explicações para essa discrepância está na falta de consolidação da estrutura da autoridade nacional responsável pela regulamentação e fiscalização (LGPD: art. 55), que poderia preencher essas lacunas.

Segundo Paola CANTARINI ([2022]), o próprio mercado assumira a incorporação de vetores éticos nas suas regulamentações devido à necessidade de demonstrar "comprometimento com o requisito de confiança", o que pode ser um diferencial competitivo, mesmo considerando os impactos em todos os aspectos da vida individual, incluindo concepções de tempo, espaço, cultura e subjetividades [445].

Diante da demora das instâncias estatais na produção de regulamentações, vários documentos internacionais foram produzidos para enfatizar o papel da autorregulação regulada, estabelecendo requisitos e parâmetros mínimos de governança pelo Estado. Um exemplo concreto é o "IA Act de 04.2021" da União Europeia, que, com base no princípio da precaução,

---

[442] LGPD: "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. ; 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."

[443] As *Fair Information Practice Pinciples* consubstanciam exemplos de que a criação de normas sobre a matéria da proteção de dados acaba por ser adaptada ou copiada por regulações posteriores na medida em que foram gestadas no contexto estadunidense e acabaram cruzando o Atlântico influenciando toda a jornada europeia. (BENNETT; RAAB, 2018 *apud* DONEDA et al., 2021, pp. 73-95)

[444] Segundo Mendes e Fonseca (2019), a "Diretiva 95/46/CE e, posteriormente, o Regulamento Geral de Proteção de Dados europeu (RGPD) acabaram incorporando também esse consenso em torno dos FIPPs". Ademais, a LGPD "(...) prevê todos os princípios presentes no Regulamento europeu e estabelece ainda outros três: segurança, prevenção e não discriminação".

[445] CANTARINI, 2022.

aborda a calibragem dos procedimentos de conformidade de acordo com o grau de risco derivado do uso da tecnologia, em relação aos direitos e liberdades fundamentais[446].

Ainda na esteira de Paola CANTARINI (2022), essa mesma abordagem estaria presente nas propostas europeias de regulamentação da IA, particularmente no "*White paper On Artificial Intelligence - A European approach to excellence and trust*"[447], de 19.02.2020, modelo que encamparia vertente mais complexa do direito regulatório, envolvendo técnicas de prevenção e mitigação de riscos a direitos e liberdades fundamentais, incluindo a preocupação com a proteção individual, coletiva e social.

Nesse sentido, o "*White paper on IA*" classifica como alto risco a utilização de IA que envolva significativos riscos na proteção da segurança, dos direitos dos consumidores e dos direitos fundamentais. Nessa avaliação, segundo os critérios da *AI Act de* 2021, seriam considerados **riscos inaceitáveis** uma possível ameaça aos cidadãos europeus as aplicações cuja finalidade inclua a manipulação de comportamentos, opiniões e emoções humanas, notadamente em setores vulneráveis da população, como o de brinquedos com assistentes de voz, com potencial para influenciar facilmente crianças e adolescentes. Seria também inaceitável o recurso a sistemas de pontuação social por parte de governos, como parece ocorrer na China.

Seguindo-se a abordagem da *risquificação*, as obrigações são definidas e vinculadas a avaliação adequada do risco e mitigação dos sistemas e maior controle na qualidade dos conjuntos de dados de entrada dos sistemas, garantindo maior controle na qualidade dos conjuntos de dados de entrada e na documentação e supervisão humanas obrigatórias para garantir a rastreabilidade dos resultados.

---

[446] Conforme sugere a autora, poderiam ser utilizadas ferramentas tecnológicas de governança na própria construção dos sistemas de decisão automatizada, de forma a dar efetividade, por exemplo, ao direito de revisão de decisões automatizadas, através de uma abordagem preventiva (*privacy by design*), que seriam instituídas obrigação de respeito aos direitos fundamentais como um objetivo central do processo de construção de software, aplicável a todo o ciclo de vida do sistema, à guisa de requisito para a viabilidade de tal projeto, como já prevê o Artigo 25 da GDPR. Prossegue, noticiando que a Proposta de 04.2021 da UE seguiria a ótica de uma regulamentação via risquificação", traçando uma "análise de risco e separando em diversos patamares e níveis de risco as aplicações de IA, de alto risco, moderado-limitado, baixo risco e risco inaceitável, envolvendo aplicações que jamais deveriam ser desenvolvidas". Tais exigências poderiam ser fundamentadas nas regulamentações ex ante, baseadas no princípio da precaução, como códigos de conduta, certificações, auditorias independentes, elaboração de documentos como DPIA – relatório de impacto de proteção de dados e LIA – avaliação do legítimo interesse, e na área da IA, relatório de impacto algoritmo, ou relatórios de direitos fundamentais e humanos, sob a ótica do direito regulatório e do direito ambiental, aplicáveis à proteção de dados, em conformidade com a GPDR ou com a LGPD. (CANTARINI, 2022)

[447] *The Artificial Intelligence Act* (2021).

Enfim, tem-se o raciocínio de CANTARINI (2022) no sentido de que, embora a proposta de regulamentação da IA via IA ACT de 2021[448] contemple particularmente a estratégia europeia de 2018 (COM/2018/237 – "Inteligência para Europa") e englobe objetivos específicos como o da competitividade da União Europeia frente ao protagonismo tecnológico dos EUA e China, essas regulamentações em curso na União Europeia terão impacto – em razão do aludido "efeito Bruxelas" - nos demais países como já ocorreu com o GDPR, que inspirou outras iniciativas legislativas locais, como é notório, a própria lei geral brasileira (LGPD).

De qualquer forma, tanto o Brasil quanto muitos outros países, especialmente na União Europeia, estão buscando estabelecer um marco regulatório para promover a confiança geral da sociedade na utilização de sistemas de IA, conciliando a inovação baseada nessas tecnologias com direitos individuais, valores sociais e princípios de proteção de dados (SARTOR, LAGIOIA, 2020, p. 73, passim).[449].

6.3 MARCO LEGAL PARA A INTELIGÊNCIA ARTIFICIAL NO BRASIL

A teleologia das estratégias para IA - voltadas ao desenvolvimento de sistemas de uma inteligência artificial (IA) ética, segura e confiável[450] - está amplamente disseminada nos países e organizações internacionais, todos virtualmente interessados no fomento e no protagonismo nesses domínios da tecnologia[451] .

Embora o segredo seja valorizado nos negócios, a realidade é que cada Estado-nação competidor não reserva exclusivamente uma estratégia nesse sentido. Isso pode ser atribuído à incompatibilidade dessa abordagem individualista com os imperativos da conexão e cooperação global, inerentes à inevitável convergência tecnológica (v. seção 6.2).

---

[448] *The Artificial Intelligence Act* (2021).

[449] V. proposição ("*4. Policy options: How to reconcile AI-based innovation with individual rights & social values and ensure the adoption of data protection rules and principles*") em Sartor e Lagioia (2020), tendo a RGPD como referencial normativo.

[450] ESTRATÉGIAS..., 2019.

[451] No Brasil, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) lançou, em dezembro de 2019, a Consulta Pública da Estratégia Brasileira de Inteligência Artificial, com o objetivo de "colher subsídios para a construção de uma Estratégia Nacional de Inteligência Artificial que permita potencializar os benefícios da IA para o país, mitigando eventuais impactos negativos" (ITSRIO, 2020)

Na prática, o País tende a alinhar-se às diretrizes internacionais, conforme destacado em documentos oficiais, como o Anexo à Portaria 4679, de 13.07.2021, que altera o Anexo da Portaria 4617, de 6.4.2021, do Ministério da Ciência, Tecnologia e Inovações. A Estratégia Brasileira de Inteligência Artificial (BRASIL, 2021) [452] é fundamentada nos cinco princípios definidos pela OCDE (Organização para a Cooperação e Desenvolvimento Econômico) para a gestão responsável dos sistemas de IA[453]: crescimento inclusivo, desenvolvimento sustentável e bem-estar; valores centrados no ser humano e na equidade; transparência e explicabilidade; robustez, segurança e proteção; e prestação de contas (accountability).

Em seu texto, o documento estatal sinaliza preocupação com a disseminação da IA no País, considera que a Lei Geral de Proteção de Dados em vigor (LGPD) estabelece diversos requisitos no tocante ao uso da IA, e, nesse aspecto, firma entendimento de que é necessário avançar no debate público e participativo e nos estudos dos impactos da IA em diferentes setores.

Após uma discussão pública realizada no segundo semestre de 2022 para coletar subsídios para a construção do marco legal da IA no País[454], uma proposta[455] foi apresentada

[452] Ao que se depreende, esses princípios, em tese, derivam das seguintes recomendações da OCDE*:" (*a) A IA deve beneficiar as pessoas e o planeta, impulsionando o crescimento inclusivo, o desenvolvimento sustentável e o bem-estar; (b) Os sistemas de IA devem ser projetados de maneira a respeitar o Estado de Direito, os direitos humanos, os valores democráticos e a diversidade e devem incluir salvaguardas apropriadas – possibilitando a intervenção humana sempre que necessário – para garantir uma sociedade justa; (c) Organizações e indivíduos que desempenham um papel ativo no ciclo de vida de IA devem se comprometer com a transparência e com a divulgação responsável em relação a sistemas de IA, fornecendo informações relevantes e condizentes com o estado da arte que permitam: (i) promover a compreensão geral sobre sistemas de IA; (ii) tornar as pessoas cientes quanto às suas interações com sistemas de IA; (ii) permitir que aqueles afetados por um sistema de IA compreendam os resultados produzidos; e (iv) permitir que aqueles adversamente afetados por um sistema de IA possam contestar seu resultado.; (d) os sistemas de IA devem funcionar de maneira robusta, segura e protegida ao longo de seus ciclos de vida. (e) Os riscos em potencial devem ser avaliados e gerenciados continuamente."

[453] Para além da recomendação, o documento (ibidem) menciona outros instrumentos havidos como referenciais indicativos do debate em torno do estabelecimento de princípios gerais e éticos a serem adotados pelos atores públicos e privados em relação ao tema, e da necessidade de observância à harmonização dos princípios que guiam a noção de Estado de Direito, de modo que beneficie a sociedade, impulsionando o crescimento inclusivo, o desenvolvimento sustentável e o bem-estar, ei-los: Princípios da OCDE sobre Inteligência Artificial (2019); G20: Declaração Ministerial sobre Comércio e Economia Digital – Princípios para IA Centrada nos Humanos (2019); Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial criado pela Comissão Europeia: Orientações Éticas para uma IA de Confiança; A Declaração de Toronto: Protegendo os Direitos à Igualdade e à Não-Discriminação em Sistemas de Aprendizado por Máquinas (2018); Comunicação da Comissão Europeia: Inteligência Artificial para a Europa (2018); Diretrizes Universais para Inteligência Artificial (2018); Declaração sobre Ética e Proteção de Dados em Inteligência Artificial (2018); *Asilomar AI Principles* (2017).

[454] Projeto de Lei 2338nº 2.338, de /2023, de autoria do Senador Rodrigo Pacheco (BRASIL, 2023)

[455] Proposição apresentada no bojo relatório finaldo Relatório Final encaminhado ao Senado Federal em 06 de dezembro de .12.2022. (FRAGOSO, 2022)

ao Senado Federal em 08.12.2022 por um grupo de especialistas[456]. Essa proposta define um "sistema de inteligência artificial" em termos de sua finalidade e uso.

Eis a redação proposta.

> Art. 4°. Para as finalidades desta Lei, adotam-se as seguintes definições:
>
> I – **sistema de inteligência artificial**: sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real. (s.n..)[457]

Sem adentrar na análise dos aspectos "técnicos" incorporados na aludida definição, parece esclarecedor anotar que a proposição relacionada com a "definição de IA" incorporou diferentes pontos de vista do debate.

Para garantir o alinhamento regulatório e evitar que a regulação restrinja a inovação e a adoção da IA no País, é reconhecida a importância de observar princípios relacionados a desenvolver estruturas legais existentes, adotar uma abordagem regulatória baseada em princípios e resultados, realizar um "teste de equilíbrio de riscos/benefícios" centrado no indivíduo humano e conduzir avaliações de impacto (BRASIL, 2021, EBIA):

Que ou quais as iniciativas relacionadas com o debate público se seguiram à formulação da estratégia regulatória? O já aludido Relatório Final (BRASIL, 2022), subscrito pela Comissão de Juristas[458], adotado como justificação do projeto de lei (Projeto), atribuído ao Senador Rodrigo Pacheco (BRASIL, 2023, PL 2338/2023) parece materializar referida discussão, razão por que se descreve aqui seus pontos centrais.

O Projeto em questão anuncia dois objetivos. Por um lado, busca estabelecer direitos para proteger as pessoas afetadas pelos sistemas de IA, incluindo desde recomendações de

---

[456] Projeto de 2338Lei nº 2.338, de /2023 (BRASIL, 2023) teve por subsídios o debate público coordenado pela já referida Comissão de Juristas instituída em 17 de fevereiro de 2022, por meio do Ato do Presidente do Senado nº 4, de 2022, presidida por Ricardo Villas Bôas CUEVA e relatada por Laura Schertel Ferreira MENDEs, e também integrada por Ana de Oliveira FRAZÃO; Bruno Ricardo BIONI; Danilo Cesar Maganhoto DONEDA *(in memoriam);* Fabrício de Mota ALVES; Miriam WIMMER; Wederson Advincula SIQUEIRA; Claudia Lima MARQUES; Juliano Souza de Albuquerque MARANHÃO; Thiago Luís Santos SOMBRA; Georges ABBOUD; Frederico Quadros D'ALMEIDA; Victor Marcel PINHEIRO; Estela ARANHA; Clara Iglesias KELLER; Mariana Giorgetti VALENTE; Filipe José Medon AFFONSO. Disponivel em https://legis.senado.leg.br/comissoes/comissao?codcol=2504, acesso em 08.12.2022.

[457] BRASIL, (2023).

[458] Relatório Final apresentado em 6 de dezembro de 2022, ao Senado Federal, pela Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil. (BRASIL, 2022)

conteúdo na Internet até análise de elegibilidade para crédito e políticas públicas. Por outro lado, visa criar condições de previsibilidade e segurança jurídica para a inovação e o desenvolvimento tecnológico, estabelecendo ferramentas de governança e um arranjo institucional de fiscalização e supervisão.

A proposição pressupõe (i) não haver um *trade-off* entre a proteção de direitos e liberdades fundamentais, a valorização do trabalho e a dignidade da pessoa humana, e a ordem econômica e a criação de novas cadeias de valor e (ii) que é possível harmonizar esses elementos de acordo com os fundamentos e princípios estabelecidos na Constituição Federal.

O projeto se baseia em uma regulação de riscos e em uma modelagem regulatória fundamentada em direitos, com instrumentos de governança para garantir a prestação de contas dos agentes econômicos envolvidos na IA. São estabelecidos fundamentos e princípios gerais para o desenvolvimento e uso dos sistemas de IA, bem como direitos para proteção das pessoas afetadas por esses sistemas, incluindo o direito à não-discriminação e à correção de vieses discriminatórios.

O projeto também trata da responsabilização civil integral, da fiscalização da IA, da promoção da inovação, da conformidade com o direito internacional e dos direitos autorais e propriedade intelectual relacionados aos dados utilizados pela IA.

São em tese estabelecidos direitos básicos e transversais para todas as interações entre máquinas e seres humanos, como informação e transparência. Essas obrigações seriam acentuadas quando o sistema de IA produzir efeitos jurídicos relevantes ou impactarem os indivíduos de maneira significativa. Neste aspecto, depreende-se que a regulação é calibrada de acordo com os potenciais riscos do contexto de aplicação da tecnologia. Medidas gerais e específicas de governança são distintamente estabelecidas para sistemas de inteligência artificial com qualquer grau de risco e para aqueles categorizados como de alto risco.

A proposição estabelece a exigência de avaliação preliminar dos riscos da inteligência artificial, definindo as aplicações vedadas por risco excessivo e aplicações de alto risco sujeitas a normas de controle mais rigorosas.

Quanto à governança dos sistemas, o projeto elenca medidas para garantir transparência, mitigação de vieses e estabelece medidas adicionais para sistemas de alto risco e

sistemas governamentais de inteligência artificial. Também normatiza o procedimento para avaliação de impacto algorítmico.

O texto aborda as regras de responsabilização civil integral envolvendo sistemas de inteligência artificial, com exclusão das hipóteses em que os responsáveis pelo desenvolvimento e utilização desses sistemas não seriam responsabilizados. A responsabilidade civil é graduada de acordo com o risco imposto pelo sistema. Em sistemas de alto risco ou risco excessivo, os responsáveis respondem objetivamente pelos danos causados, na medida da participação de cada um no dano. Em sistemas que não sejam de alto risco, a culpa do agente causador do dano é presumida, aplicando-se a inversão do ônus da prova em favor da vítima.

A proteção contra a discriminação é reforçada por meio de diversos instrumentos, como o direito à informação, compreensão, contestação e correção de vieses discriminatórios. O texto também qualifica a discriminação direta e indireta e dá atenção especial a grupos (hiper)vulneráveis tanto na definição de sistemas de alto risco como no fortalecimento de certos direitos.

No que diz respeito à fiscalização da inteligência artificial, o projeto determina que o Poder Executivo designe uma autoridade responsável pelo cumprimento das normas estabelecidas. As competências dessa autoridade são especificadas e são estabelecidas sanções administrativas.

O projeto também prevê medidas para fomentar a inovação da inteligência artificial, incluindo a criação de um ambiente regulatório experimental (sandbox regulatório). Ele combina disposições *ex-ante* e *ex-post*, definindo critérios para avaliação e ação a serem tomadas para mitigar os riscos envolvidos. Também envolve os setores interessados no processo regulatório por meio da corregulação.

Alinhado com o direito internacional, o projeto estabelece diretrizes para conformar direitos autorais e de propriedade intelectual à ideia de que os dados devem ser um bem comum, devendo circular para treinamento de máquinas e desenvolvimento de sistemas de inteligência artificial sem prejudicar os titulares desses direitos. Assim, são considerados os desdobramentos da regulação na promoção da inovação.

Em termos concretos, a proposição do marco legal da IA (BRASIL, 2022, Relatório Final) encampa a ideia de que todos os sistemas de IA deverão ser pautados e justificados nos seguintes princípios (BRASIL, 2023, PL 2338/2023, art. 3º):

> i. crescimento inclusivo, desenvolvimento sustentável e bem-estar;
> ii. autodeterminação e liberdade de decisão e de escolha;
> iii. participação humana no ciclo da inteligência artificial e supervisão humana efetiva;
> iv. não discriminação;
> v. justiça, equidade e inclusão;
> vi. transparência, explicabilidade, inteligibilidade e auditabilidade;
> vii. confiabilidade e robustez dos sistemas de inteligência artificial e segurança da informação;
> viii. devido processo legal, contestabilidade e contraditório;
> ix. rastreabilidade das decisões durante o ciclo de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica;
> x. prestação de contas, responsabilização e reparação integral de danos;
> xi. prevenção, precaução e mitigação de riscos sistêmicos derivados de usos intencionais ou não intencionais e efeitos não previstos de sistemas de inteligência artificial; e
> xii. não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas dos sistemas de inteligência artificial.

Assim, fica evidente a interseção entre a definição técnica dos sistemas de IA e as premissas normativas propostas no marco legal. Essas questões são discutidas neste trabalho, especialmente em relação ao equilíbrio sistêmico com a LGPD e a proteção do segredo de negócios, que são aspectos centrais do estudo

6.3.1 Devido processo informacional e a proteção dos direitos básicos das pessoas afetadas por sistemas de IA[459]

[459] O processo informacional, ao que se infere da proposição constante do Relatório Final, iniciar-se-ia em momento anterior ao tratamento de dados (v. definição art. 5º da LGPD), visto que a pessoa afetada terá – idealmente – direito a ser previamente informada de suas interações com os sistemas de IA. V. Minuta de Substitutivo (cf. Anexo), cuja leitura deverá ser integrada com o art. 3º: "Art. 3º O desenvolvimento, implementação e uso de sistemas de inteligência artificial observarão a boa-fé e os seguintes princípios: I – crescimento inclusivo, desenvolvimento sustentável e bem-estar; II – autodeterminação e liberdade de decisão e de escolha; III – participação humana no ciclo da inteligência artificial e supervisão humana efetiva; IV – não discriminação; V – justiça, equidade e inclusão; VI – transparência, explicabilidade, inteligibilidade e auditabilidade; VII – confiabilidade e robustez dos sistemas de inteligência artificial e segurança da informação; VIII – devido processo legal, contestabilidade e contraditório; IX – rastreabilidade das decisões durante o ciclo

Conceitualmente, uma abordagem possível para aproximar os dados pessoais do segredo de negócios parece estar na privacidade. Antes das leis de proteção de dados pessoais não surgiam questões importantes em relação à inclusão desses dados (por exemplo, uma "lista de clientes") como parte das "informações ou dados confidenciais utilizados na indústria, comércio ou prestação de serviços", conforme inferido da Lei de Propriedade Industrial nacional (LPI ou Lei 9279/1998: art. 195, incisos XI e XII).

A questão da privacidade apresenta diferentes nuances no mundo "analógico" e no mundo "digital", e a partir dessas percepções o conceito de privacidade foi reinterpretado, passando de proteção da intimidade e do "direito de estar só" para o de controle do fluxo de informações (pessoa-informação-circulação-controle)[460].

Foi nesse contexto que a observação de Danilo Doneda (2021, p.40) parece se aplicar especificamente à propriedade intelectual. Segundo Doneda, o instituto não está imune à nova lógica do fluxo de informações, uma vez que suas estruturas foram afetadas por uma nova maneira de lidar com conteúdo e proteger os direitos das pessoas afetadas por eles. Normas e técnicas estão sendo criadas, e dependendo de como forem implementadas pela indústria e aceitas no mercado podem restringir a circulação de informações nos meios eletrônicos.

Na realidade, as leis gerais de proteção de dados pessoais não têm impedido o fluxo dessas informações, que teoricamente deveriam ser protegidas. Isso ocorre porque muitos negócios têm permissão para avaliar o perfil comportamental de seus clientes e obter outras informações necessárias para suas atividades econômicas, como prevenção de fraudes, previsão de receita e saúde financeira da empresa.

Isso explica o clamor da sociedade por melhorias no sistema jurídico, a fim de corrigir a assimetria informacional entre os atores envolvidos nessa interação inevitável entre segredos comerciais e proteção de dados pessoais. Essa tensão é evidente no processo explicativo exigido para as tomadas de decisões automatizadas, conforme estabelecido no artigo 20 da LGPD

No bojo do debate público com vista a elaboração de minuta de substitutivo da propositiva legislativa do marco de legal da IA, tem-se o interessante argumento – que se atribui

---

de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica; X – prestação de contas, responsabilização e reparação integral de danos; XI – prevenção, precaução e mitigação de riscos sistêmicos derivados de usos intencionais ou não intencionais e efeitos não previstos de sistemas de inteligência artificial; e XII – não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas dos sistemas de inteligência artificial."

[460] DONEDA (2021).

a João Sérgio dos Soares Pereira (BRASIL, 2022, Relatório Final)[461] - em torno da necessidade de observância dos direitos fundamentais, especificamente relacionado com as garantias do devido processo

Com efeito, na opinião do especialista, é preciso ter em mente que, para o Direito, o conteúdo das respostas e das decisões (por hipótese, automatizadas) importam, na medida em que no Estado Democrático de Direito vigente no País o devido processo não abrange apenas a necessidade de eficiência, como também do resguardo de uma resposta adequada ao Ordenamento, um justo procedimento que englobe a participação dos interessados.

Nesse sentido, o especialista argumenta que uma decisão opaca, ininteligível ou incompreendida pelos destinatários vai contra a dignidade da pessoa humana, abalando os fundamentos da República (Constituição Federal de 1988, art. 1º-III). Portanto, é necessário evitar que sistemas de aplicação tecnológica desconsiderem as diversas perspectivas do ser humano, levando em conta sua pluralidade, diversidade cultural e contextos.

À primeira leitura, parecem que tais preocupações iluminaram o encaminhamento de algumas das proposições normativas em curso - aquelas com vistas à regulação do desenvolvimento e a aplicação da inteligência artificial (IA), no País, especialmente.

Nota-se, nesse sentido, que as disposições gerais do Capítulo II ("Dos Direitos", Artigo 5º) da Minuta do Substitutivo (Relatório Final, 2022) estabelecem, de um lado, os direitos das pessoas afetadas por sistemas de IA, especialmente os concernentes à informação prévia quanto às suas interações com essas sistemas (v. também Art. 7º)[462]; a explicação sobre a decisão,

[461] Da contribuição escrita de João Sérgio dos Santos Soares Pereira, no Relatório Final (BRASIL, 2022), tem-se destaque para o seguinte trecho: "(...) *no mundo jurídico, para o Direito, não é possível admitir respostas ou decisões rápidas, céleres, sem se preocupar com o conteúdo delas. Ou seja, este conteúdo importa, pois, no Estado Democrático de Direito brasileiro, o devido processo não abrange apenas a necessidade de eficiência, mas também do resguardo de uma resposta adequada à Constituição, um procedimento justo que engloba a participação dos interessados, sua visão, interferência, consideração. Só assim a resposta estatal ganha relevo justificativo deontológico. Sob o ponto, a devida explicação da decisão, e o resguardo para que não se torne opaca (ininteligível, incompreendida por seus destinatários) garante a dignidade da pessoa humana, enquanto um dos fundamentos da República, na forma do artigo 1º, III da Constituição de 1988, pois é impossível imaginar qualquer sistema de aplicação tecnológica que não valorize o ser humano em sua perspectiva plural, cultural e poli contextual. Como saber se os requisitos constitucionais foram respeitados se não há a possibilidade do controle democrático sobre a decisão administrativa proferida? Os órgãos estatais, o Poder Público, só podem e devem ser reconhecidos como elemento de Estado Democrático, como tal, se substituirmos o código algorítmico pelo código da eticidade e cultura preliminar de confiança e promoção de políticas públicas adequadas de fomento à responsabilidade na formulação e construção das bases de dados e variáveis usadas para a tomada da decisão*".

[462] Minuta de Substitutivo (v. Anexo): "Art. 7º Pessoas afetadas por sistemas de inteligência artificial têm o direito de receber, previamente à contratação ou utilização do sistema de inteligência artificial, informações

recomendação ou previsão tomada por sistemas de IA (v. Art. 8º)[463]; ao de contestar decisões ou previsões de IA, inclusive de intervenção humana, que produzam efeitos jurídicos ou que impactem de maneira significativa seus interesses (v. Art.9º e Art. 11)[464]; ao de participar nas decisões de IA, a depender do contexto e do estado de arte da tecnologia (Art. 5º- IV); ao de não ser discriminado e ter corrigido os vieses discriminatórios diretos, indiretos, ilegais ou abusivos (v. Art. 10)[465]; à privacidade e à proteção de dados pessoais, nos termos legais (Art.

---

claras e adequadas quanto aos seguintes aspectos: I - caráter automatizado da interação e da decisão em processos ou produtos que afetem a pessoa; II - descrição geral do sistema, tipos de decisões, recomendações ou previsões que se destina a fazer e consequências de sua utilização para a pessoa; III - identificação dos operadores do sistema de inteligência artificial e medidas de governança adotadas no desenvolvimento e emprego do sistema pela organização; IV - papel do sistema de inteligência artificial e dos humanos envolvidos no processo de tomada de decisão, previsão ou recomendação; IV - categorias de dados pessoais utilizados no contexto do funcionamento do sistema de inteligência artificial; V - medidas de segurança, de não-discriminação e de confiabilidade adotadas, incluindo acurácia, precisão e cobertura; e VI - outras informações definidas em regulamento. § 1º Sem prejuízo do fornecimento de informações de maneira completa em meio físico ou digital aberto ao público, a informação referida no inciso *I do caput* deste artigo será também fornecida, quando couber, com o uso de ícones ou símbolos facilmente reconhecíveis. *§ 2°* Pessoas expostas a sistemas de reconhecimento de emoções ou a sistemas de categorização biométrica serão informadas sobre a utilização e o funcionamento do sistema no ambiente em que ocorrer a exposição. *§ 3°* Os sistemas de inteligência artificial que se destinem a grupos vulneráveis, tais como crianças, adolescentes, idosos e pessoas com deficiência, serão desenvolvidos de tal modo que essas pessoas consigam entender o seu funcionamento e seus direitos em face dos agentes de inteligência artificial."

[463] Minuta de Substitutivo (v. Anexo): "Art. 8º A pessoa afetada por sistema de inteligência artificial poderá solicitar explicação sobre a decisão, previsão ou recomendação, com informações a respeito dos critérios e dos procedimentos utilizados, assim como sobre os principais fatores que afetam tal previsão ou decisão específica, incluindo informações sobre: I- a racionalidade e a lógica do sistema, bem como o significado e as consequências previstas de tal decisão para a pessoa afetada; II - o grau e o nível de contribuição do sistema de inteligência artificial para a tomada de decisões; III - os dados processados e a sua fonte, bem como os critérios para a tomada de decisão e, quando apropriado, a sua ponderação, aplicados à situação da pessoa afetada; IV - os mecanismos por meio dos quais a pessoa pode contestar a decisão; e V - a possibilidade de solicitar intervenção humana, nos termos desta lei. Parágrafo único. As informações mencionadas no *caput* serão fornecidas por procedimento gratuito e facilitado, em linguagem que permita que a pessoa compreenda o resultado da decisão ou previsão em questão, no prazo de até quinze dias a contar da solicitação, permitida prorrogação, uma vez, por igual período, a depender da complexidade do caso."

[464] Minuta de Substitutivo (v. Anexo): "Art. 9º A pessoa afetada por sistema de inteligência artificial terá o direito de contestar e de solicitar a revisão de decisões, recomendações ou previsões geradas por tal sistema que produzam efeitos jurídicos relevantes ou que impactem de maneira significativa seus interesses. § 1º Fica assegurado o direito de correção de dados incompletos, inexatos ou desatualizados utilizados por sistemas de inteligência artificial, assim como o direito de solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação, nos termos do art. 18 da Lei nº 13.709, de 14 de agosto de 2018 e da legislação pertinente. *§ 2°* O direito à contestação previsto no *caput* deste artigo abrange também decisões, recomendações ou previsões amparadas em inferências discriminatórias, irrazoáveis ou que atentem contra a boa-fé objetiva, assim compreendidas as inferências que: I - sejam fundadas em dados inadequados ou abusivos para as finalidades do tratamento; II - sejam baseadas em métodos imprecisos ou estatisticamente não confiáveis; ou III - não considerem de forma adequada a individualidade e as características pessoais dos indivíduos. Art. 11. Em cenários nos quais as decisões, previsões ou recomendações geradas por sistemas de inteligência artificial tenham um impacto irreversível ou de difícil reversão ou envolvam decisões que podem gerar riscos à vida ou à integridade física de indivíduos, haverá envolvimento humano significativo no processo decisório e determinação humana final."

[465] Minuta de Substitutivo (v. Anexo): "Art. 10. Quando a decisão, previsão ou recomendação de sistema de inteligência artificial produzir efeitos jurídicos relevantes ou que impactem de maneira significativa os interesses da pessoa, inclusive por meio da geração de perfis e da realização de inferências, esta poderá solicitar a intervenção ou revisão humana. Parágrafo único. A intervenção ou revisão humana não será exigida caso a sua

5º- VI).

Além disso, há prescrições que obrigam os agentes de inteligência artificial a fornecer informações claras e facilmente acessíveis sobre os procedimentos necessários para exercer esses direitos (Art. 5º, Parágrafo Único), com a ressalva de que a defesa desses interesses e direitos pode ser exercida em juízo ou perante órgãos administrativos competentes, individualmente ou coletivamente, de acordo com as disposições específicas dos instrumentos de proteção individual, coletiva e difusa (Art. 6º).

Em suma, em uma análise preliminar, a proposta legislativa parece refletir a presença dos elementos básicos para concretizar o processo informacional, conforme discutido pela doutrina mencionada nas seções anteriores.

6.3.2 Inovação e propriedade intelectual

No âmbito do debate público (BRASIL, 2022, Relatório Final) , sinaliza-se não se vislumbrar possível *trade off* entre a proteção de dados e os novos desenvolvimentos no âmbito dos sistemas de IA, opções essas não excludentes em relação aos direitos fundamentais relacionados com a proteção dos dados pessoais (Constituição Federal, Artigo 5º, LXXIX, acrescentado pela EC 115/2022).

Como se viu, atribui-se à IA a possibilidade de utilização massiva dos dados pessoais para a análise, previsão e influência de comportamentos humanos, o que transforma os dados e as informações tecnológicas em mercadorias valiosas.

A IA permite a tomada de decisão automatizada mesmo em face dos múltiplos fatores envolvidos em que as escolhas são complexas.

Dentre os muitos riscos, é certo que as decisões automatizadas por sistemas de IA ainda podem se equivocadas e até discriminatórias, com a potencialidade de reproduzir preconceitos humanos, ou mesmo induzindo a novas escalas de discriminação.

Haverá casos em que as decisões automatizadas mostrem-se justas e corretas porém igualmente problemática por afetar negativamente os indivíduos, mesmo assim nada afasta a

---

implementação seja comprovadamente impossível, hipótese na qual o responsável pela operação do sistema de inteligência artificial implementará medidas alternativas eficazes, a fim de assegurar a reanálise da decisão contestada, levando em consideração os argumentos suscitados pela pessoa afetada, assim como a reparação de eventuais danos gerados."

possibilidade de que sejam usadas técnicas de manipulação e de vigilância continuada.

De outro lado, o marco legal da IA também focaria na criação de condições para que a IA prospere, e, para isso, é preciso viabilizar o processamento de quantidades massivas de dados sobre os indivíduos, em proveito do aprimoramento desses sistemas.

Ademais, o processamento massivo de dados em princípio poderá oferecer oportunidade para conhecimento da sociedade, de melhor governança, embora se corra os riscos extremos ainda não determináveis, que idealmente a regulação poderia evitar.

Com essas digressões, volta-se ao exame do Relatório Final (BRASIL, 2022) no que concerne à Inovação e Propriedade Intelectual declaradamente alinhada com as diretrizes internacionais, tendentes a conferir aos direitos autorais interpretação ajustada à noção de que os dados devem ser um "bem comum", de sorte a permitir a sua circulação para o treinamento de máquina e o desenvolvimento de sistema de inteligência artificial, com o destaque de que tal permissivo não implicaria prejuízo aos titulares desses direitos.

Como se depreende do artigo 42[466] da proposição (BRASIL, 2022, Relatório Final), o objetivo é instrumentalizar a regulação com mecanismos de estímulos à inovação tecnológica.

Nesse sentido, a teor da Minuta de Substitutivo (BRASIL, 2022, Relatório Final), sugere-se inclusão de ressalva expressa no sentido de que "a atividade de mineração de dados por organizações e instituições de pesquisa, jornalismo e por museus, arquivos e bibliotecas, bem como por outros atores em situações específicas, não viola direitos autorais", para o que seria preciso considerar a efetiva finalidade e observar o cumprimento de requisitos de convenções internacionais aos quais o País tenha aderido.

---

[466] Eis redação proposta, nesse particular: "Art. 42. Não constitui ofensa a direitos autorais a utilização automatizada de obras, como extração, reprodução, armazenamento e transformação, em processos de mineração de dados e textos em sistemas de inteligência artificial, nas atividades feitas por organizações e instituições de pesquisa, de jornalismo e por museus, arquivos e bibliotecas, desde que: I- não tenha como objetivo a simples reprodução, exibição ou disseminação da obra original em si; II - o uso ocorra na medida necessária para o objetivo a ser alcançado; III - não prejudique de forma injustificada os interesses econômicos dos titulares; e IV - não concorra com a exploração normal das obras. § 1º Eventuais reproduções de obras para a atividade de mineração de dados serão mantidas em estritas condições de segurança, e apenas pelo tempo necessário para a realização da atividade ou para a finalidade específica de verificação dos resultados da pesquisa científica. § 2º Aplica-se o disposto no caput à atividade de mineração de dados e textos para outras atividades analíticas em sistemas de inteligência artificial, cumpridas as condições dos incisos do *caput* e do § 1º, desde que as atividades não comuniquem a obra ao público e que o acesso às obras tenha se dado de forma legítima. § 3º A atividade de mineração de textos e dados que envolva dados pessoais estará sujeita às disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)." (BRASIL, 2022)

6.3.3 Responsabilização

Liberdade e responsabilidade. Com essa dualidade a proposição aparentemente pretendeu afastar uma possível e pretensa imunidade dos sistemas ditos autônomos em relação à responsabilidade civil, optando por um regime que alcance tanto o fornecedor quanto o operador de sistema de IA.

A proposição sugere duas categorizações centrais de riscos: a de risco excessivo e a de alto risco. A categoria de risco excessivo indica que o sistema não pode operar, tendo a sua utilização vedada pela legislação brasileira.

Na categoria de alto risco leva-se em conta as finalidades dos sistemas que acarretem elevado risco aos direitos fundamentais dos cidadãos e à coletividade de uma forma geral e condiciona o funcionamento do sistema a um maior número de obrigações, sem as quais reputa-se não legítimo e inadequado, e, porque não dizer, ilícito.

No entanto, considerando as percepções estabelecidas ao longo deste estudo, embora o debate em torno da regulação da IA tenda a deslegitimar o tratamento de dados pessoais envolvidos em riscos excessivos[467], deve-se levar em consideração que esse aspecto negativo pode ser superado factualmente se o avanço tecnológico permitir a efetiva anonimização dos dados pessoais. Nesse caso, a regulação de proteção (LGPD: art. 5 III e Art. 12) [468] não seria aplicável devido à exclusão dos dados anonimizados do conceito de dados pessoais.

---

[467] Exposição de Motivosmotivos de Substitutivo:substitutivo (BRASIL, 2022): "Seguindo a lógica da dosagem proporcional da intervenção regulatória às externalidades negativas de um sistema de inteligência artificial, listam-se, ainda, as chamadas hipóteses de riscos excessivos. Isto é, situações em que se veda o uso da tecnologia por estarem em jogo direitos inegociáveis, como é o caso de indução de comportamentos lesivos à segurança e integridade física e, em sentido mais amplo, prejudiciais à autodeterminação, como nos casos do chamado *social scoring* – ranqueamento e atribuição de notas universais para o acesso a bens e serviços e políticas públicas. Sistemas de identificação biométrica à distância de forma contínua e em espaços acessíveis ao público, por sua vez, pela elevada periculosidade indicada em múltiplas contribuições recebidas por esta Comissão, passam a depender de lei federal específica, que deve atender aos requisitos estabelecidos na proposta".

[468] LGPD: art. 5"artArt. 5º (...) -III - dado anonimizado: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; ;"
"Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.."

Em suma, prosseguem os esforços para calibrar a norma de acordo com o grau de risco percebido em relação aos sistemas de IA. Nesse aspecto, a Proposição (BRASIL, 2022) sugere uma diferenciação em seu Capítulo V (responsabilidade civil). Quando se tratar de sistemas de IA de alto risco [469] ou risco excessivo [470], tanto o fornecedor quanto o operador serão objetivamente[471] responsáveis pelos danos causados, levando em conta a participação de cada um no dano. Já quando se tratar de IA que não seja de alto risco, a culpa do responsável pelo dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima.

6.3.4 Rastreabilidade, documentação e auditoria (governança dos sistemas de IA).

Admitir que a IA "não é controlável" implicaria atribuir um caráter místico a essas tecnologias. Esse discurso, que tende a personificar o aparato tecnológico, não foi aceito no

[469] Alto risco: "Art. 17. São considerados sistemas de inteligência artificial de alto risco aqueles utilizados para as seguintes finalidades: I - aplicação como dispositivos de segurança na gestão e no funcionamento de infraestruturas críticas, tais como controle de trânsito e redes de abastecimento de água e de eletricidade; II- educação e formação profissional, incluindo sistemas de determinação de acesso a instituições de ensino e de formação profissional ou para avaliação e monitoramento de estudantes; III - recrutamento, triagem, filtragem, avaliação de candidatos, tomada de decisões sobre promoções ou cessações de relações contratuais de trabalho, repartição de tarefas e controle e avaliação do desempenho e do comportamento das pessoas afetadas por tais aplicações de inteligência artificial nas áreas de emprego, gestão de trabalhadores e acesso ao emprego por conta própria; IV - avaliação de critérios de acesso, elegibilidade, concessão, revisão, redução ou revogação de serviços privados e públicos que sejam considerados essenciais, incluindo sistemas utilizados para avaliar a elegibilidade de pessoas naturais quanto a prestações de serviços públicos de assistência e de seguridade; V - avaliação da capacidade de endividamento das pessoas naturais ou estabelecimento de sua classificação de crédito; VI - envio ou estabelecimento de prioridades para serviços de resposta a emergências, incluindo bombeiros e assistência médica; VII - administração da justiça, incluindo sistemas que auxiliem autoridades judiciárias na investigação dos fatos e na aplicação da lei; VIII - veículos autônomos, quando seu uso puder gerar riscos à integridade física de pessoas; IX - aplicações na área da saúde, inclusive as destinadas a auxiliar diagnósticos e procedimentos médicos; X - sistemas biométricos de identificação; XI - investigação criminal e segurança pública, em especial para avaliações individuais de riscos pelas autoridades competentes, a fim de determinar o risco de uma pessoa cometer infrações ou de reincidir, ou o risco para potenciais vítimas de infrações penais ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos; XII - estudo analítico de crimes relativos a pessoas naturais, permitindo às autoridades policiais pesquisar grandes conjuntos de dados complexos, relacionados ou não relacionados, disponíveis em diferentes fontes de dados ou em diferentes formatos de dados, no intuito de identificar padrões desconhecidos ou descobrir relações escondidas nos dados; XIII - investigação por autoridades administrativas para avaliar a credibilidade dos elementos de prova no decurso da investigação ou repressão de infrações, para prever a ocorrência ou a recorrência de uma infração real ou potencial com base na definição de perfis de pessoas singulares; XIV - gestão da migração e controle de fronteiras;"

[470] Risco excessivo: "Art. 14. São vedadas a implementação e uso de sistemas de inteligência artificial: I - que empreguem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança ou contra os fundamentos deste lei; II - que explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como associadas à sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma prejudicial à sua saúde ou segurança ou contra os fundamentos desta lei; III - pelo poder público, para avaliar, classificar ou ranquear as pessoas naturais, com base no seu comportamento social ou em atributos da sua personalidade, por meio de pontuação universal, para o acesso a bens e serviços e políticas públicas, de forma ilegítima ou desproporcional."

[471] Como se sabe, a responsabilidade objetiva ("sem culpa") é objeto de disposição expressa do art. 927, parágrafo único, do Código Civil (Lei nº 10.406, de 2002): "Art. 927. Aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem."

debate público do País. Como mencionado na seção anterior, a opção legislativa é definir um regime abrangente de imputação de responsabilidade civil tanto para o fornecedor quanto para o operador desses sistemas de IA. Isso eliminaria qualquer dúvida sobre a responsabilização desses agentes quando causarem danos, independentemente do grau de autonomia do sistema de IA que utilizam.

Uma IA incontrolável parece não se compatibilizar com o "dever de cuidado" (em sentido amplo) estabelecido no âmbito da própria tutela do segredo dos negócios, que, como já afirmado, foi condicionado ao cumprimento de deveres (*rectus*: ônus) razoáveis desse cuidado, materializáveis em procedimentos de governança, dentre os quais a auditoria[472] , que em princípio consubstanciaria *ato normal*[473] de gestão inerente à atividade empresarialmente organizada, indistintamente se endereçados aos respectivos ativos "tangíveis" e "intangíveis", o que inclui os artefatos autônomos ("autômatos") e os conhecimentos tecnológicos neles embarcados.

Para a Ciência da Administração, como qualquer bem "intangível", os dados são em princípio considerados um ativo organizacional (acepção de um conjunto de bens), em relação aos quais o agente econômico normalmente tem (deveria ter) preocupação com as boas práticas de gestão como aquelas orientadas na obtenção de lucros da atividade, as relacionadas com a performance geral da empresa (incluída a gestão reputacional) ou ainda as voltadas ao atendimento às exigências regulatórias[474].

A auditoria é um dos mecanismos de governança importantes na atividade econômica voltada para o tratamento de dados. Ela se concentra na rastreabilidade dos dados e informações gerados na extração, transformação e geração de dados, e é necessário verificar se os dados no sistema de origem estão corretos (AMARAL, 2016)[475].

---

[472] "De modo simples, podemos definir auditoria como o procedimento para averiguar a eficiência de atividades ou processos. Dessa forma, a ideia da auditoria é avaliar, de forma objetiva e independente, se os processos atendem os padrões definidos. Por isso, o procedimento em si é abrangente — com as devidas adaptações, ele pode ser adotado em diferentes departamentos e empresas. Entretanto, independente do contexto, o que não muda, é o objetivo geral da auditoria: verificar se os processos da instituição seguem os padrões definidos e investigar se há possíveis falhas, que possam comprometer os resultados". (TSUKADA, 2021)

[473] A partir do conceito de *ato normal de gestão* do Direito Comercial, Marco Aurélio GRECO (1998, p.100,101, 102) define o ato "anormal" de gestão como aquele que fuja do padrão rotineiro da vida da empresa. Raciocina que se existem atos regulares, também haverá de existir os irregulares e os atos anormais de gestão, lembrando que a ideia há de se aplicar no direito moderno, cuja centralidade não é mais a do dano mas sim a do risco da atividade empresarial.

[474] AMARAL, 2016, p. 135.

[475] AMARAL, 2016, p. 144.: "Além das etapas normais de um processo de geração de dados (extrair,

Se concebida a governança (na perspectiva do agente de tratamento de dados) como ato normal de gestão, então as medidas técnicas e/ou administrativas são indissociáveis da regular atividade de tratamento de dados pessoais. Nesse contexto, a auditoria passaria pela rastreabilidade dos dados e informações gerados na extração, transformação e geração de dados, cujos conteúdo devem portanto ser passíveis de verificação. Assim, é possível especular que o conceito de documentação [476] poderia (rectus: deveria) estar alinhado com os objetivos regulatório de escrutínio individual e social da IA[477], escopos esses amparados no princípio da contestabilidade e da explicabilidade [478] da tomada de decisão automatizada que afete significativamente direitos e liberdades dos indivíduos aos quais os dados se referem.

Portanto, a governança do tratamento de dados pessoais, incluindo a auditoria, é fundamental para a proteção dos direitos individuais. A documentação dos sistemas de IA e a transparência na tomada de decisões automatizadas são conceitos que se alinham aos objetivos regulatórios de escrutínio individual e social da IA. A auditabilidade também é relevante tanto na Lei Geral de Proteção de Dados quanto na proteção do segredo de negócios. A regulação deve calibrar as exigências de controle, documentação e avaliação de acordo com os riscos envolvidos no uso da IA.

De acordo com HOFFMANN-RIEM (2021, p.244), uma boa governança não acontece automaticamente e requer complementações éticas, morais e comportamentais dos

---

transformar, gerar), obrigações acessórias devem ter obrigatoriamente uma etapa complementar: auditoria. A auditoria se refere ao conteúdo dos arquivos gerados, e não do processo em si. Uma obrigação acessória é uma confissão eletrônica, e tem intrinsecamente um risco associado. Afinal, a informação que está sendo transmitida pelo arquivo é correta, íntegra, completa e precisa? A auditoria neste contexto tem uma característica diferenciada: não basta certificar que a extração e transformação de dados foi executada corretamente gerando informação de qualidade, é preciso também averiguar se os dados, no sistema de origem, estão corretos, o que nos leva a um processo de verificação paralela".

[476] O conceito de documento, em aspectos jurídico-funcionais, associa-se, ao nosso entendimento, com o objeto dos atos processuais disciplinados nos art. 369 e 400 do Código de Processo Civil (Lei 13.105/2015), este último relacionado ao procedimento instrutório de exibição de documento ou coisa, no âmbito judicial.

[477] Nota 144 do Relatório Final (BRASIL, 2022): Diego Machado considerou que "a previsão de deveres de registro e documentação não está clara no projeto de lei como está no Congresso Nacional", destacando que existe "a necessidade de termos registros de documentação, (...) como são desenvolvidos esses sistemas, durante toda a criação, a concepção, o treinamento, o desenvolvimento (...) e a sua execução." Da mesma forma, Fernanda Viegas sugeriu regulação sobre a questão da documentação dos sistemas". Para Hoffmann-Riem, a eficácia da governança passa pela "obrigação de registrar/documentar certos usos também deve ser considerada aqui. Exemplos de campos para obrigações de documentação referentes aos critérios de decisão utilizados seriam perfilagem e pontuação, por exemplo, ao calcular as taxas de seguro ou ao decidir sobre a concessão de um empréstimo. Limitações nas opções de armazenamento também seriam importantes."

[478] V. Nota 143 do Relatório Final, a reflexão que oferece Nina Horta: "(...) a explicabilidade para o jornalismo é uma coisa, mas, para o direito, é outra e, para a computação, é outra, (...). Mas e a sociedade? (...) uma das questões que precisaria ser discutida, antes de pensar a regulamentação, é pensar como você inclui a sociedade nesse debate. (...) a tradução correta do que a gente está falando, do que a gente está propondo (...) se encaixa muito mais no contexto brasileiro de explicabilidade e transparência. Então, não seria só documentação."

destinatários. Cabe ao Estado criar leis que possibilitem e estimulem a boa governança digital. No entanto, garantir a transparência, responsabilidade e auditabilidade adequadas em relação aos sistemas de IA apresenta desafios, pois as garantias de transparência podem interferir na proteção dos segredos comerciais. A divulgação do projeto tecnológico e dos sistemas algorítmicos pode afetar a liberdade de organização das empresas e o interesse legítimo de proteger seus conhecimentos.

Dado que as diretrizes éticas, por si só, seriam insuficientes na tarefa de prevenir os riscos associados à digitalização em geral e ao uso da IA em particular, trona-se necessária uma lei estatal ancorada em sanções que confiram eficácia aos padrões éticos a ser nela positivados (p. 250), notadamente aqueles relacionados com a boa governança "durante o desenvolvimento" de sistemas algorítmicos – *Governance of Algorithms* – e "também durante sua aplicação" – *Governance by Algorithms*.

Todavia, repita-se, eventual imposição de obrigação abstrata de divulgação do projeto tecnológico e dos sistemas algorítmicos utilizados interferiria sensivelmente na liberdade de organização (autonomia) das empresas, afetando o seu legítimo interesse de impedir que os algoritmos sejam apropriados por concorrentes, que os utilizariam como *free riders*, ou por outras pessoas que decerto utilizariam esses conhecimentos para seus propósitos específicos, *a priori* não determináveis.

De outro lado, a divulgação se justificaria, em casos concretos, com base em interesses de igual ou maior estatura do que o segredo de negócios.

Resulta daí, então, que a transparência e o controle teriam que ser assegurados em relação aos algoritmos cuja utilização possa prejudicar a proteção dos direitos fundamentais, especialmente contra a discriminação, estigmatização e manipulação. Nesse ponto corroboram os desenvolvimentos ao longo da seção 6.2, retro.

Portanto, coloca-se a questão da necessidade de um procedimento adequado para a tutela dos direitos e interesses em potencial colisão, tudo sob supervisão de uma autoridade de proteção.

Nesse sentido, HOFFMANN-RIEM (2021, p. 248) argumenta que dada a multiplicidade de direitos e de interesses envolvidos (que vão além daqueles implicados com o segredo de negócios e proteção dos dados pessoais), "faz sentido recorrer às autoridades de proteção de

dados existentes para a tarefa de supervisão". Observa, neste particular, que tal autoridade de proteção deveria ter poderes suficientes a tais misteres e pessoal quantitativa e qualitativamente adequados para o exercício das respectivas competências.

Em contexto de tecnologias de IA, entende o autor que "seria preferível criar uma instituição especializada em monitorar não apenas, mas acima de tudo, a IA, e possivelmente com jurisdição nacional ou mesmo comunitária, como uma agência digital".

Nesse ponto, o autor recorre a Andrew TUTT (2017, p. 85)[479], para quem seria adequada a criação de uma autoridade que deveria ser tão poderosa quanto a Administração Federal de Drogas (FDA) estadunidense, com incumbências que iriam para além do monitoramento, para se encarregar do desenvolvimento de normas (*Performance Standards*, *Design Standards*, *Liability Standards*) ou, no mínimo, envolver-se no respectivo desenvolvimento.

Concorda-se com HOFFMANN-RIEM (2021, p. 248, Op. Cit.) quanto ao fato de que, para superação desses desafios de governança dos sistemas de IA, é essencial recorrer-se à expertise e envolvimento da sociedade civil, para além da expertise da comunidade jurídica e técnica; e, não só, provavelmente serão igualmente necessários "novos conceitos, acordos e instituições de governança transnacional, que devem ser orientados para a cooperação entre os atores públicos e os interessados envolvidos" (ibidem, p. 250-251).

Em suma, a transparência e o controle devem ser assegurados quando os algoritmos utilizados afetarem a proteção dos direitos fundamentais. Também, é necessária a criação de um procedimento adequado para conciliar esses interesses, sob a supervisão de uma autoridade de proteção de dados com poderes suficientes. Pode ser necessário estabelecer uma agência especializada em monitorar a IA, desenvolver normas e garantir a conformidade. Além disso, a expertise da sociedade civil e a cooperação entre os atores públicos e interessados serão essenciais para enfrentar os desafios da governança da IA.

[479] TUTT, 2017, pp. 83 ss. *apud* HOFFMANN-RIEM, 2021, p. 363.

6.4 RESULTADO PROVISÓRIO: DIÁLOGO ABERTO[480][481]

Em 2016, ao avaliar as dificuldades na identificação de um ponto de equilíbrio entre direitos de proteção de dados pessoais e direitos de segredos comerciais sobre informações de clientes no quadro da União Europeia (UE), Gianclaudio Malgieiri atribui tal estado de coisas à vagueza e a um suposto estado de esquizofrenia da regulação local (MALGIERI, 2016; v. também Seção 3.2).

No ano de 2023, em carta aberta, subscrita e divulgada na mídia global, um grupo de empresários e seus especialistas[482] solicitam um prazo de seis meses de suspensão de novos desenvolvimentos da inteligência artificial (IA), por eles considerado necessário[483] para que a sociedade pudesse se adaptar a essas novas tecnologias, mediante instituição de mecanismos estatais de controle e de transparência endereçados aos desenvolvedores dessas tecnologias.

O registro do fato, aparentemente não superado, ilustra de forma abrangente a

---

[480] "*Diálogo' porque há influências recíprocas, 'diálogo' porque há aplicação conjunta das duas normas ao mesmo tempo e ao mesmo caso, seja complementarmente, seja subsidiariamente, seja permitindo a opção pela fonte prevalente ou mesmo permitindo uma opção por uma das leis em conflito abstrato - solução flexível e aberta, de interpenetração, ou mesmo a solução mais favorável ao mais fraco da relação (tratamento diferente dos diferentes)*". *)*" (MARQUES, 2009, p. 90).

[481] A expressão "diálogo aberto" parece adequada para, em parte, exprimir a provisoriedade desta pesquisa, em face do hipotético estado de crise e incertezas no direito, reflexo possivelmente da suposta esquizofrenia que, ao senso comum, acomete a sociedade nesta era digital. Quer-se relacionar com o seu sentido originário – relacionado à terapêutica psiquiátrica – de "princípios dialogais" de Bakthtin (1984), em sua dimensão poética fundada na ideia de "tolerância à incerteza", "dialogismo" e "polifonia em redes sociais" (KANTORSKI e CARDANO, 2017).

[482] Além de Elon Musk - **cofundador da OpenAI, o laboratório responsável pela** criação do ChatGPT **e do** GPT-4 **-** assinaram a carta Emad Mostaque, fundador da Stability AI, Steve Wozniak, cofundador da Apple e vários engenheiros de empresas como DeepMind, Microsoft, Meta, Google e Amazon. Para os subscritores da carta aberta, os responsáveis pelo desenvolvimento da Inteligência Artificial devem utilizar os seis meses de suspensão para "desenvolver e implementar em conjunto um leque de protocolos de segurança, para o *design* e desenvolvimento de Inteligência Artificial avançada." Estes protocolos devem ser "auditados de forma rigorosa e supervisionados por peritos independentes". https://observador.pt/2023/03/29/elon-musk-assina-carta-aberta-que-defende-a-suspensao-da-inteligencia-artificial/

[483] Em referência a mencionada carta aberta, os veículos de imprensa sinalizam motivação concorrencial, portanto funda em visão pragmática utilitarista (mercadológica) dos idealizadores do manifesto: "(...) O Twitter parece estar trabalhando em um projeto de inteligência artificial generativa. Segundo o portal Business Insider, duas pessoas familiarizadas com o assunto disseram que Elon Musk, CEO da empresa, comprou recentemente cerca de 10.000 unidades de processamento gráfico (GPUs) para a plataforma – normalmente, as companhias de tecnologia usam esses microprocessadores para desenvolver grandes modelos de IA, dada a carga de trabalho computacional que eles exigem. Outro indício de que bilionário terá a sua própria IA é que ele contratou novos talentos da área. Dentre eles, os engenheiros Igor Babuschkin e Manuel Kroiss, que trabalhavam na DeepMind, subsidiária de pesquisa de IA da Alphabet. O portal The Information relatou que, pelo menos desde fevereiro deste ano, Musk tem abordado especialistas no assunto para iniciar seu próprio empreendimento e, assim, rivalizar com o ChatGPT, da OpenAI". https://epocanegocios.globo.com/tecnologia/noticia/2023/04/depois-de-dizer-que-e-contra-avancos-da-ia-elon-musk-faz-preparativos-para-lancar-seu-proprio-chatgpt.ghtml

problemática abordada neste estudo exploratório.

Nesse contexto, surge a indagação quanto a terem sido alcançados os resultados e hipóteses inicialmente considerados neste estudo. O objetivo era obter uma melhor compreensão das interações (ou possibilidades "dialógicas") entre o Direito e as novas tecnologias de IA, com foco no equilíbrio potencial entre os interesses protegidos no âmbito dos segredos de negócio e da proteção de dados pessoais.

Acredita-se que sim, na medida em que os sinais e eventos mencionados anteriormente reforçam a compreensão positiva de que embora o direito estatal seja autorreferencial e autopoiético por natureza — desempenhando a função de integrar e estabilizar as expectativas sociais —, ele está destinado a abranger apenas uma parte da realidade(LUHMANN, 1983) e ao regular de forma universal os conflitos em torno de expectativas, nem todas as expectativas individuais poderiam ser atendidas por não possuírem respaldo social(VILAS BOAS FILHO, 2009, pp. 151-152).

O reconhecimento dessa limitação está presente na abordagem voltada aos movimentos regulatórios de diversos países, inclusive o Brasil, cujo Parlamento parece empreender esforços no sentido de harmonizar o Ordenamento do País às diretrizes reconhecidas internacionalmente, no âmbito das quais são consideradas a complexidade e a diversidade das interações globais entre os direitos nacionais e suas estratégias na regulação do uso das tecnologias de IA (Seção 6.2), ajustadas à realidade de cada jurisdição.

Em certa medida, as proposições apresentadas ao Parlamento Brasileiro (BRASIL, 2022, Relatório Final) convergem no sentido de definir o papel dos agentes envolvidos no desenvolvimento dos sistemas de IA na tarefa de conformar essas novas tecnologias aos princípios democráticos e direitos fundamentais contemplados na Constituição.

Nesse aspecto, verificou-se forte consenso no âmbito do debate público de que a regulação da IA deverá estar pautada na garantia de direitos fundamentais, em especial da liberdade e igualdade e no desenvolvimento da personalidade dos indivíduos. Dado o reconhecimento da ampla desigualdade da sociedade brasileira, é preciso mitigar o risco de que o racismo e a discriminação estrutural sejam perpetuados no bojo do desenvolvimento e

utilização dos sistemas de IA no País. (BRASIL, 2022, Relatório Final) [484].

Ao examinar os desequilíbrios normativos relacionados à problemática da IA em sua interação com os institutos estudados, surgem visões pessimistas, otimistas ou realistas, todas merecedoras de consideração. Como verificado, optou-se por adotar a perspectiva dialógica em tese presente no processo informacional, cujas diretrizes caberia ao Estado Regulador estabelecer. De mais a mais, acredita-se aqui que a tecnologia está destinada a evoluir e a se ajustar para equilibrar o estado de assimetria informacional que ela mesma deu causa, isso em um período "pré-regulatório" caracterizado por ampla discricionariedade.

[484] Nas palavras de Laura Schertel Mendes aqui parafraseadas, a lógica adotada nas proposições da Comissão de Juristas foi a de ampliar a segurança jurídica e ao mesmo tempo viabilizar que o uso e implementação da IA no País beneficiem toda sociedade, todos os indivíduos ou grupos potencialmente por ela afetados, inclusive o mercado e o próprio Estado Administração. V. apresentação do relatório dos trabalhos atribuídos pelo Senado à Comissão de Juristas por ela coordenada. Disponível em https://www.youtube.com/watch?v=7RVvvAqYZIU&t=1202s, acesso em 01.06.2023.

CONSIDERAÇÕES FINAIS

Esta Dissertação tem como objetivo examinar as interações entre as tecnologias de Inteligência Artificial (IA), a proteção de segredos comerciais e a proteção de dados pessoais. O foco é no debate sobre a aplicabilidade dos princípios de transparência e explicabilidade nas decisões automatizadas.

Para entender a complexidade desses temas, optamos por uma abordagem exploratória e procuramos fornecer uma visão panorâmica do fenômeno, analisando-o sob três perspectivas de tempo: passado, presente e futuro.

Retrospectivamente, percebemos que as mudanças nos sistemas tecnológico, social e jurídico desafiam nossas interpretações tradicionais da realidade. As soluções clássicas nem sempre são aplicáveis aos novos desafios, e as questões que enfrentamos hoje não são simplesmente problemas antigos em uma nova roupagem.

A digitalização e a tomada de decisões automatizadas, frutos da popularização da internet e dos computadores pessoais no final do século XX, introduziram desafios e riscos inéditos. Com o avanço da tecnologia de análise de dados e da inteligência de negócios, processos decisórios também foram digitalizados, culminando na decisão automatizada. Devido ao avanço da IA, especialmente do aprendizado de máquina, decisões podem ser tomadas automaticamente com base em *big data* e algoritmos complexos de IA.

Nessa nova realidade, torna-se vital para as organizações protegerem não apenas os dados coletados, mas também os algoritmos e processos usados nas decisões. Isso se tornou ainda mais crítico com a expansão da decisão automatizada, pois os algoritmos usados são muitas vezes considerados segredos comerciais.

À medida que a tecnologia evolui, aumenta a pressão para adaptá-la às leis de proteção de dados pessoais. A preocupação com o abuso no tratamento e utilização de dados pessoais por entidades públicas e privadas levou a uma mudança na perspectiva normativa de privacidade. Anteriormente, a privacidade era entendida como o direito à intimidade, ao segredo e à solidão. Agora, o foco da privacidade é na autonomia individual e no direito de controlar as próprias informações.

No momento atual, a preocupação se concentra na automação das decisões diárias proporcionada pela IA, realidade que estimulou o enfoque da pesquisa nos desafios relacionados à transparência e explicabilidade das decisões automatizadas.

O estudo mostrou que a falta de conhecimento dos parâmetros de racionalidade dos algoritmos dificulta a garantia da transparência.

Existem pontos relevantes na União Europeia, com a GDPR, e no Brasil, com a LGPD, para compreender o direito à explicação. É preciso encontrar um equilíbrio entre o princípio da transparência e a limitação de acesso às informações, pois nenhum desses direitos é absoluto.

Dentro do âmbito das decisões automatizadas, concorda-se que o direito de explicação estabelecido no Art. 20 da Lei Geral de Proteção de Dados (LGPD) tem o potencial de fomentar o diálogo entre os agentes sociais. Isso pode ocorrer caso as normas do devido processo sejam respeitadas sob a supervisão de uma autoridade estatal independente.

Ademais, percebe-se que **(i)** a regulamentação de dados na LGPD é crucial para a proteção do segredo tecnológico, permitindo que o controlador apresente argumentos concretos e legais contra solicitações relacionadas aos dados; e **(ii**) para os titulares de dados, este procedimento garante o direito de revisar a decisão automatizada ou o perfilamento algorítmico.

Isso inclui o acesso aos dados pessoais, a correção de informações incorretas e a solicitação de anonimização, bloqueio ou exclusão de dados desnecessários ou tratados inadequadamente.

Face à complexidade das questões e às lacunas na regulamentação da proteção de dados pessoais e na proteção dos segredos de negócio, argumenta-se que é fundamental que os controladores/desenvolvedores e os titulares de dados pessoais recebam e estejam sob a intervenção do Estado, sem que isso implique um paternalismo incompatível com a autonomia e a liberdade individual.

Considerando a complexidade das interações que envolvem aspectos sociais, legais e algorítmicos, a Lei pode enfrentar dificuldades em estabilizar as expectativas normativas. Isso, porém (i) não legitima a suposição de que a solução emergirá de uma visão tecnocêntrica que ignore as nuances do problema, (ii) nem nega que a tecnologia possa ser usada para ajudar a corrigir as assimetrias existentes.

Os esforços atuais buscam adaptar o sistema jurídico brasileiro à era da inteligência artificial (IA). Esses esforços se manifestam nas propostas apresentadas pela comunidade de especialistas, fornecendo subsídios ao Parlamento para a criação do marco legal da IA, incorporadas no Projeto de Lei 2338/2023 em trâmite no Senado Federal.

Apesar da aspiração, não se pode afirmar que as propostas normativas em debate no parlamento brasileiro garantam que as decisões automatizadas sejam justas e imparciais. No entanto, essas propostas parecem tentar equilibrar a proteção dos titulares dos dados com as inovações tecnológicas da IA, buscando benefícios para todos os envolvidos.

Esta Dissertação apresenta limitações e não explora de forma aprofundada muitos dos temas abordados. Mesmo assim, adotando uma perspectiva interdisciplinar, aponta para novas pesquisas diante dos desafios sociotécnicos da IA, onde tecnologias estão assumindo funções que eram tradicionalmente do Direito na mediação e organização das interações na sociedade.

A compreensão do sistema jurídico de forma isolada não será suficiente para criar regras claras em um ambiente digital descentralizado, fluido e dominado por poucos agentes econômicos. A transparência é desafiadora quando a tecnologia esconde segredos compreendidos apenas por uma elite de especialistas.

Sem uma atuação adequada do Estado, as garantias constitucionais perdem sentido porque claramente destituídas de eficácia. É necessário, portanto, uma regulamentação que estabeleça regras e diretrizes sobre o uso ético e responsável da tecnologia, de modo a proteger os direitos dos cidadãos potencialmente afetados pelas decisões automatizadas.

Resolver essas questões requer uma constante interação e experimentação democrática, com foco na correção das desigualdades estruturais do País. A abertura da "caixa-preta" algorítmica, expondo os segredos da esfera estatal e privada ao escrutínio público, seria uma consequência necessária.

REFERÊNCIAS

ABRANCHES, S. Presidencialismo de coalizão: o dilema institucional brasileiro. **Dados: Revista de Ciências Sociais**, v. 31, n. 1, pp. 5-34, 1988.

AGÊNCIA EUROPEIA PARA A SEGURANÇA DAS REDES E DA INFORMAÇÃO. Big data security good practices and recommendations on the security of big data systems. Disponível em: https://www.enisa.europa.eu/publications/big-data-security/at_download/fullReport. Acesso em: 5 maio 2023.

ALEXY, R. **Teoria dos direitos fundamentais**. 2. ed. São Paulo: Malheiros, 2012.

ALGORITMO. *In:* WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em: https://pt.wikipedia.org/w/index.php?title=Algoritmo&oldid=62298816. Acesso em: 24 out. 2021.

ALMADA, M. Direito à revisão de decisões automatizadas. 2020. Tese de Láurea (Graduação em Direito) Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020. Disponível em: https://www.marcoalmada.com/publication/almada-direito-2020/almada-direito-2020.pdf. Acesso em: 4 abr. 2023.

ALMELING, D. S. Seven reasons why trade secrets are increasingly important. **Berkeley Technology Law Journal**, n. 27, pp. 1098-1101, 2012.

AMARAL, F. **Introdução a ciência de dados**: mineração de dados e big data. Rio de Janeiro: Alta Books, 2016.

ANDRADE, F. S. de. Notas sobre a aplicabilidade dos direitos da personalidade à pessoa jurídica como evolução da dogmática civil. **RJLB**, a. 4, n. 5, pp. 806-837, 2018.

ANDREU, J. *et al*. Big data for health. **IEEE Journal of Biomedical and Health Informatics**, v. 19, n. 4, pp. 1193-1208, 2015.

ARAUJO, V. D. de. **A gênese dos direitos da personalidade e sua inaplicabilidade à pessoa jurídica**. 2015. Tese (Doutorado em Direito Civil) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015. Disponível em: https://teses.usp.br/teses/disponiveis/2/2131/tde-02102017-111538/publico/Tese_doutorado_Vaneska_COMPLETA.pdf. Acesso em: 4 maio 2023.

ASCENSÃO, J. de O. O princípio da prestação: um novo fundamento para a concorrência desleal? **ROA**, a. 56, v. I, p. 7, 1996. Disponível em: https://portal.oa.pt/upl/%7B3aef442f-f195-4f7a-a003-318724af7bec%7D.pdf. Acesso em: 15 abr. 2023.

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS. Opinion nº 7, de 2015. Meeting the challenges of big data. Disponível em: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf. Acesso em: 5 maio 2023.

BANTERLE, F. **The interface between data protection and IP Law**:

the case of trade secrets and the database sui generis right in marketing operations, and the ownership of raw data in big data analysis. Disponível em: https://www.researchgate.net/publication/333602235_The_Interface_between_Data_Protection_and_IP_Law_The_Case_of_Trade_Secrets_and_Database_Sui_Generis_Right_in_Marketing_Operations_and_the_Ownership_of_Raw_Data_in_Big_Data_Analysis. Acesso em: 4 maio 2023.

BAPTISTA, P.; KELLER, C. I. Por que, quando e como regular as novas tecnologias? **RDA: Revista de Direito Administrativo**, Rio de Janeiro, v. 273, pp. 123-163, set./dez. 2016.

BARBOSA, D. B. **Tratado da propriedade intelectual**. Rio de Janeiro: Lumen Juris, 2015.

BARONE, D. M. **A proteção internacional do segredo industrial**. 2009. 134 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

BARROSO, L. R. **Temas de Direito Constitucional**. Tomos II e IV. Rio de Janeiro: Renovar, 2009.

BATCHELOR, B.; MURRAY, G. Internet of Things: antitrust concerns in the pipeline? **Kluwer Competition Law Blog**, 12 maio 2016. Disponível em: https://competitionlawblog.kluwercompetitionlaw.com/2016/05/12/internet-of-things-antitrust-concerns-in-the-pipeline/. Acesso em: 4 maio 2023.

BATISTA NETO, J. **O que é direito digital**. Disponível em: https://tecnodireito.wordpress.com/o-que-e-direito-digital. Acesso em: 5 maio 2023.

BENNETT MOSES, L. How to think about law, regulation and technology: problems with 'technology' as a regulatory target law. **Innovation and Technology**, v. 5, n. 1. pp. 1-20, 2013. Disponível em: http://ssrn.com/abstract=2464750. Acesso em: 4 maio 2023.

BERCOVICI, G. **Constituição econômica e desenvolvimento:** uma leitura a partir da Constituição de 1988. São Paulo: Malheiros, 2005.

BIG DATA. *In:* DICIONÁRIO Cambridge. Cambridge: Cambridge University Press, [s.d.]. Disponível em: https://dictionary.cambridge.org/dictionary/english/big-data. Acesso em: 4 maio 2023.

BINENBOJM, G. **Uma teoria do Direito Administrativo**. Rio de Janeiro: Renovar, 2014.

BIONI, B.; SCHERTEL MENDES, L. 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:* FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOBBIO, N. **Democracia e segredo**. 1. ed. São Paulo: UNESP, 2015.

BONE, R. G. The (still) shaky foundations of trade secret law. **Texas Law Review**, n. 563, 2014. Disponível em: https://ssrn.com/abstract=2445024. Acesso em: 1 dez. 2022.

BORGES, R. F. **Descontrole de estruturas**: dos objetivos do antitruste às desigualdades econômicas. 2020. Tese (Doutorado em Direito Comercial) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2132/tde-24032021-163117/publico/6856660_Tese_Original.pdf. Acesso em: 5 maio 2023.

BUNGE, M. **Seudociencia e ideología**. Madri: Alianza, 1985.

BRAGA NETO, F. P. Ilícito civil, esse desconhecido. *In*: DIDIER JR., F.; EHRDT JR, M. (org.). **Revisitando a teoria do fato jurídico**: homenagem a Marcos Bernardes de Mello. São Paulo: Saraiva, 2010. pp. 175-212.

BRANDÃO, L. C. C. **Fluxo transnacional de dados**: estruturas, políticas e o Direito nas vertentes da governança. 2020. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal de Minas Gerais, Belo Horizonte, 2020. Disponível em: https://repositorio.ufmg.br/handle/1843/33716. Acesso em: 24 abr. 2023.

BRASIL. Advocacia-Geral da União (AGU). **Manual de negociação baseado na Teoria de Harvard**. Brasília: EAGU, 2017. Disponível em: https://www.gov.br/agu/pt-br/composicao/escola-da-agu-1/avaliacao-editorial/ebook__manual_de_negociacao_baseado_na_teoria_de_harvard.pdf. Acesso em: 5 maio 2023.

BRASIL. Conselho Nacional de Justiça (CNJ). Resolução nº 125, de 29 de novembro de 2020. Dispõe sobre a Política Judiciária Nacional de tratamento adequado dos conflitos de interesses no âmbito do Poder Judiciário. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2014/04/resolucao_125_29112010_23042014190818.pdf. Acesso em: 5 maio 2023.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9 279.htm. Acesso em: 5 maio 2023.

BRASIL. Ministério da Ciência, Tecnologia e Inovações (MCTI). Portaria nº 4.979, de 13 de agosto de 2021. Altera o Anexo da Portaria MCTI nº 4.617, de 6 de abril de 2021, que institui a Estratégia Brasileira de Inteligência Artificial e seus eixos temáticos. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MCTI_n_4979_de_13072021.html. Acesso em: 5 maio 2023.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). **Estratégia Brasileira para a Transformação Digital**. Brasília: 2018. Disponível em: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf. Acesso em: 5 maio 2023.

BRASIL. Senado Federal. **Relatório final.** 2022. Disponível em: https://legis.senado.leg.br/comissoes/mnas?codcol=2504&tp=4. Acesso em: 2 fev. 2023.

BRASIL. Senado Federal. Projeto de Lei nº 23338, de 2023. Disponível, em https://www25.senado.leg.br/web/atividade/materias/-/materia/157233, Acesso: 2 fev. 2023.

BRESSER-PEREIRA, L. **O conceito histórico de desenvolvimento econômico**.

2006. Disponível em: https://www.bresserpereira.org.br/papers/2006/06.7-ConceitoHistoricoDesenvolvimento.pdf. Acesso em: 5 maio 2023.

BUCAR, D.; VIOLA, M. Tratamento de dados pessoais por "legítimo interesse do controlador". *In:* FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

BUCCI, M. P. D. **Direito administrativo e políticas públicas**. São Paulo: Saraiva, 2002.

BUCCI, M. P. D. **Fundamentos para uma teoria jurídica das políticas públicas**. São Paulo: Saraiva, 2013.

BUCCI, M. P. D. O conceito de política pública em Direito. *In*: BUCCI, M. P. D. (org.). **Políticas públicas**: reflexões sobre o conceito jurídico. São Paulo: Saraiva, 2006. pp. 1-49.

BUCCI, M. P. D. Quadro de referência de uma política pública: primeiras linhas de uma visão jurídico institucional. **Revista Direito do Estado**, n. 122, 2016. Disponível em: http://www.direitodoestado.com.br/colunistas/maria-paula-dallari-bucci/quadro-de-referencia-de-uma-politica-publica-primeiras-linhas-de-uma-visao-juridico-institucional. Acesso em: 5 maio 2023.

BUCCI, M. P. D.; COUTINHO, D. R. Arranjos jurídico-institucionais da política de inovação tecnológica: uma análise baseada na abordagem de Direito e políticas públicas. *In*: COUTINHO, D. R.; FOSS, M. C.; MOUALLEM, P. S. B. **Inovação no Brasil**: avanços e desafios jurídicos e institucionais. São Paulo: Blucher, 2017.

BUCHNER, B. **Informationelle Selbstbestimmung im Privatrecht**. Tübingen: Mohr Siebeck, 2006.

CABRAL, P. **A nova Lei de Direitos Autorais**. Porto Alegre: Sagra, 1998.

CAETANO, G. As diferenças entre digitalização, digitização e transformação digital. **Exame**, 29 set. 2021. Disponível em: https://exame.com/blog/gustavo-caetano/as-diferencas-entre-digitalizacao-digitizacao-e-transformacao-digital/. Acesso em: 3 nov. 2021.

CANABARRO, Diego. **Governança global da internet:** tecnologia, poder e desenvolvimento. Tese (Doutorado em Ciência Política) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014. Disponível em: https://www.academia.edu/10513610/Governan%C3%A7a_global_da_Internet_Tecnologia_Poder_e_Desenvolvimento_Volume_1. Acesso em: 2 abr. 2022.

CANOTILHO, J. J. G. **"Brancosos" e interconstitucionalidade**: itinerários dos discursos sobre a historicidade constitucional. 2. ed. Coimbra: Almedina, 2008.

CANTARINI, P. Inteligência artificial e abordagem via risquificação. **Migalhas**, 19 abr. 2022. Disponível em: https://www.migalhas.com.br/arquivos/2022/4/40AB87D6286F11_IAemmovimento.pdf. Acesso em: 30 maio 2023.

CARNEIRO, J. V. C.; ALMADA, G. M. A gênese do direito à proteção de dados brasileiro: uma conceitualização e contextualização histórica face à nova lei pátria e

as relações do ramo com a propriedade intelectual. *In*: XII CONGRESSO DE DIREITO DE AUTOR E INTERESSE PÚBLICO. **Anais**... Porto Alegre: 2019. Disponível em: https://www.gedai.com.br/wp-content/uploads/2019/06/033-A-G%C3%8ANESE-DO-DIREITO-%C3%80-PROTE%C3%87%C3%83O-DE-DADOS-BRASILEIRO.pdf. Acesso em: 12 de. 2022.

CASSESE, S. **Le basi del Diritto Amministrativo**. Torino: Garzanti, 1998.

CASSIOLATO, J. E.; BRITTO, J.; VARGAS, M. A. Arranjos cooperativos e inovação na indústria brasileira. *In*: DE NEGRI, J. A.; SALERNO, M. S. (org.). **Inovações, padrões tecnológicos e desempenho das firmas industriais brasileiras**. Brasília: IPEA, 2005.

CASTELLS, M. **Redes de indignação e esperança**. Rio de Janeiro: Zahar, 2013.

CASTELLS, M. **Ruptura:** a crise da democracia liberal. Rio de Janeiro: Zahar, 2018.

CASTILLO VÁSQUEZ, I. del. **Protección de datos**: cuestiones constitucionales y administrativas. Cizur Menor: Thomson-Civitas, 2007.

CERQUEIRA, J. da G. **Tratado da propriedade industrial**. Da propriedade industrial e do objeto dos direitos. v. I. Rio de Janeiro: Lumen Juris, 2012.

CERRILLO-I-MARTÍNEZ, A. La contribución de las TIC a la mejora de la transparencia administrativa. **Arbor: Ciencia, Pensamiento y Cultura**, v. 188, n. 756, p. 208, jul./ago. 2012.

CHAMAS, C. I. (coord.). **Scientia 2000**: propriedade intelectual para a academia. Rio de Janeiro: Fundação Oswaldo Cruz, Ministério da Ciência e Tecnologia, Fundação Konrad Adenauer, 2003.

CHANOCA, S. E. V. **Conceito e extensão da tutela**. 2016. Dissertação (Mestrado em Direito) – Universidade de Lisboa, Lisboa, 2016. Disponível em: https://repositorio.ul.pt/handle/10451/26148?locale=en. Acesso em: 21 dez. 2023.

CHAUÍ, M. Contingência e necessidade. *In*: NOVAES, A. *et al.* **A crise da razão**. São Paulo: Companhia das Letras, 1999.

CHINELLATO, S. J. de A.; MORATO, A. C. Direitos básicos de proteção de dados pessoais. O princípio da transparência e a proteção dos direitos intelectuais. *In*: DONEDA, D. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. pp. 641-664.

BENNETT, C.; RAAB, C. D. Revisiting 'the governance of privacy': contemporary policy instruments in global perspective. **Privacy Law Scholars Conference**, Berkeley, jun., 2017. Disponível em: https://ssrn.com/abstract=2972086. Acesso em: 18 abr. 2023.

COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões. Uma abordagem global da protecção de dados pessoais na União Europeia. Bruxelas, 4 nov. 2010. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52010DC0609. Acesso em: 5 maio 2023.

COMISSÃO EUROPEIA. Cyber: towards a thriving data-driven economy. **Shaping Europe's digital future**, n. 442, jul. 2014. Disponível em:

https://ec.europa.eu/digitalagenda/en/news/communication-data-driven-economy. Acesso em: 5 maio 2023.

COMISSÃO EUROPEIA. Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679. Bruxelas: 2018. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053/en. Acesso em: 2 jun. 2023.

CONESA, T. R. **Estudo sobre o know-how**: o know-how sob a perspectiva dos direitos da personalidade. 2017. Dissertação (Mestrado em Direito Comercial) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2017.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). Ato de Concentração nº 08012.003107/2010-62. Requerente: TNL PCS S.A. (Oi). Interessada: Phorm Veiculação de Publicidade Ltda. (Phorm). Brasília: 2010.

CONVERGÊNCIA tecnológica. *In:* WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2022. Disponível em: https://pt.wikipedia.org/wiki/Converg%C3%AAncia_tecnol%C3%B3gica. Acesso em: 24 out. 2022.

CORMEN, T. H. **Algorithms unlocked.** Cambridge: MIT Press, 2013.

CORTEZ, N. Regulating disruptive innovation. *In*: BAPTISTA, P.; KELLER, C. I. **RDA: Revista de Direito Administrativo**, Rio de Janeiro, v. 273, pp. 123-163, set./dez. 2016.

COSTA, J. M. **A boa-fé no Direito Privado**. São Paulo: Revista dos Tribunais, 1998.

COUTINHO, D. R. **Direito Econômico e desenvolvimento democrático:** uma abordagem institucional. 2015. Tese – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015.

COUTINHO, D. R. O Direito Econômico e a construção institucional do desenvolvimento democrático. **Revista Estudos Institucionais**, v. 2, n. 1, 2016. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/36. Acesso em: 5 maio 2023.

COUTINHO, D. R. O Direito nas políticas públicas. *In*: MARQUES, E.; FARIA, M. A. P. (org.). **A política pública como campo multidisciplinar**. São Paulo: Unesp; Fiocruz, 2013. pp. 181-198.

COUTINHO, D. R.; MOUALLEM, P. S. B. O Direito contra a inovação? A persistência dos gargalos jurídicos à inovação no Brasil. *In*: LASTRES, M. M. *et al.* **O futuro do desenvolvimento:** tópicos em homenagem a Luciano Coutinho. Campinas: Unicamp, 2016. pp. 181-214.

COUTINHO, D. R.; SCHAPIRO, M. G. Economia política e Direito Econômico: do desenvolvimentismo aos desafios da retomada do ativismo estatal. *In*: COSTA, J. A. F.; ANDRADE, J. M. A. de; MATSUO, A. M. H. (org.), **Direito**: teoria e experiência. Estudos em homenagem a Eros Roberto Grau. São Paulo: Malheiros, 2013. pp. 581-617.

CRAVO, D. C. **Direito à portabilidade na Lei Geral de Proteção de Dados**. Indaiatuba: Foco, 2020.

CRÉMER, J.; MONTJOYE, Y. de; SCHWEITZER, H. Competition policy for the digital era.

European Union, p. 3, abr. 2019. Disponível em: http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf. Acesso em: 5 maio 2023.

CUEVAS, G. C. de las. **Derecho de las patentes de invención**. 2. ed. Buenos Aires: Heliasta, 2004.

CUNDIFF, V. A. Reasonable measures to protect trade secrets in a digital environment. **IDEA: The Intellectual Property Law Review**, n. 49, p. 361, 2009.

DANAHER, J. *et al*. Algorithmic governance: developing a research agenda through the power of collective intelligence. **Big data & Society**, v. 4, n. 2, 2017. Disponível em: https://doi.org/10.1177/2053951717726554. Acesso em: 5 maio 2023.

DATASETS, o que são e como utilizá-los. **Aquarela**, 23 abr. 2018. Disponível em: https://www.aquare.la/datasets-o-que-sao-e-como-utiliza-los/. Acesso em: 2 dez. 2020.

DAVIS, K. E.; TREBILCOCK, M. A relação entre Direito e desenvolvimento: otimistas versus céticos. **Revista Direito GV 9**, São Paulo, v. 5, n. 1, pp. 217-232, 2009.

DE LUCCA, N.; LIMA, C. R. P. de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: LIMA, C. R. P. de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina Brasil, 2019. pp. 373-398. [edição *Kindle*]

DE MAURO, A. *et al*. A formal definition of big data based on its essential features. **Library Review**, v. 65, n. 3, pp. 122-135, 2016.

DE NEGRI, J. A.; SALERNO, M. S.; CASTRO, A. B. Inovações, padrões tecnológicos e desempenho das firmas industriais brasileiras. *In*: DE NEGRI, J. A.; SALERNO, M. S. (org.). **Inovações, padrões tecnológicos e desempenho das firmas industriais brasileiras**. Brasília: IPEA, 2005. pp. 5-46.

DEEP learning: o que é, conceitos e definições. **Cetax**, 23 jan. 2022. Disponível em: https://cetax.com.br/o-que-e-deep-learning/. Acesso em: 8 maio 2023.

DIAS, R. **Análise:** Aquisição do WhatsApp une duas visões de mundo opostas, 20 fev. 2014. Disponível em: http://www1.folha.uol.com.br/tec/2014/02/1414823-analise-aquisicao-do-whatsapp-une-duas-visoes-de-mundo-opostas.shtml. Acesso em: 5 maio 2023.

DIGITALIZAÇÃO. *In*: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em: https://pt.wikipedia.org/w/index.php?title=Digitaliza%C3%A7%C3%A3o&oldid=61339957. Acesso em: 8 jun. 2021.

DINIZ, M. H. **Compêndio de introdução à Ciência do Direito**. 13. ed. São Paulo: Saraiva, 2001.

DOMINGOS, P. **The master algorithm**: how the quest for the ultimate learning machine will remake our world. [s.l.]: Basic Books, 2015.

DONEDA, D. A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção

de Dados. *In*: DONEDA, D. *et al* (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. pp. 459-469.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021. [edição *Kindle*].

DRAKE, W. J.; CERF, V. G.; KLEINWÄCHTER, W. Internet fragmentation: an overview. **Future of the Internet Initiative White Paper**, jan. 2016. Disponível em: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf. Acesso em: 5 maio 2023.

DREXL, J. *et al*. Data ownership and access to data: position statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate. **Max Planck Institute for Innovation & Competition Research Paper**, n. 16-10, 2016. Disponível em: https://ssrn.com/abstract=2833165. Acesso em: 5 maio 2023.

EMPOLI, G. da. **Os engenheiros do caos** [Como as fake news, as teorias da conspiração e os algoritmos estão sendo utilizados para disseminar ódio, medo e influenciar eleições]. 1. ed. São Paulo: Vestígio, 2020.

ENGELFRIET, A. **Database protection in the USA**. Disponível em: http://www.iusmentis.com/databases/us/. Acesso em: 5 maio 2023.

ESPECIALISTAS falam das diferentes consequências da digitalização da vida. **Fundação Heinrich Böll**, 7 ago. 2019. Disponível em: https://br.boell.org/pt-br/2019/08/07/especialistas-falam-das-diferentes-consequencias-da-digitalizacao-da-vida. Acesso em: 5 maio 2023.

ESTADOS UNIDOS DA AMÉRICA (EUA). Securities and Exchange Commission. **Google's 2004 Annual Report**. 2004. Disponível em: https://www.sec.gov/Archives/edgar/data/1288776/000119312505065298/d10k.htm. Acesso em: 5 maio 2023.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Legado:** Grupo de Trabalho do Artigo 29. Disponível em: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_pt. Acesso em: 31 maio 2023.

EVANS, D. S.; SCHMALENSEE, R. Matchmakers: the new economics of multisided platforms. **Harvard Business Press Review**, Boston, pp. 39-45, 2016.

EVANS, D. S.; SCHMALENSEE, R. The antitrust analysis of multi-sided platform businesses. **University of Chicago Institute for Law & Economics Olin Research Paper**, n. 623, 2013. Disponível em: https://ssrn.com/abstract=2185373. Acesso em: 5 maio 2023.

FARIA, J. E. **O direito na economia globalizada**. São Paulo: Malheiros, 2007.

FEIGELSON, B.; LEITE, L. **Sandbox:** experimentalismo no Direito Exponencial. São Paulo: Thomson Reuters Brasil, 2020.

FEKETE, E. K. **O regime jurídico do segredo de indústria e comércio no Direito brasileiro**. Rio de Janeiro: Forense, 2003.

FEKETE, E. K. **Perfil do segredo de indústria e comercio no Direito brasileiro**: identificação

e análise crítica. 1999. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 1999.

FEKETE, E. K. **Segredo de empresa.** *In*: CAMPILONGO, C. F.; GONZAGA, Á. A.; FREIRE, A. L. (coord.). Direito Comercial. **Enciclopédia Jurídica da PUC-SP**. 1. ed. São Paulo: PUC-SP, 2017. p. 5.

FELIX DE SOUZA MACHADO, H. **Imaginários sociotécnicos da governança da Internet: uma análise de redes do Mapa de Soluções da Netmundial**. Brasília, 2019. Dissertação (mestrado em direito) Universidade de Brasília.

FERNÁNDEZ-SAMANIEGO, J.; FERNÁNDEZ-LONGORIA, P. El Derecho de la portabilidade de los datos. *In*: MANÃS, J. L. P.; CARO, M. A.; GAYO, M. R. (coord.). **Regulamento general de protección de datos**: hacia un nuevo modelo europeo de privacidad. Madri: Reus, 2016. pp. 257-274.

FERRARESE, M. R. Mercati e globalizzazione. Gli incerti cammini del Diritto. *In*: FERRARESE, M. R. **Le istituzioni della globalizzazione**. Bolonha: Il Mulino, 2000. p. 59.

FERRARI, I. **Accountability de algoritmos:** a falácia do acesso ao código e caminhos para uma explicabilidade efetiva. Disponível em: https://beta.itsrio.org/wp-content/uploads/2019/03/Isabela-Ferrari.pdf. Acesso em: 5 maio 2023.

FERRAZ JR., T. S. **A ciência do Direito**. 2. ed. São Paulo: Atlas, 1980.

FERRAZ JR., T. S. **Introdução ao estudo do Direito**. São Paulo: Atlas, 1988.

FERRO, M. R. **Pontos de convergência entre as teses doutrinárias brasileiras quanto ao princípio da supremacia do interesse público sobre o particular**. 2014. Dissertação (Mestrado em Direito do Estado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2134/tde-11022015-133301/publico/Murilo_Ruiz_Ferro_DissertacaoIntegral.pdf. Acesso em: 5 maio 2023.

FIDELIS, A. L. Data-driven mergers: a call for further integration of dynamics effects into competition analysis. **Revista de Defesa da Concorrência**, Brasília, v. 5, n. 2, pp. 189-219, nov. 2017. Disponível em: http://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/354/175. Acesso em: 5 maio 2023.

FINANCIADORA DE ESTUDOS E PROJETOS (FINEP). **Manual de Oslo**. Brasília: FINEP, 2004. Disponível em: http://download.finep.gov.br/imprensa/manual_de_oslo.pdf. Acesso em: 23 nov. 2018.

FISHER, R. **Como chegar ao sim:** como negociar acordos sem fazer concessões. 1. ed. Rio de Janeiro: Solomon, 2014.

FORGIONI, P. A. Análise Econômica do Direito (AED): paranóia ou mistificação. **Revista de Direito Mercantil, Industrial, Econômico e Financeiro**, São Paulo, v. 54, n. 139, pp. 243-256, 2005.

FORGIONI, P. A. **Contrato de distribuição.** São Paulo: Revista dos Tribunais, 2005.

FRAGOSO, R. Comissão de juristas da inteligência artificial entrega relatório final a Pacheco. **Senado Notícias**, 6 dez. 2022. Disponível em: https://www12.senado.leg.br/noticias/audios/2022/12/comissao-de-juristas-da-inteligencia-artificial-entrega-relatorio-final-a-pacheco. Acesso em: 8 maio 2023.

FRAZÃO, A. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, A. O direito à explicação e à oposição diante de decisões totalmente automatizadas. **Jota**, 9 jul. 2019. 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: 5 maio 2023.

FRAZÃO. A. Big data e aspectos concorrenciais do tratamento de dados. *In*: DONEDA, D. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. pp. 535-555.

FRAZÃO, A.; CARVALHO, Â. P. de; MILANEZ, G. **Curso de proteção de dados:** fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022. [edição *Kindle*]

FREITAS, R. L. **Propriedade intelectual:** paradigma internacional e(m) crise(s): uma análise teórica interdisciplinar sob a perspectiva de crise e lições para o século XXI. Rio de Janeiro: Lumen Juris, 2021.

FREITAS, R. L. Direito, tecnologia e ideologia. *In:* MEYER, E.; POLIDO, F.; TRIVELLATO, M. (org.). **Direito, democracia e internet**: perspectivas comparadas. Belo Horizonte: Initia Via, 2021.

FUKUYAMA, F. **Confiança**: as virtudes sociais e a criação da prosperidade. Rio de Janeiro: Rocco, 1996.

GABARDO, E. Interesse público e subsidiariedade: o Estado e a sociedade civil para além do bem e do mal. **Revista de Investigações Constitucionais**, Belo Horizonte, v. 4, n. 2, pp. 95-130, 2017. Disponível em: https://doi.org/10.5380/rinc.v4i2.53437. Acesso em: 5 maio 2023.

GARCIA AMADO, J. A. **La filosofia del Derecho de Habermas y Luhmann**. Bogotá: Universidad Externado de Colombia, 1997.

GARCIA, B. V. **Contrafação de patentes violação de direitos de propriedade industrial com ênfase na área químico-farmacêutica**. São Paulo: LTr, 2005.

GARCIA, B. V. **Direito e tecnologia**: regime jurídico da ciência, tecnologia e inovação. São Paulo: LTr, 2008.

GARCIA, B. V.; SILVEIRA, N. **Direito e tecnologia**: contribuição ao estudo do regime jurídico da ciência, tecnologia e inovação. 2007. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2007.

GARCÍA, N. B. Procedimientos por vulneración de la normativa de protección de datos: tramitación de denuncias. *In*: LOMBARTE, A. R. (org.). **Tratado de protección de datos**. Valência: Tirant lo Blanch, 2019. pp. 548-581.

GASPARDO, M. Democracia participativa e experimentalismo democrático em tempos sombrios. **Estudos Avançados**, v. 32, n. 92, pp. 65-88, 2018. Disponível em: https://www.revistas.usp.br/eav/article/view/146438. Acesso em: 16 nov. 2021.

GONÇALVES, E. das N.; STELZER, J. Princípio da eficiência econômico-social no Direito brasileiro: a tomada de decisão normativo-judicial. **Sequência**, Florianópolis, n. 68, pp. 261-290, jun. 2014. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552014000100012&lng=en&nrm=iso. Acesso em: 5 maio 2023.

GONZÁLEZ, L. A. D. **Transparencia de la información pública y protección de datos personales:** un balanceo necesario. Madri: Universidad Complutense Madrid, 2010.

GRAU, E. R. Lei do plano. **Revista de Direito Público**, São Paulo, a. XIII, n. 53-54, pp. 315-ss., jan./jun. 1980.

GRAU, E. R. **A ordem econômica na Constituição de 1988**: interpretação e crítica. 14. ed. São Paulo: Malheiros, 2010.

GRAU, E. R. **Direito, conceito e normas jurídicas**. São Paulo: Revista dos Tribunais, 1988.

GRECO, M. A. G. **Planejamento fiscal e interpretação da lei tributária**. São Paulo: Dialética, 1998.

GRUNES, A. P.; STUCKE, M. E. No mistake about it: the important role of antitrust in the era of *big data*. **University of Tennessee Legal Studies Research Paper**, n. 269, 2015. Disponível em: https://ssrn.com/abstract=2600051. Acesso em: 5 maio 2023.

GUERRA FILHO, W. S. **Processo constitucional e direitos fundamentais**. São Paulo: Instituto Brasileiro de Direito Constitucional, 1999.

HABERMAS, J. **A inclusão do outro**: estudos de teoria política. 2. ed. São Paulo: Loyola, 2004.

HABERMAS, J. **Mudança estrutural da esfera pública**. Rio de Janeiro: Tempo Brasileiro, 1984.

HASSEMER, W. Datenschutz: die Aufgaben der nächsten Jahre. *In*: BÄUMLER, H.; MUTIUS, A. von (org.). **Datenschutzgesetze der dritten Generation**. Neuwied, Kriftel: Luchterland, 1999.

HEILMANN, L. F. P. A livre forma de comercializar, o spam, proteção de dados pessoais e os direitos fundamentais envolvidos. *In*: PÉREZ, D. V. (org.). **Direito e justiça**: derecho ante los desafíos de la globalizaión. Curitiba: Juruá, 2017.

HESSE, K. **A força normativa da Constituição**. Porto Alegre: Sérgio Fabris, 1991.

HILDEBRANDT, M. Pre-emptive computing system. *In*: HILDEBRAND, M. **Smart technologies and the end(s) of law**. [s.l.]: Edward Elgar Publishing Ltd., 2016.

HOFFMAN-RIEM, W. **Teoria geral do Direito Digital**: transformação digital. Desafios para o Direito. Rio de Janeiro: Forense, 2021.

HONDA, H.; FACURE, M.; YAOHAO, P. Os três tipos de aprendizado de máquina. **LAMFO**, 27 jul. 2017. Disponível em: https://lamfo-unb.github.io/2017/07/27/tres-tipos-am/. Acesso em: 8 maio 2023.

HOUAISS, A.; VILLAR, M. de S. **Dicionário Hoauiss da Língua Portuguesa**. 1. ed. Rio de Janeiro: Objetiva, 2009.

HU, H. *et al*. Toward scalable systems for big data analytics: a technology tutorial. **IEEE Access**, v. 2, pp. 652-687, maio 2014. Disponível em: https:// http://ieeexplore.ieee.org/document/6842585/?reload=true. Acesso em: 5 maio 2023.

HUSTINX, P. Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Bruxelas: 2014.

HYLA, E. Corporate cybersecurity: the international threat to private networks and how regulations can mitigate it. **Vanderbilt Journal of Entertainment and Technology Law**, v. 21, p. 309, 2018. Disponível em: http://www.jetlaw.org/wp-content/uploads/2018/12/6_Hyla_Final.pdf. Acesso em: 5 maio 2023.

IMMERGUT, E. O núcleo teórico do novo institucionalismo. *In*: SARAIVA, E.; FERRAREZI, E. **Políticas públicas**. Brasília: ENAP, 2007. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4182349/mod_resource/content/1/ellen%20immergut_o%20nucleo%20teorico%20do%20novo%20institucionalismo.pdf. Acesso em: 5 maio 2023.

INFOCURIA. Acórdão do Tribunal de Justiça (3. Seção), de 17 de julho de 2014. YS v Minister voor Immigratie, Integratie. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-141/12&language=en. Acesso em: 2 jun. 2023.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Big data and data protection**. Disponível em: https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220. Acesso em: 5 maio 2023.

INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO (ITSRIO). Contribuições para a Estratégia Brasileira de Inteligência Artificial Consulta Pública – MCTIC. Rio de Janeiro: 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/04/Contribui%C3%A7%C3%B5es-ITS-Consulta-P%C3%BAblica-IA.pdf. Acesso em: 23 jan. 2023.

INTERNET SOCIETY. The commercialization of the internet. Module 1: The history of internet. Disponível em: https://www.internetsociety.org/tutorials/shaping-the-internet/module-1- history-of-the-internet/. Acesso em: 5 maio 2022.

IRTI, N. Direito e Economia. **Revista de Direito Privado**, v. 62, abr./jun. 2015. Disponível em: http://professor.pucgoias.edu.br/SiteDocente/admin/arquivosUpload/17851/material/Direito%20e%20Economia%20-%20Natalino%20Irti.PDF. Acesso em: 7 dez. 2021.

ISAACSON. W. **Os inovadores:** uma biografia da revolução digital. 1. ed. São Paulo: Companhia das Letras, 2014.

JABUR, W. P.; SANTOS, M. J. P. dos. (coord.). **Propriedade intelectual**: criações industriais, segredo de negócio e concorrência desleal. São Paulo: Saraiva, 2007.

KAHNEMAN, D. **Rápido e devagar:** duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

KANTORSKI, L. P.; CARDANO, M. Diálogo Aberto: a experiência finlandesa e suas contribuições. **Saúde em Debate**, v. 41, n. 112, pp. 23-32, 2017. Disponível em: https://doi.org/10.1590/0103-1104201711203. Acesso em: 29 maio 2023.

KATZ, M. L., SHAPIRO, C. Systems competition and network effects. **Journal of Economic Perspectives**, v. 8, n. 2, pp. 93-115, 1994.

KEARNS, M; ROTH, A. **The Ethical Algorithm**: the science of socially aware algorithm design. Nova Iorque: Oxford University Press, 2019. [edição *Kindle*]

KENNEDY, J. The myth of data monopoly: why antitrust concerns about data are overblown. **Information, Technology & Innovation Foundation (ITIF)**, p. 3, mar. 2017.

KESSLER, D. S.; DRESCH, R. de F. V. Direito à portabilidade de dados e a sua relação com a proteção do consumidor e da concorrência pela perspectiva da Behavioral Law and Economics. *In*: CRAVO, D. C. **Direito à portabilidade na Lei Geral de Proteção de Dados**. Indaiatuba: Foco, 2020. pp. 55-75.

KROES, P. Philosophy of technology. *In*: GRAIG, E. (ed.). **Routledge Encyclopedia of Philosophy**. [s.l.]: Routledge, 1998.

KUHN, T. S. **A estrutura das revoluções científicas**. São Paulo: Perspectiva, 2017. [edição *Kindle*]

KUNTZ, R.; FARIA, J. E. **Qual o futuro dos direitos?** São Paulo: Max Limonad, 2002.

LAZZARINI, S. G. **Capitalismo de laços:** os donos do Brasil e suas conexões. São Paulo: Elsevier, 2011.

LEE, R.; ANDERSON, J. Code-dependent: pros and cons of the algorithm age. **Pew Research Center**, 8 fev. 2017. Disponível em: https://www.pewresearch.org/internet/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/. Acesso em: 8 maio 2023.

LESSIG, L. **Code**: and other laws of the cyberspace. Nova Iorque: Basic Books, 1999.

LESSIG, L. **Code (Version 2.0)**. Nova Iorque: Basic Books, 2006.

LEINER, B. M. *et al*. **A brief history of the internet.** 1997, Disponível em: https://www.internetsociety.org/internet/history-internet/brief-history-internet/#JCRL62. Acesso em: 26 dez. 2019.

LIMA, C. R. P. de et al. Coord. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. [edição *Kindle*]

LIMA, C. R. P. de. **Validade e obrigatoriedade dos contratos de adesão eletrônicos (shrink-wrap e click-wrap) e dos termos e condições de uso (browse-wrap)**: um estudo comparado entre Brasil e Canadá. 2009. Tese (Doutorado em Direito Civil) – Faculdade de Direito,

Universidade de São Paulo, São Paulo, 2009.

LIMONGI, F.; FIGUEIREDO; A. Bases institucionais do presidencialismo de coalizão. **Lua Nova**, n. 44, 1998.

LINDITCH, F. Discernement et transparence dans les marchés publics. *In*: NGAMPIO-OBÉLÉ-BÉLÉ, U. (org.). **Le discernement en Droit Public**. Aix-en Provence: Presses Universitaires d' Aix-Marseille, 2016. p. 51.

LOMBARTE, A. R. Del derecho a la protección de datos a la garantia de nuevos derechos digitales. *In*: LOMBARTE, A. R. (org.). **Tratado de protección de datos**. Valência: Tirant lo Blanch, 2019. pp. 23-52.

LÓPEZ, M. S. **La protección de datos en el Reino Unido**: evolución del right to privacy y escenarios post-Brexit. Cizur Menor: Thomson Reuters, 2019.

LYON, D. **Surveillance as social sorting: privacy, risk and digital discrimination**. 1. ed. [s.l.]: Routledge, 2003.

LUHMANN, N. **Sociologia do Direito**. Rio de Janeiro: Edições Tempo Brasileiro, 1983.

MACHADO, H. F. de S. **Imaginários sociotécnicos da governança da internet:** uma análise de redes do Mapa de Soluções da NET mundial. 2019. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2019. Disponível em: https://repositorio.unb.br/handle/10482/35995. Acesso em: 3 mar. 2023.

MACHADO, J. A. S.; BIONI, B. R. A proteção de dados pessoais nos programas de nota fiscal: um estudo de caso do "Nota Fiscal paulista". **LIINC em Revista**, Rio de Janeiro, v.12, 2016. Disponível em: https://doi.org/10.18617/liinc.v12i2.919. Acesso em: 5 maio 2023.

MADEIRA, D. C. O que é solipsismo judicial. **Revista Jurídica da Presidência**, Brasília, v. 22, n. 126, pp. 191-210, fev./maio 2020. Disponível em: http://dx.doi.org/10.20499/2236-3645.RJP2020v22e126-1916. Acesso em: 31 maio 2023.

MALGIERI, G. Trade secrets v personal data: a possible solution for balancing rights. **International Data Privacy Law**, v. 6, n. 2, pp. 102-116, maio 2016. Disponível em: https://ssrn.com/abstract=3002685. Acesso em: 5 maio 2023.

MAÑAS, J. L. P.; GAYO, M. R. **El derecho a la protección de datos em la jurisprudencia del Tribunal de Justicia de la Unión Europea**. Madri: Wolters Kluwer, 2018.

MANICA, F. B. **Racionalidade econômica e racionalidade jurídica na Constituição de 1988**. Disponível em: http://fernandomanica.com.br/site/wp-content/uploads/2015/10/racionalidade_economica_e_juridica.pdf. Acesso em: 13 out. 2019.

MANUAL de Oslo. *In:* WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em: https://pt.wikipedia.org/wiki/Manual_de_Oslo. Acesso em: 23 nov. 2018.

MARQUES, C. L. **Manual de Direito do Consumidor**. 2. ed. São Paulo: Revista dos Tribunais, 2009.

MARQUES NETO, F. P. de A. **Regulação estatal e interesses públicos**. São Paulo: Malheiros, 2002. pp.100-133.

MARTIN, L; MENNICKEN, A. The importance of regulation of and by algorithm. **Algorithmic Regulation**, Londres, n. 85, pp. 2-6, 2017. Disponível em: https://www.lse.ac.uk/accounting/Assets/CARR/documents/D-P/Disspaper85.pdf#page=5. Acesso em: 23 maio 2023.

MARTINS JR., W. P. **Transparência administrativa**. São Paulo: Saraiva, 2004.

MATTIOLI, M. Disclosing big data. **Minnesota Law Review**, 2014. Disponível em: http://www.repository.law.indiana.edu/facpub/1480. Acesso em: 5 maio 2023.

MATTOS, P. T. L. A formação do Estado regulador. **Novos Estudos CEBRAP**, n. 76, pp. 139-156, 2006.

MAYER-SCHÕNBERGER, V.; CUKIER, K. **Big data:** a revolution that will transform how we live, work, and think. Nova Iorque: Houghton Mifflin Harcourt, 2014.

MAZZUCATO, M. **The entrepreneurial state:** debunking public vs. private sector myths. Landers: Anthem Press, 2013.

McAFEE, A.; BRYNJOLFSSON, E. Big data: the management revolution. **Harvard Business Review**, v. 90, n. 10, pp. 60-68, 2012.

MELLO, M. P. de. A perspectiva sistêmica na sociologia do Direito: Luhmann e Teubner. **Tempo Social**, v. 18, n. 1, pp. 351–373, jun. 2006. Disponível em: https://www.scielo.br/j/ts/a/LKjSyhSTYhx457xb76WMPfk/?lang=pt#. Acesso em: 29 maio 2023.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, L. S.; FONSECA, G. C. S. da. Proteção de dados para além do consentimento: tendências de materialização. *In*: DONEDA, D. *et al*. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MENDES, L. S.; MATIUZO, M.; FUJIMOTO, M. T. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. *In*: DONEDA, D. *et al*. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro, Forense, 2021.

MEYRAN, R. São os humanos, não as máquinas, que criam significado. **Correio da Unesco,** mar. 2018. Disponível em: https://pt.unesco.org/courier/2018-3/sao-os-humanos-nao-maquinas-que-criam-significado. Acesso em: 2 jun. 2023.

MILAGRE, J. A.; SANTAREM SEGUNDO, J. E. A propriedade dos dados e a privacidade na perspectiva da Ciência da Informação. **Revista Eletrônica de Biblioteconomia e Ciência da Informação**, v. 20, n. 43, pp. 47-76, maio/ago. 2015.

MILLER, H. G.; MORK, P. From data to decisions: a value chain for big data. **IT Professional**, v. 15, n. 1, 2013. Disponível em: https://www.researchgate.net/publication/260305818_From_Data_to_Decisions_A_Value_Ch

ain_for_Big_Data. Acesso em: 5 maio 2023.

MIRAGEM, B. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, Porto Alegre, v. 1009, p. 2, nov. 2019.

MITTELSTADT, B. D. *et al*. The ethics of algorithms: mapping the debate. **Big data & Society**, v. 3, n. 2, jul./dez. 2016. Disponível em: https://doi.org/10.1177/2053951716679679. Acesso em: 5 maio 2023.

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

MONTEIRO, R. L. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. **Jota**, 14 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 5 maio 2023.

MONTEIRO, R. L. **Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil**. 2021. Tese (Doutorado em Filosofia e Teoria Geral do Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-22072022-120338/fr.php. Acesso em: 22 fev. 2023.

MOROZOV, E. **Big tech**: a ascensão dos dados e a morte da política. São Paulo: UBU, 2018.

MUCHIUTI, M. M. **Do RGPD à LGPD**: difusão internacional de normas e o caso das regulamentações de proteção de dados pessoais. 2022. Dissertação (Mestrado em Direito) – Programa de Estudos de Pós- Graduação em Governança Global, Pontifícia Universidade Católica de São Paulo, São Paulo, 2022. Disponível em: https://repositorio.pucsp.br/handle/handle/29644. Acesso em: 5 mar. 2023.

MULHOLLAND, C. **Responsabilidade civil e processos decisórios autônomos em sistemas de inteligência artificial (IA)**: autonomia, imputabilidade e responsabilidade. *In*: FRAZÃO, A.; MULHOLLAND, C. (org.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. pp. 332 e ss.

MULHOLLAND, C.; FRAJHOF, I. Z. Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação frente à tomada de decisões por meio de machine learning. *In*: FRAZÃO, A.; MULHOLLAND, C. (org.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. 2. ed. Rio de Janeiro: Revista dos Tribunais, 2019. pp. 265-287.

NETO, R. J. Inovação disruptiva. **UNESC**, 11 dez. 2017. Disponível em: https://www.unesc.net/portal/blog/ver/571/40459. Acesso em: 8 maio 2023.

O DESAFIO das fintechs financeiras. **Exame**, 16 abr. 2021. Disponível em: https://exame.com/blog/visao-global/o-desafio-das-fintechs-financeiras/. Acesso em: 5 maio 2023.

O MUNDO é plano. *In*: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em: https://pt.wikipedia.org/w/index.php?title=O_Mundo_%C3%89_Plano:_uma_Breve_Hist%C

3%B3ria_do_S%C3%A9culo_XXI&oldid=61486885. Acesso em: 27 jun. 2021.

O USO de machine learning na otimização de pricing. **Ilumeo**, 2020. Disponível em: https://ilumeo.com.br/todos-posts/2020/08/15/o-uso-de-machine-learning-na-otimizacao-de-pricing. Acesso em: 5 maio 2023.

O'REILLY, T. Data is the new sand. **The Information**, 24 fev. 2021. Disponível em: https://www.theinformation.com/articles/data-is-the-new-sand. Acesso em: 5 maio 2023.

OHLHAUSEN, M.; OKULIAR, A. Competition, consumer protection, and the right [approach] to privacy. **Antitrust Law Journal**, v. 80, n. 1, p. 136, 2015.

OHLWEILER, L. P.; CADEMARTORI, S. U. **Do segredo à transparência na administração pública**: os arcana imperii e o direito de acesso à informação. Canoas: Unilasalle, 2018.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data**. 2002.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Big data**: bringing competition policy to the digital era. 2016. Disponível em: https://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm. Acesso em: 22 jun. 2021.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Data-driven innovation for growth and well-being**. 2021. Disponível em: http://oe.cd/bigdata. Acesso em: 5 maio 2023.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Going Digital Project**. 2023. Disponível em: www.oecd.org/going-digital. Acesso em: 5 maio 2023.

OSTROM, E. Institutional analysis and development: elements of the framework in historical perspective. *In*: CROTHERS, C. (org.). **Historical developments and theoretical approaches in sociology**. Oxford: EOLSS Publishers, 2010.

OSTROM, E. Institutional rational choice: an assessment of the institutional analysis and development framework. *In*: SABATIER, P. (org.). **Theories of the policy process**. Colorado: Westview Press, 2007. pp. 21-63.

PASQUALE, F. **The black box society**. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PELENCE, B. M. **Avaliação de medidas de similaridade para criação de hierarquias de rótulos na classificação multirrótulo.** 2022. 68 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Controle e Automação) – Universidade Federal de Santa Catarina, Blumenau, 2022. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/243411/TCC%20Bruno%20Mafra.pdf?sequence=1. Acesso em: 14 fev. 2023.

PEREIRA NETO, C. M. da S.; RENZETTI, B. P. Big data entre três microssistemas jurídicos: consumidor, privacidade e concorrência. *In:* PEREIRA

NETO, C. M. da S. (org.). **Defesa da concorrência em plataformas digitais**. São Paulo: FGV Direito SP, 2020. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/30031/Defesa%20da%20Concorre%CC%82ncia%20em%20Plataformas%20Digitais.pdf?sequence=1. Acesso em: 5 maio 2023.

PEREZ, M. A. **Testes de legalidade:** métodos para o amplo controle jurisdicional da discricionariedade administrativa. Belo Horizonte: Fórum, 2020.

PFEIFFER, R. A. C. Digital Economy, big data and competition law. **Market and Competition Law Review**, v. III, n. 1, pp. 53-89, abr. 2019. Disponível em: https://ssrn.com/abstract=3440296. Acesso em: 5 maio 2023.

PFEIFFER, R. A. C. ANPD em busca de sua autonomia: é preciso aperfeiçoar a MP 869/2018. **Conjur**, 1 maio 2019. Disponível em: https://www.conjur.com.br/2019-mai-01/garantias-consumo-anpd-busca-autonomia-preciso-aperfeicoar-mp. Acesso em: 5 maio 2023.

PINHEIRO, P. P. **Direito Digital**. [s.l.]: Saraiva, 2007.

PINTO, Á. V. **O conceito da tecnologia**. Rio de Janeiro: Contraponto, 2005.

PIRES, T. C. F.; SILVA, R. P. da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, n. 3, p. 242, 2017.

POSNER, R. A.; LANDES, W. M. **The economic structure of intellectual property law**. Cambridge: 2003.

REALE, M. **Lições preliminares de Direito**. São Paulo: Saraiva, 1993.

REALE, M. **Teoria tridimensional de Direito**. São Paulo: Saraiva, 1993.

REGULATING the internet giants: the world's most valuable resource is no longer oil, but data. The Economist, 6 maio 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 5 maio 2023.

REIS, N. C. M.; FURTADO, G. R. Decisões automatizadas: definição, benefícios e riscos. **Civilistica.com**, Rio de Janeiro, a. 11, n. 2, 2022. Disponível em: http://civilistica.com/decisoes-automatizadas. Acesso em: 5 dez. 2022.

REZENDE, S. M. A evolução da política de C&T no Brasil. *In*: REZENDE, S. M. **Momentos de ciência e tecnologia no Brasil**. Uma caminhada de 40 anos pela C&T. Rio de Janeiro: Vieira e Lent, 2010. pp. 301-318.

RIBEIRO, R. S. Inteligência artificial, Direito e equidade algorítmica: discriminações sociais em modelos de machine learning para a tomada de decisão. **Revista de Informação Legislativa**, Brasília, v. 59, n. 236, pp. 29-53, out./dez. 2022. Disponível em: https://www12.senado.leg.br/ril/edicoes/59/236/ril_v59_n236_p29.pdf. Acesso em: 4 maio 2023.

RISCH, M. Why do we have trade secrets? **Marquette Intellectual Property Law Review**, v.

11, n. 1, p. 33, 2007. Disponível em: https://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=1089&context=iplr. Acesso em: 8 maio 2023.

RODA. *In*: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em: https://pt.wikipedia.org/wiki/Roda. Acesso em: 26 nov. 2018.

RUST, R. T.; KANNAN, P. K.; PENG, N. The customer economics of internet privacy. **Journal of the Academy of Marketing Science**, n. 30, pp. 455-464, 2002.

SAMPAIO, P. R. P. **Regulação e concorrência nos setores nos setores de infraestrutura**: análise do caso brasileiro à luz da jurisprudência do CADE. 2012. Tese (Doutorado em Filosofia e Teoria Geral do Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

SANDEN, A. F. M. de S. **A proteção de dados pessoais do empregado no Direito brasileiro**: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado. 2012. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: http://www.teses.usp.br/teses/disponiveis/2/2138/tde-05082013-165006/pt-br.php. Acesso em: 5 maio 2023.

SANTOS, B. de S. Os processos de globalização. *In*: SANTOS, B. de S. (org.). **A globalização e as ciências sociais**. São Paulo: Cortez, 2002.

SARLET, G. B. S. Notas sobre a proteção de dados pessoais na sociedade informacional na perspectiva do atual sistema normativo brasileiro. *In*: LIMA, C. R. P. de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2019. [edição *Kindle*]

SARLET, I. W. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: DONEDA, D. *et al* (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SARLET, G. B. S., RUARO R. L. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018. *In*: DONEDA, D. et al (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. pp. 177-198.

SARTOR, G.; LAGIOIA, F. **The impact of the General Data Protection (GDPR) on artificial intelligence**. Bruxelas: 2020. p. 64. Disponível em: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)641530https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)641530. Acesso em: 19 jan. 2023.

SAUSSURE, F. **Curso de linguística geral**. 27. ed. São Paulo: Cultrix, 2006.

SCHAPIRO, M. G. Repensando a relação entre Estado, Direito e desenvolvimento: os limites do paradigma rule of law e a relevância das alternativas institucionais. **Revista Direito GV 11**, São Paulo, v. 6, n. 1, pp. 213-252, 2011.

SCHIRATO, R. N. M. Transparência administrativa, participação, eficiência e controle social: Direito Administrativo em evolução? *In*: ALMEIDA, F. D. M. de *et al* (org.). **Direito Público**

em evolução. Belo Horizonte: Fórum, 2013.

SCHOLZ, L. Big data não é big oil: o papel da analogia no direito das novas tecnologias. **Tennessee Law Review**, set. 2018. Disponível em: http://dx.doi.org/10.2139/ssrn.3252543. Acesso em: 5 maio 2023.

SCHULTZ, M.; LIPPOLDT, D. Approaches to protection of undisclosed information (trade secrets): background paper. **OECD Trade Policy Papers**, Paris, n. 162, Paris, 2014. Disponível em: http://dx.doi.org/10.1787/5jz9z43w0jnw-en. Acesso em: 3 abr. 2023.

SCHUMPETER, J. **Capitalism, socialism and democracy**. Estados Unidos da América: Harper Perennial, 2015.

SEGADE, G. **El secreto industrial (know how)**: concpeto y protection. [s.l.]: Tecnos, 1974.

SEIKKULA, J., OLSON, M. E. A abordagem do diálogo aberto para a psicose aguda: sua poética e micropolíticas. **Family Process**, v. 42, n. 3, pp. 403-418, 2003.

SEN, A. **Development as freedom**. Nova Iorque: Anchor Books, 2000.

SERICK, R. **Forma e realtá della persona giuridica.** Milão: Giuffrè, 1966.

SICHMAN, J. S. Inteligência Artificial e sociedade: avanços e riscos. **Estudos Avançados**, v. 35, n. 101, pp. 37-50, 2021. Disponível em: https://www.revistas.usp.br/eav/article/view/185024. Acesso em: 12 abr. 2023.

SILVA, F. M. da; MAIA, J. S. da S. Neologismos na mídia em meio à pandemia da covid-19. **Fórum Linguístico**, Florianópolis, v. 18, n. 2, pp. 6079-6100, abr./jun. 2021.

SILVEIRA, C. **Bancos de dados originais e não-originais**. [s.d.]. Disponível em: http://www.interpatents.com.br/pdfs/csilveira_bancos_dados.pdf. Acesso em: 5 maio 2023.

SILVEIRA, N. **Propriedade intelectual**: propriedade industrial, direito de autor, software, cultivares. 3. ed. Barueri: Manole, 2005.

SILVEIRA, S. A. da. Discursos sobre regulação algorítmica. **Estudos de Sociologia**, Araraquara, v. 25, n. 48, pp. 63-85, jan./jun. 2020.

SIMÃO FILHO, A. O direito da empresa à vida privada e seus reflexos no Direito Falimentar. *In*: MARTINS, I. G. da S.; FERREIRA JR., A. J. (coord.). **Direito à privacidade**. São Paulo: Centro de Extensão Universitária, 2005. pp. 337-365.

SOUSA E SILVA, N. Quando o segredo é a "alma do negócio". Definição de um conceito. **Revista da Associação Brasileira da Propriedade Intelectual**, n. 126, pp. 3-22, 2013. Disponível em: https://repositorio.ucp.pt/handle/10400.14/13526. Acesso em: 14 out. 2019.

SOUSA E SILVA, N. Um retrato do regime português dos segredos de negócio. **Propriedades Intelectuais**, v. 3, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2508867. Acesso em: 8 maio 2023.

SOUSA E SILVA, N. What exactly is a trade secret under the proposed directive? **Journal of Intellectual Property Law & Practice**, v. 9, n. 11, 2014. Disponível em:

http://jiplp.oxfordjournals.org/. Acesso em: 5 maio 2023.

SOUZA, C. A.; PERRONE, C; MAGRANI, E. O direito à explicação: entre a experiência europeia e a sua positivação na LGPD. *In*: DONEDA, D. *et al*. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SOUZA, R. P. de. Participação pública nos processos decisórios das agências reguladoras: reflexões sobre o Direito brasileiro a partir da experiência norte americana. **Fórum Administrativo – Direito Público**, Belo Horizonte, a. 2, n. 16, jun. 2002.

SPIEKERMANN, S. *et al*. The challenges of personal data markets and privacy. **Electronic Markets**, v. 25, n. 2, pp. 161-167, 2015. Disponível em: https://ssrn.com/abstract=3305307 Acesso em: 23 maio 2023.

SRNICK, N. **Platform capitalism**. Cambridge: Polity Press, 2018.

STRECK, L. L. **Verdade e consenso**: constituição, hermenêutica e teorias discursivas. 4. ed. São Paulo: Saraiva, 2012.

STUCKE, M. E.; GRUNES, A. P. **Big data and competition policy**. Nova Iorque: Oxford University Press, 2016.

SZNIAWSKI, E. Considerações sobre o direito à intimidade das pessoas jurídicas. **Revista da Faculdade de Direito**, Curitiba, v. 25, n. 25, pp. 81-92, 1989.

TEIXEIRA, J. A. Crise moderna e racionalidade argumentativa no Direito: o modelo de Aulis Aarnio. **Revista de Informação Legislativa**, v. 39, n. 154, abr./jun. 2002. Disponível em: http://www2.senado.leg.br/bdsf/handle/id/781. Acesso em: 5 maio 2023.

TEIXEIRA, R. A. A produção capitalista do conhecimento e o papel do conhecimento na produção capitalista: uma análise a partir da teoria marxista do valor. **Revista Economia**, maio/ago. 2009.

TEUBNER, G. Direito e teoria social: três problemas. **Tempo Social**, v. 27, n. 2, pp. 75-101, 2015.

TOMASEVICIUS FILHO, E. Inteligência artificial e direitos da personalidade: uma contradição em termos? **Revista da Faculdade de Direito**, São Paulo, n. 113, pp. 133-149, 2018. Disponível em: https://doi.org/10.11606/issn.2318-8235.v113i0p133-14. Acesso em: 5 maio 2023.

TORRES, J. **Teoria da complexidade**: uma nova visão de mundo para a estratégia. **I EBEC**, Curitiba, jul. 2005. Disponível em: https://www.researchgate.net/publication/237319052_Teoria_da_complexidade_uma_nova_visao_de_mundo_para_a_estrategia. Acesso em: 6 dez. 2022.

TREBILCOCK, M. J.; PRADO, M. M. **What makes poor countries poor?** Institutional determinants of development. Cheltenham: Edward Elgar, 2011.

TRUBEK, D. M. Max Weber on law and the rise of capitalism. **Faculty Scholarship Series**, n. 4001, 1972.

TRUBEK, D. M.; GALANTER, M. Acadêmicos auto-alienados: reflexões sobre a crise norte-americana da disciplina “Direito e desenvolvimento”. **Revista Direito GV 6**, São Paulo, v. 3, n. 2, pp. 261-280, 1974.

TSUKADA, J. Auditoria: conheça como funciona o procedimento e aprenda a gerenciar seus documentos. **Assinei**, 17 jun. 2021. Disponível em: https://assinei.digital/auditoria-documentos/. Acesso em: 21 jan. 2023.

TUCKER, D. S.; HILL, W. Big mistakes regarding big data. **Antitrust Source**, American Bar Association, dez. 2014. Disponível em: https://ssrn.com/abstract=2549044. Acesso em: 5 maio 2023.

TYSVER, D. A. **Database legal protection**. Disponível em: http://www.bitlaw.com/copyright/database.html. Acesso em: 5 maio 2023.

UNESCO. **Draft text of the Recommendation on the Ethics of Artificial Intelligence**. 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000377897. Acesso em: 5 maio 2023.

UNGER, R. M. **A economia do conhecimento**. [s.l.]: Autonomia Literária, 2018. [edição *Kindle*]

UNIÃO EUROPEIA. Diretiva (UE) nº 2016/943 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0943. Acesso em: 19 dez. 2022.

VAINZOF, R.; GUTIERREZ, A. Capítulo 2. Inteligência Artificial: conceitos fundamentais. *In*: VAINZOF, R.; GUTIERREZ, A. **Inteligência Artificial (IA)**. São Paulo: Revista dos Tribunais, 2021. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/1394839564/inteligencia-artificial-ia. Acesso em: 19 jan. 2023.

VALENTE, J. C. O paradigma tecnológico das TICs: para uma reconstrução não determinista da dimensão técnica no capitalismo contemporâneo. **Revista Eptic**, v. 20, n. 3, 2018. Disponível em: https://seer.ufs.br/index.php/eptic/article/view/10777. Acesso em: 16 nov. 2022.

VANTAGEM competitiva. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em: https://pt.wikipedia.org/w/index.php?title=Vantagem_competitiva&oldid=62469700. Acesso em: 22 nov. 2021.

VÉLIZ, C. **Privacidade é poder**. [s.l.]: Contracorrente, 2021. [edição *Kindle*]

VERDASCA, N. M. da C. F. **Identificação e análise de movimento humano com ultrassons**. 2013. Dissertação (Mestrado em Engenharia Eletrónica e Comunicações) – Instituto Superior de Engenharia de Lisboa, Lisboa, 2013.

VÉU da ignorância. *In:* WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2023. Disponível em:

https://pt.wikipedia.org/wiki/V%C3%A9u_da_ignor%C3%A2ncia. Acesso em: 8 maio 2023.

VICENTIN, D. Governança da internet: infraestrutura e resistência. *In*: IV SIMPÓSIO INTERNACIONAL LAVITS. **Nuevos paradigmas de vigilancia?** Miradas desde América Latina. Buenos Aires, 2016. Disponível em: https://lavits.org/wp-content/uploads/2017/08/P8_Vicentin.pdf. Acesso em: 28 abr. 2023.

VILAS BÔAS FILHO, O. **Teoria dos sistemas e o Direito brasileiro**. São Paulo: Saraiva, 2009.

WEBER, M. **Economia e sociedade**: fundamentos da sociologia compreensiva. 4. ed. Brasília: UnB, 2015.

WIENER, J. B. The regulation of technology, and the technology of regulation. **Technology in Society**, Durham, n. 26, pp. 483-500, 2004. Disponível em: http://scholarship.law.duke.edu. Acesso em: 1 maio 2016.

YEUNG, K. Algorithmic regulation and intelligent enforcement. **Centre for Analysis of Risk and Regulation Discussion Paper Series**, n. 84, pp. 50-61, out. 2016.

ZARSKY, T. The trouble with algorithmic decisions: an analytic road map to examine efficiency and fairness in automated and opaque decision making. **Science, Technology & Human Values**, v. 41, n. 1, 2016.

ZUBOFF, S. Surveillance capitalism and the challenge of collective action. **SAGE Journals**, 24 jan. 2019. Disponível em: https://journals.sagepub.com/doi/full/10.1177/1095796018819461. Acesso em: 23 maio 2023.