Universidade de Brasília
Faculdade de Direito
Programa de Pós-Graduação em Direito
Curso de Doutorado

MARIA CRISTINE BRANCO LINDOSO

A OPACIDADE E OS SEGREDOS DE NEGÓCIO NO MERCADO DE DADOS PESSOAIS

Tensões entre sigilo e transparência na busca pela garantia fundamental à proteção de dados.

Brasília
2024

Universidade de Brasília
Faculdade de Direito
Programa de Pós-Graduação em Direito
Curso de Doutorado

MARIA CRISTINE BRANCO LINDOSO

A OPACIDADE E OS SEGREDOS DE NEGÓCIO NO MERCADO DE DADOS PESSOAIS

Tensões entre sigilo e transparência na busca pela garantia fundamental à proteção de dados.

Tese apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília como requisito parcial para a obtenção do título de Doutora em Direito, elaborada sob a orientação da Prof.ª Dra. Ana Frazão.

Brasília
2024

UNIVERSIDADE DE BRASÍLIA

Faculdade de Direito

Programa de Pós-Graduação em Direito

Tese apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília como requisito parcial para a obtenção do título de Doutora em Direito.

MARIA CRISTINE BRANCO LINDOSO

BANCA EXAMINADORA

_____

Professora Doutora Ana Frazão (Orientadora)
Universidade de Brasília

_____

Professor Doutor Gustavo Tepedino (Avaliador Externo)
Universidade do Estado do Rio de Janeiro

_____

Professora Doutora Caitlin Mulholland (Avaliadora Externa)
Pontifícia Universidade Católica do Rio de Janeiro

_____

Professor Doutor Alexandre Veronese (Avaliador Interno)
Universidade de Brasília

Brasília, 21 de agosto de 2024.

Para o Mauricio: um rio de inspiração do tamanho do Amazonas, com um coração maior do que a Quinta Avenida.

AGRADECIMENTOS

Concluir este trabalho é um momento muito emocionante, não só pela superação das dificuldades que ele representa, mas também pela possibilidade de agradecer, nestas páginas iniciais, às pessoas que participaram dos mais de 10 anos de Universidade de Brasília que me trouxeram até aqui. Durante a graduação, o mestrado e doutorado, pude conhecer o Direito como um instrumento poderoso e interdisciplinar, de uma forma que só é ensinada no *campus* pensado por Darcy Ribeiro.

A UnB me permitiu fazer amigos para a vida toda e conhecer pessoas que mudaram o rumo da minha história. Nela, vivi da militância à advocacia; do PIBIC ao Doutorado; da solidão ao casamento; da experiência de aluna à vivência de professora. A UnB me formou em vários sentidos e me permitiu viver as experiências mais incríveis da minha jornada pessoal, profissional e acadêmica. Então a ela, representando seus servidores/as, professores/as, alunos/as e colegas, o meu mais profundo agradecimento.

Para além da gratidão genérica, imprescindível detalhar meu agradecimento à Professora Ana Frazão: minha orientadora desde o primeiro PIBIC em 2015, sempre se esforçou para contemplar meus variados interesses acadêmicos, dando-me espaço para amadurecer as reflexões que me trouxeram até aqui. Fico feliz em perceber que esses quase 10 anos de jornada me permitiram encontrar nela não só uma mentora, como também uma amiga.

Ainda dentro do corpo docente da UnB, agradeço à Professora Ana Cláudia Farranha e ao Professore Tarcisio Vieira de Carvalho Neto, que fizeram parte da minha jornada de doutorado com debates, orientações e até empréstimos de livros. Na figura deles, estendo esse agradecimento a todos os professores e professoras do PPGD.

Agradeço ao Professor Alexandre Veronese e às Professoras Caitlin Mulholland e Laura Schertel Mendes, pelo gentil aceite em comprem minha banca. Todos acompanham a minha jornada acadêmica há anos – o professor Veronese desde a graduação e as professoras Caitlin e Laura desde o mestrado – e são verdadeiras inspirações no Direito e na área de Proteção de Dados.

Ao professor Gustavo Tepedino, por também aceitar o convite para compor a banca. É uma alegria indescritível poder ser avaliada por um dos maiores mestres do Direito Civil brasileiro.

Ao professor Pedro Marcos Nunes Barbosa, que tive a alegria de conhecer na banca de qualificação e que certamente tornou meu trabalho muito melhor.

Ao Angelo Prata de Carvalho, Amanda Visoto, Carlos Ávila e Paula Baqueiro: faltam-me palavras para expressar como vocês deram sentido a todos esses anos de UnB, como me fizeram uma pessoa melhor, mais feliz, mais inteligente e mais completa. Angelo ilumina o caminho de todos nós e leu as mais iniciais versões deste trabalho, acompanhando de perto a evolução da pesquisa. Amanda é a força e a resiliência que nos mantém com os pés no chão (e com a barriga cheia). Carlos nos fornece a companhia perfeita, que vai desde a escuta sempre disponível até a companhia fiel de todos os domingos. E Paula nos mantém engajados, barraqueiros, curiosos e constantemente se esforçando para termos mais encontros presenciais. Em conjunto, vocês me forneceram apoio, confiança e amor imprescindíveis para a conclusão deste trabalho.

À Flávia Ferreira, minha companheira desde a barriga de nossas mães, que se responsabiliza por ser meu HD externo, a memória da minha vida fora do corpo. Obrigada pelo apoio, por estar presente todos esses anos e por acreditar em mim com olhos de admiração que só você tem.

À Lígia Melo, que tanto me inspira na coragem de sair da zona de conforto e alcançar voos mais longes: uma pessoa excepcional, cuja amizade inabalável pelos milhares de quilômetros que hoje nos separam foi fundamental para me dar a confiança necessária à conclusão desta tese. À Marcella Zarattini, pelas caminhadas que trouxeram tranquilidade e pelo apoio perene, honesto e sempre cheio de carinho. Ao Guilherme Fonseca, amigo fiel que conheci dando uma monitoria de Teoria Geral do Direito Privado e que não largo nunca mais.

À Isabela Maria Rosal, Mônica Fujimoto e Gabriel Nami, com quem dividi pedaços da UnB e da jornada profissional, e que contribuíram fortemente com essa pesquisa, fornecendo apoio e amizade (às vezes na modalidade à distância), além de revisão, leitura cuidadosa e indicações de bibliografias que muito agregaram ao trabalho final.

Também não poderia deixar de agradecer à Giuliana Schunck e ao Tiago Zapater, por serem profissionais amigos que tanto me apoiaram na difícil tarefa de conciliar a advocacia com a jornada acadêmica. Em nome deles, do Marcio Polto, Gledson Campos e Tulio Coelho, agradeço aos meus amigos e às minhas amigas de Trench, Rossi e Watanabe pelo cotidiano de mais de 9 anos. Um agradecimento especial à Bruna Silveira e à Mariana Badia, com quem divido uma especial conexão formada no eixo Brasília-São Paulo e que fazem da advocacia um ambiente que tem, antes de tudo, amizade e parceria.

Não menos importantes são os agradecimentos que faço, por fim, à minha família.

Ao Mauricio. Não é fácil criar uma filha pesquisadora, mas seus esforços me permitiram chegar até aqui. Foi você quem lidou com minhas curiosidades incansáveis, com os meus

questionamentos sobre quase tudo. Foi você quem mais ouviu minhas hipóteses sobre a vida e deu o apoio financeiro e emocional para que eu pudesse entregar este trabalho. E no meio disso tudo, nunca deixou dúvida do seu amor por mim e da confiança que tinha na minha trajetória. Obrigada, paizinho. Sei que o velho Zecão estaria orgulhoso de mim, mas certamente estaria muito mais orgulhoso de você por ter me proporcionado tanto para chegar tão longe.

Agradeço também à Cristine Branco e aos meus irmãos Carolina, Alex e Luis Mauricio Lindoso. Obrigada pela rede de apoio, pelo amor de uma vida inteira e pela confiança no meu potencial.

À Olga, por ser meu suporte emocional em toda a jornada do doutorado. Filha canina de uma pandemia, foi (e ainda é) uma companheira inabalável, que não deixou de dormir no sofá ao meu lado nem nos dias mais quentes, nem nos dias mais difíceis.

À Ângela e ao Alberto de Faria, pelo acolhimento na família e pelo amor em forma de companhia, escuta e almoço todas as semanas. Também agradeço ao Gustavo de Faria, que muito me auxiliou com acesso às bibliografias importantes para este trabalho.

Agradeço, por último, ao Henrique de Faria. Um amor de vida, que colocou o doutorado como um projeto da nossa família e empenhou sacrifícios enormes para me ajudar a concluir esta tese. Quem mais acreditou no meu potencial e vivenciou as dores e as delícias de chegar ao final. Você faz parte de cada linha, não só deste trabalho, mas da história que eu construí ao longo dos últimos 8 anos. Que seja apenas o nosso prólogo.

“Dentro de cada ser há um segredo
a que nem a paixão consegue acesso”

Anna Akhmátova

RESUMO

O presente trabalho tem por objetivo explorar a tensão entre transparência e sigilo no mercado de dados pessoais e compreender de que forma essa tensão se intensifica com o uso dos segredos de negócio, considerando as ressalvas previstas na Lei Geral de Proteção de Dados Pessoais (LGPD) em relação a essa categoria jurídica. Para tanto, pretende-se inicialmente identificar as dificuldades já existentes para a concretização da proteção de dados pessoais e a materialização da transparência. A partir disso, pretende-se compreender como os agentes de tratamento podem criar uma opacidade adicional em suas operações a partir de categorias jurídicas, como a dos segredos de negócio. Ao longo do trabalho, objetiva-se demonstrar as repercussões que surgem da possibilidade de escolher o enquadramento legal de elementos essenciais ao mercado, como bases de dados, dados pessoais ou algoritmos. Defende-se que essa não é uma escolha neutra e que os agentes de tratamento podem, muitas vezes, optar pelos segredos de negócio como tal enquadramento, beneficiando-se da sua condição sigilosa para distanciar ainda mais os titulares e as autoridades da necessária explicabilidade sobre suas operações. Adicionalmente, a pesquisa objetiva compreender de que forma a LGPD brasileira se mostrou alheia a importantes discussões sobre segredos e transparência, acabando por criar caminhos que favorecem uma retórica de opacidade por parte dos agentes de tratamento. Ao fim, o trabalho busca trazer reflexões propositivas sobre como se deve pensar o alcance do sigilo conferido aos segredos de negócio e de que maneira se deve orientar a interpretação da LGPD, a fim de que o uso dessas categorias jurídicas não crie dificuldades adicionais para a concretização da garantia fundamental à proteção de dados pessoais.

Palavras-chave: proteção de dados pessoais; segredos de negócio; opacidade.

ABSTRACT

The purpose of this work is to explore the tension between transparency and secrecy in personal data market and to understand how this tension is intensified by the use of trade secrets, considering the mentions of this legal category provided in the Brazilian Data Protection Law (LGPD). To this end, the initial goal is to identify current difficulties in achieving personal data protection and ensuring transparency. From there, the work aims to understand how data controllers can create additional opacity in their operations through legal categories such as trade secrets. Throughout the work, the goal is to demonstrate the repercussions that arise from the ability to choose the legal framework for essential market elements, such as databases, personal data, or algorithms. It is argued that this is not a neutral choice and that data controllers can often opt for trade secrets as such a framework, benefiting from its confidential nature to further distance data subjects and authorities from the necessary explainability of their operations. Additionally, the research aims to understand how the LGPD has overlooked important discussions about secrecy and transparency, ultimately creating paths that favor a rhetoric of opacity on the part of data controllers. Finally, the work seeks to provide reflections on how the scope of confidentiality granted to trade secrets should be reavaluated and how the interpretation of the LGPD should be guided so that the use of these legal categories does not create additional obstacles in realizing the fundamental guarantee of personal data protection.

Keywords: data protection; trade secret; opacity.

SUMÁRIO

INTRODUÇÃO

A expansão constante do mercado de dados pessoais vem trazendo importantes reflexões sobre o atual contexto do capitalismo[1]. Sabe-se que os agentes de tratamento de dados pessoais são atores econômicos que acumulam cada vez mais poder[2], seja pela crescente vigilância dos indivíduos[3]; seja por meio de algoritmos[4], tecnologias de intermediação e direcionamento de conteúdo[5]. Os agentes de tratamento conseguem interferir de forma cada vez mais direta na conformação da personalidade individual e no desenrolar de importantes processos coletivos e sociais[6] – como a formação de opiniões políticas, as eleições[7], a construção de relacionamentos, e outros[8].

Em razão dessas preocupações, foram editadas, ao longo dos anos, normas de proteção de dados e regulações setoriais cujos objetivos primários eram assegurar a proteção das garantias individuais, além de legitimar as operações envolvendo dados

---

[1] Em seu discurso ao receber o Prêmio Nobel de Literatura, Olga Tokarczuk descreveu esse processo de mudança da seguinte forma: "A humanidade percorreu um longo caminho no que diz respeito à transmissão e à partilha da experiência individual, desde a oralidade, dependente da palavra viva e da memória humana, até a revolução de Gutenberg, quando a narrativa passou a ser mediada universalmente pela escrita, perpetuada, codificada, e suscetível de reprodução sem alteraç!ord. A maior conquista dessa jornada foi o momento em que identificamos o próprio pensamento com a escrita, ou seja, um modo concreto de utilização de ideiais, categorias ou símbolos. Hoje, claro, estamos perante uma revolução com implicações semelhantes, quando a experiência pode ser transmitida diretamente, sem a ajuda da palavra impressa". Ao descrever o processo de mudança do processo de transmissão da vivência humana pela superação da escrita, finaliza a autora: "O maior inimigo do texto já não é a imagem, como pensávamos no século XX, preocupados com o impacto do cinema e da televisão. É, na realidade, uma dimensão completamente diferente da experiência do mundo, que afeta diretamente os nossos sentidos". Ver: TOKARCZUK, Olga. Discurso do Prêmio Nobel de Literatura. In:TOKARCZUK, Olga *Escrever é muito perigoso*: ensaios e conferências; tradução Gabriel Borowski. 1ª ed.. São Paulo: Todavia, 2023. pp. 246-247.

[2] RODOTÀ, Stéfano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

[3] *Ibid*.

[4] LESSIG, Lawrence. *Code 2.0*. New York: Basic Books, 2006. p. 1-8.

[5] KITCHIN, Rob. Thinking critically about and researching algorithms. *Information, Communication & Society*, *20:*1, p. 15, 2016. Disponível em: https://doi.org/10.1080/1369118X.2016.1154087. Acesso em: 03 jan. 2024; MENDONÇA, Ricardo F.; FILGEURIAS, Fernando; ALMEIDA, Virgílio. *Algorithmic Institutionalism*. The Change Rules of Social and Political Life. United Kingdom: Oxford University Press, 2023. p. 54.

[6] BEER, David. The social power of algorithms. *Information, communication & society*, 20:1, 1-13, 2016. p. 8-9. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2016.1216147?needAccess=true. Acesso em: 08 abr. 2022.

[7] GILLESPIE, Tarleton. The relevance of algorithms. *In*: GILLESPIE, T.; GILLESPIE, Tarleton; BOCZKOWSKI, Pablo J.; FOOT, Kirsten A. *Media Technologies*: Essays on Communication, Materiality, and Society. MIT Press, 2014. p. 107. Traduzido por Amanda Jurno mediante autorização do autor e da editora. Revisão: Carlos d'Andréa. *§ Parágrafo*, São Paulo, Brasil, v. 6, n. 1. p. 95-121, jan./abr. 2018 Disponível em: https://edisciplinas.usp.br/pluginfile.php/5971548/mod_resource/content/1/722-2195-1-PB.pdf. Acesso em: 25 dez. 2023.

[8] LASH, Scott. Power after Hegemony: Cultural Studies in Mutation? *Theory, Culture & Society*, v. 24, n. 3. p. 55–78, 2007. p. 70-71.

pessoais. No Brasil, apesar de leis anteriores que já tratavam da proteção de dados[9], foi a Lei Geral de Proteção de Dados Pessoais (LGPD) que inseriu um marco normativo principiológico de tutela dos dados pessoais em território nacional[10].

Estruturada em alguns eixos centrais, a LGPD tem como princípio norteador do sistema de proteção de dados pessoais a transparência. Por meio dela, concretizam-se obrigações direcionadas aos titulares de dados e às autoridades, que objetivam materializar a proteção da privacidade dos titulares de dados.

Contudo, apesar dos esforços, são significativas já são as dificuldades de fazer com que a transparência seja um princípio efetivo, capaz de criar deveres e obrigações que tragam aos titulares e às autoridades o conhecimento necessário sobre como se dão as operações envolvendo dados pessoais. Essas dificuldades são tratadas no presente estudo como tipos de opacidade.

A pesquisa se inicia, então, com a compreensão sobre quais são essas diferentes dimensões de opacidade que criam óbices à transparência. A partir das categorias jurídicas desenvolvidas por Jena Burrel[11], foram sistematizadas quatro principais opacidades: (i) os óbices relacionados ao titular dos dados; (ii) as opacidades (*stricto sensu*) inerentes ao funcionamento do sistema; (iii) as dificuldades de concretizar a fiscalização por parte da autoridade; e (iv) os óbices legais e institucionais explorados pelos agentes para dificultar a compreensão das operações.

As três primeiras categorias já haviam sido mapeadas por Burrel em seu trabalho, sendo ela, portanto, um relevante marco teórico a ser explorado. A quarta categoria constitui um esforço da pesquisa e o problema a ser enfrentado ao longo do presente trabalho: pretende-se compreender como um outro tipo de opacidade, chamado de opacidade capitalista[12] ou *black box* jurídico[13], é criada pelos agentes de tratamento, para constituírem uma barreira adicional à compreensão das operações.

---

[9] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo *et al*. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 10-12.

[10] ZANATTA, Rafael Augusto Ferreira. O Uso da Lei Geral de Proteção de Dados Pessoais por Gestores Públicos: Origens e Funções Procedimentais em Políticas Públicas no Brasil. *Revista de Estudos em Organizações e Controladoria-REOC*, ISSN 2763-9673, UNICENTRO, Irati-PR, v. 3, n. 2. p. 221, jul./dez., 2023. Disponível em: https://revistas.unicentro.br/index.php/reoc/article/view/7614. Acesso em: 08 jun. 2024.

[11] BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023.

[12] TIMCKE, Scott. *Algorithms and the end of politics*: how technology shapes 21st-century American life. Bristol: Bristol University Press, 2021. p. 27.

[13] LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. *International Journal of Law and Information*

A hipótese é que os agentes de tratamento não querem disponibilizar amplamente informações sobre suas operações. Dentre outros motivos, isso pode se justificar para que os agentes de tratamento não precisem esclarecer como utilizam o poder que lhes é conferido pelos dados pessoais e pelos algoritmos. Por isso, utilizam o Direito e suas categorias jurídicas para criar uma opacidade e dificultar a materialização da transparência.

Para teste dessa hipótese, o presente trabalho se utiliza das conclusões de Katharina Pistor. A autora observa que o Direito pode servir como um importante instrumento de promoção dos interesses dos agentes econômicos[14]. Aplicando-se suas conclusões ao mercado de dados pessoais, a pesquisa pretende mostrar que os agentes de tratamento utilizam a categoria jurídica dos segredos de negócio para criarem essa outra forma de opacidade sobre suas operações e, assim, conseguirem explorar livremente todas as possibilidades que lhes são franqueadas por meio dos dados pessoais e dos algoritmos.

O presente trabalho é dividido em quatro capítulos. No capítulo 1, pretende-se analisar quais são os elementos essenciais do mercado de dados pessoais e de que forma esses elementos conferem poder aos agentes de tratamento. Pretende-se também analisar como a Lei Geral de Proteção de Dados brasileira institui um marco regulatório principiológico para orientar as operações do mercado e como o sistema principiológico dela está centrado, principalmente, na transparência. Ainda, objetiva-se compreender os óbices tradicionais à materialização da transparência que já foram amplamente mapeados pela doutrina.

No capítulo 2, busca-se analisar como os segredos de negócio se relacionam com o mercado de dados pessoais, e de que forma a categoria jurídica dos segredos pode se mostrar inadequada diante das complexidades que envolvem as operações de dados. O que se verifica é que a escolha pelo tratamento dos elementos do mercado como segredos de negócio é uma escolha política que beneficia os propósitos dos agentes de tratamento, mas que pode acabar prejudicando a materialização da transparência e, por consequência, a autodeterminação informativa e a *accountability*.

No capítulo 3, o objetivo é analisar de que forma os segredos de negócio são utilizados pelos agentes de tratamento para criar um óbice adicional à compreensão sobre

---

Technology, Vol. 27, Issue 2, 2019. p. 122-141. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313916. Acesso em: 10 jan. 2024.

[14] PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019.

como se dão as operações. Pretende-se avaliar de que forma são exploradas lacunas e distorções sobre a condição sigilosa atribuída aos segredos de negócio, e de que modo os agentes de tratamento se apropriam disso para obstarem a materialização da transparência. Ainda, o objetivo do capítulo é compreender como a LGPD ignora a possível inadequação da categoria jurídica dos segredos e cria caminhos adicionais para que o agente consiga limitar os direitos e garantias dos titulares de dados pessoais.

Por fim, o capítulo 4 traz considerações sobre como o direito fundamental à proteção de dados precisa orientar todos os esforços relacionados ao mercado. Assim, pretende-se mostrar que ainda que se supere a inadequação dos segredos de negócio como categoria jurídica para proteger os elementos essenciais do mercado, deve-se buscar uma interpretação da LGPD que prestigie a concretização da transparência e a efetivação das garantias dos titulares, notadamente a autodeterminação informativa. Dessa forma, são propostas reflexões sobre possíveis saídas interpretativas que observem a proteção de dados pessoais como vetor normativo central para quaisquer conflitos entre os direitos dos titulares e a proteção aos segredos de negócio. O capítulo não tem o objetivo de esgotar as reflexões, mas pretende trazer importantes propostas para que o Direito não seja utilizado como instrumento de opacidade, prestigiando interesses de grupos econômicos específicos em detrimento de garantias fundamentais.

CAPÍTULO I: LEGITIMANDO O MERCADO DE DADOS PESSOAIS: ENTRE A PRIVACIDADE E A TRANSPARÊNCIA

I.1 CARACTERÍSTICAS E ELEMENTOS ESSENCIAIS DO MERCADO DE DADOS PESSOAIS

O que se denomina *mercado*[15] *de dados pessoais* comporta atividades muito variadas entre si. Empresas que vendem dados e anúncios; que intermediam relações ou funcionam como plataformas; que desenvolvem pesquisas e tecnologias; dentre tantas outras, enquadram-se nesse grupo por possuírem em comum o uso massivo de dados pessoais como objeto fundamental à exploração de suas atividades econômicas.

Trata-se de um mercado fruto do desenvolvimento tecnológico[16][17] que aprimorou as busca pela atenção ao longo dos anos[18] e conseguiu, pela agregação massiva de

[15] A definição de mercado adotada neste trabalho é aquela desenvolvida dentro da Sociologia Econômica, segundo a qual mercados são arenas socialmente construídas onde ocorrem interações entre elementos econômicos e não econômicos, como elementos culturais, aspectos sociais, políticos e outros (Ver: POLANYI, Karl. The Economy as Instituted Process. *In*: GRANOVETTER, Mark; SWEDBERG, Richard. (Eds). *The Sociology of Economic Life*. Boulder, Westview Press, 1992.). Algumas interações se dão por meio de trocas, reguladas por elementos formais, como leis e regulações, e informais, como relações entre os agentes e interações entre competidores, fornecedores e consumidores (Ver: FLIGSTEIN, Neil; CALDERS, Ryan. *Architecture of Markets. Emerging Trends in the Social and Behavioral Sciences*. John Wiley & Sons, Inc, 2015. p. 1).

[16] Como afirma Patrick J. Deneen: "Nossa natureza tecnológica é causa de elogios e apreensão há milênios, mas foi só na era moderna – grosso modo desde a aurora da industrialização – que entramos no que pode ser chamado de era tecnológica. Embora sempre tenhamos sido criaturas tecnológicas, nossa dependência da tecnologia mudou visivelmente, assim como nossa atitude em relação à tecnologia e nossa relação com ela. É difícil lembrar de obras de poesia, literatura ou música que expressem uma grande paixão da sociedade pela tecnologia no período pré-moderno. Não há grandes obras medievais exaltando a invenção do estribo de ferro ou do colar de cavalo. Nossa relação intelectual e emocional com essas tecnologias – tanto nosso imenso otimismo em relação ao progresso humano, quanto nosso profundo terror causado pelo apocalipse que essa mesma tecnologia pode gerar – é produto dos tempos modernos" (DENEEN, Patrick J. *Por que o liberalismo fracassou?* Editora Âyiné, 2020. p. 127. Tradução de Rogério W. Galindo).

[17] Alguns países vivem a chamada Quarta Revolução Industrial, marcada pelo aprimoramento do digital (em termos de velocidade, profundidade e impacto sistêmico); pela existência de inteligências artificiais e máquinas autônomas; pelo surgimento de novos tipos de dados; pela fusão de várias tecnologias diferentes para impactar o cotidiano humano e, em última medida, pela "interação entre os domínios físicos, digitais e biológicos" (SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016. p. 34-36).

[18] Tim Wu é um clássico autor que estuda o processo de aprimoramento do chamado mercado da atenção: um mercado voltado para captação da atenção dos consumidores em prol do impulsionamento (ou da própria criação) da vontade de consumir. Em seus estudos, há um resgate histórico de como o comércio se desenvolveu ao longo dos anos a partir da constante busca pela atenção, utilizando variados meios de comunicação, os quais evoluíram desde os jornais e rádios até a internet. Em suas conclusões, o autor destaca que a expansão do mercado de dados foi verdadeiramente revolucionária, na medida em que permitiu explorar comercialmente os limites da atenção humana de forma mais direcionada e nichada, a partir dos interesses de cada usuário. Ver: WU, Tim. *The Attention Merchants*. The epic Scramble to Get inside Our Heads. New York: Vintage Books, 2016.

dados[19], explorar comercialmente o comportamento humano e os desdobramentos da personalidade individual (como padrões de comportamento, interações)[20].

A existência desse mercado deveria, contudo, causar estranhamento na sociedade. Afinal, trata-se de um mercado cuja atividade econômica está fundada na exploração da vivência humana; na tentativa de transformação da personalidade em instrumento para o lucro de grandes empresas.

O estranhamento é em grande medida reduzido porque a atividade que envolve o uso comercial de dados pessoais é regulada pelo Direito: foram editadas leis, dentre as quais se inclui a Lei Geral de Proteção de Dados (LGPD, Lei n. 13.709/2018), criando bases legais e circunstâncias autorizando a coleta, o tratamento e a comercialização das informações privadas.

Ocorre que o processo de legitimação da atividade econômica de tratamento de dados pessoais pelo Direito deveria trazer preocupações mais amplamente difundidas entre a população, justamente em razão dos impactos que ela pode trazer. Diante do fluxo informacional intenso da atualidade, a capacidade de fiscalização e regulação da atividade de tratamento de dados se mostra limitada e muitas iniciativas que tentam trazer mais clareza sobre como se dão as operações acabam sendo frustradas.

Maria Rosária Ferrarese leciona que o Direito é muitas vezes percebido como um instrumento apolítico, que serve para promover a eficiência e criar segurança jurídica, ao mesmo tempo em que se mascaram as interferências dos atores privados na estruturação de marcos regulatórios importantes à atividade econômica[21]. Em sentido similar, autores como Ugo Mattei e Laura Neder avaliam de que forma a retórica de proteção ao Estado de Direito pode ser utilizado como um instrumento de legitimação de situações

---

[19] HOFFMANN-RIEM, Wolfang. *Teoria do Direito Digital*: transformação digital: desafios para o Direito. Rio de Janeiro: Forense, 2022. p. 19.

[20] É importante mencionar que a existência dos dados pessoais é tão antiga quanto a vida em sociedade. Os registros históricos que existem sobre diversas civilizações são feitos através de dados, e até mesmo na era moderna, a exploração das informações individuais não é uma novidade, na medida em que sempre foi utilizada com objetivos dos mais variados: para instruir políticas públicas, viabilizar estudos estatísticos e análises mercadológicas, identificar cidadãos e organizar a atividade do Estado, fiscalizar, dentre tantos outros. (Ver: AFFELT, Amy. Big Data, Big Opportunity. *Australia Law Librarian*, vol. 21, n. 2, 2013. p. 1. Disponível em: https://www.researchgate.net/publication/269697881_Big_Data_Big_Opportunity. Acesso em: 11 abr. 2023). A exploração comercial dos dados também é contemporânea à existência do capitalismo, como bem lecionam FAUSTINO, Deivison; LIPPOLD, Walter. *Colonialismo Digital*: por uma crítica hacker-fanoniana. São Paulo: Boitempo, 2023. p. 46. As reflexões que se propõem trazer, contudo, envolvem discussões que consideram a dinâmica contemporânea de dados coletados de forma massiva por meio de instrumentos automatizados.

[21] FERRARESE, Maria Rosaria. Europe and institutional change. Law: from science to "fit for purpose"? *Économie et institutions.* v. 23, p. 1-12, 2015. p. 1-5. Disponível em: https://doi.org/10.4000/ei.5718. Acesso em: 02 jun. 2024.

profundamente desiguais, desconsiderando os impactos que diferentes dinâmicas de poder exercem na alocação de recursos e na construção da justiça[22].

Katharina Pistor igualmente traz considerações nesse sentido e comenta sobre a possibilidade de os agentes econômicos utilizarem o Direito como instrumento de seus interesses. Sendo maleável e resultante de escolhas políticas mutáveis que conformam a estrutura econômica[23], o Direito pode permitir que se construam estruturas que transformam em instrumento de poder e geração de riqueza tudo aquilo que desejam os agentes econômicos[24].

Tais autores fornecem reflexões iniciais para que, nesse primeiro momento, seja possível compreender (i) como existe uma relação de poder no mercado de tratamento de dados pessoais; (ii) como a Lei Geral de Proteção de Dados tentou lidar com esse fenômeno; e (iii) quais são possíveis obstáculos à materialização dos esforços em busca de um direito fundamental à proteção de dados pessoais.

I.1.1 Os elementos essenciais do mercado de dados pessoais

Ao falar no mercado de dados pessoais, é comum falar sobre os agentes de tratamento e sobre os seus elementos principais da atividade econômica, quais sejam os dados pessoais e as tecnologias necessárias para explorá-los.

De acordo com a LGPD, os *agentes de tratamento de dados pessoais* são os atores do mercado. Como gênero, a expressão reflete uma gama não homogênea de pessoas (físicas e jurídicas, de direito público e de direito privado) que coletam e/ou tratam informações privadas dos titulares para as mais variadas finalidades. Nos termos da Lei de Proteção de Dados brasileira, esses agentes são definidos como o conjunto de pessoas responsáveis por tomarem decisões sobre o processo de tratamento de dados e executarem as atividades necessárias para tanto[25].

---

[22] MATTEI, Ugo; NADER, Laura. *Plunder*: When the rule of law is illegal. Blackwell Publishing Ltd., 2008. p. 137. Ao longo do presente estudo, outros autores com reflexões similares também serão explorados.

[23] IRTI, Natalino. A ordem jurídica do mercado. *Revista de direito mercantil, industrial, econômico e financeiro*. Publicação do Instituto Brasileiro de Direito Comercial Comparado e Biblioteca Tullio Ascarelli do Departamento de Direito Comercial da Faculdade de Direito da Universidade de São Paulo. Ano XLVI (nova série), janeiro-março/2007. Malheiros Editores. p. 45.

[24] PISTOR, *op. cit*. p. 11.

[25] O art. 5º, VI, VIII e X da LGPD descreve que os agentes podem ser tratados coletivamente como responsáveis pelo tratamento de dados ou isoladamente com base na atividade desempenhada. O controlador toma as decisões importantes sobre o processo de tratamento e o operador as executa. A categoria criada pela lei não é necessariamente obrigatória, já que cada ente privado pode se organizar de

De forma geral, eles podem decidir sobre os aspectos da atividade (o motivo do tratamento; como ele ocorre; sobre quem será feito; qual a sua finalidade e seu tempo de duração, atividades essas feitas pelo controlador[26]) e/ou efetivamente realizar o tratamento dos dados (decidindo sobre o método ou sistema de tratamento, a forma de armazenamento de dados, o sistema utilizado, dentre outros, o que é feito pelo operador[27]). Também podem coletar dados apenas como consequência de suas atividades fim, sem que isso envolva, necessariamente, o tratamento de conteúdo[28].

Para os objetivos do presente trabalho, serão referenciados como agentes de tratamento de dados apenas aqueles que exploram dados pessoais de forma massiva, fazendo isso como atividade fim ou como meio para o desenvolvimento de outros negócios que dependem, diretamente, do conteúdo que é extraído desses dados[29].

Em relação aos dados e às tecnologias, tem-se que a separação desses dois elementos é possível apenas na teoria. Na prática, ambos os elementos compõem a simbiose necessária ao desenvolvimento do mercado nos termos em que ele se dá hoje. Isso porque dados não são simples informações coletadas isoladamente. São sofisticados processos tecnológicos (a exemplo do *big data*) que conseguem agregar informações variadas em volume, velocidade, variedade, valor e veracidade muito superiores ao que se praticava anteriormente[30].

Os esforços de separação das categorias distintas, contudo, constituem tentativas para melhor avaliar os impactos e as repercussões desses elementos no cotidiano humano

---

acordo com a demanda de seus negócios e simplificar estruturações diante da complexidade e do volume dos dados que são explorados. Ainda, é de se destacar que a figura dos agentes é institucional, a fim de caracterizar os responsáveis pela tomada de decisão e pela efetiva organização do tratamento de dados, excluindo os subordinados e funcionários que prestem serviço dentro da cadeia de operações. Ver: FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 278.

[26] KREMER, Bianca. Os agentes de tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 291-292.

[27] KREMER, *op. cit*.. p. 306.

[28] Existem aqueles agentes (adotando o conceito legal do termo) que não coletam dados pessoais de forma massiva ou em âmbito comercial, mas utilizam essas informações como meio para o exercício de uma atividade fim. É o caso de um médico que coleta dados pessoais de seu paciente. A atividade fim dele é o exercício da medicina e a coleta de dados pessoais é apenas um meio para preencher o prontuário, autorizar o seguro de saúde, cadastrar o paciente no sistema interno da clínica médica, dentre outros. Esses agentes não são o foco do presente estudo.

[29] Apesar de se entender que o tratamento dos dados pode ser considerado a atividade fim, muitas dessas grandes empresas de tecnologia utilizam a venda de anúncios como principal fonte de renda. Por esse motivo, pode-se considerar que sua atividade depende diretamente do conteúdo extraído dos dados, de modo que a exploração do conteúdo em si não é, necessariamente, a atividade econômica em si. A título de exemplo: FOURWEEKBMBA. Receitas do Facebook. Disponível em: https://fourweekmba.com/pt/receitas-do-facebook/. Acesso em: 04 jul. 2024.

[30] HOFFMANN-RIEM, Wolfang. *Teoria do Direito Digital*: transformação digital: desafios para o Direito. Rio de Janeiro: Forense, 2022. p. 19.

e na vivência social. Nesse sentido, dados pessoais, por definição legal, dizem respeito a alguém ou a um grupo de alguéns que é definido ou pode vir a ser. Qualquer informação que se associa a uma pessoa física pode ser tratada como dado pessoal: desde dados cadastrais e informações públicas disponíveis sobre os indivíduos até padrões de comportamento e tempo de uso[31].

A construção de definições isoladas frequentemente necessita de ajustes, justamente em razão de sua conexão tão direta com elementos tecnológicos. A título de exemplo, mencionam-se os dados pessoais inferidos, que resultam de processos criativos dos agentes através de um raciocínio matemático aplicado ao longo das operações de tratamento[32]. É um tipo de dado decorrente dos vários processos tecnológicos, que resulta em uma informação a partir de análises probabilísticas e correlações, mas que não foi necessariamente coletado ou produzido pelo titular a quem essa informação se refere. Ainda, trata-se de um conteúdo que não necessariamente é verídico e sobre o qual muitas vezes o usuário sequer sabe que existe[33].

Dados pessoais, portanto, são categorias mutáveis e amplas, mas cuja definição jurídica pode criar um enquadramento de todos os conteúdos que se referem a um indivíduo identificado ou identificável.

Sistemas de tratamento de dados, por sua vez, também não são tecnologias simples que possam ser reduzidas a algoritmos. Algoritmos são um conjunto de comandos com

---

[31] Destaca-se, como fez Diego Machado, que "Há dado pessoal não apenas quando houver a presença de identificadores diretos ou indiretos que diferem precisamente um indivíduo. Os dados que potencialmente conduzem à individuação da pessoa são igualmente tomados como informação pessoal" (MACHADO, Diego. Considerações iniciais sobre o conceito de dado pessoal no ordenamento jurídico brasileiro. *Civilistica.com*, Rio de Janeiro, v. 12, n. 1. p. 1–34, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/843. Acesso em: 4 maio. 2024. p. 8.

[32] "Por fim, os dados derivados ou inferidos (*derived or inferred data*) são dados resultantes de outros dados pessoais ou não pessoais, sejam eles fornecidos ou observados, devido a raciocínio ou operações lógico-matemáticas não probabilísticas (v. g., deriva-se o país de residência do indivíduo a partir do seu CEP) ou em razão da aplicação de modelos estatísticos complexos baseados em algoritmos de mineração de dados e sistemas de aprendizado de máquina (v. g., escore de crédito). A inferência computacional de dados é fundamental às tecnologias orientadas por dados e sistemas de inteligência artificial. Modelos ou perfis (de grupo ou personalizados) são inferidos, e então formados, a partir do reconhecimento de padrões em bases de dados comportamentais fornecidos e/ou observados (v. g., modelo computacional de *credit scoring* para avaliação de risco de inadimplemento, modelos de identificação de síndromes genéticas pelo processamento de imagem facial)" (MACHADO, Diego; MENDES, Laura Schertel. A proteção dos dados sensíveis inferidos: um comentário ao caso c-184/20 do Tribunal de Justiça Europeu. *In*: *Revista de Direito do Consumidor*. São Paulo: Revista dos Tribunais, vol. 144, nov-dez./2022. p. 101).

[33] Sobre o tema, ver: MACHADO; MENDES, *op cit*. Dados inferidos podem também ser considerados sensíveis se tiverem o simples potencial de criar associações potencialmente discriminatórias em relação a pessoas naturais, ainda que essas informações não sejam necessariamente verdadeiras. Ver: FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 57.

objetivo de realizar tarefas[34]; a linguagem matemática capaz de construir a sintaxe que traduz algum pensamento, opinião, texto, conhecimento ou comportamento[35].

No entanto, não é possível isolar algoritmos dentro de um processo de tratamento de dados, tampouco distinguir até que ponto um dado pessoal existe de forma independente dele. No início do mercado, a sofisticação algorítmica que trouxe o aprimoramento da tecnologia. Desenvolvida em âmbito institucional, organizacional e social, em âmbito local e global, ela permitiu que a conexão se tornasse essencial para a vida humana e que o mercado de dados criasse impactos nos níveis de produtividade, competição, inovação, criatividade e poder[36]. Mas hoje sua expressão depende dos dados pessoais e de uma série de outros elementos complexos para que sejam produzidos os resultados que têm valor comercial relevante para os agentes de tratamento.

Isto é, as operações de tratamento envolvem uma série de combinações de interações (*feedbacks*) dos usuários, conexões entre estruturas matemáticas variadas, aplicativos, redes (*networks*), hardware, dados coletados e produzidos, dentre outros[37], que, em conjunto, permitem a análise massiva das informações privadas e a produção de resultados. Ao falar desses sistemas, deve-se considerar um conjunto de códigos, algoritmos, modelos matemáticos, arquitetura e programações que, apesar de serem diferentes quando se estudam ciência da computação ou programação, em alguns campos do conhecimento (como o Direito) são tratados como uma única coisa[38].

---

[34] DONEDA, Danilo; ALMEIDA, Virgílio. O que é governança de algoritmos. *In*: BRUNO, Fernanda *et al*. *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 143.
[35] HILDEBRANDT, Mireille. *Smart Technologies and the End(s) of Law*. Novel Entanglements of Law and Technology. Northampton, MA: Edward Elgar Publishing, 2015. p. 195.
[36] CASTELLS, Manuel. *The network Society*. A Cross-cultural Perspective. Northampton, MA: Edward Elgar, 2004. p. 42.
[37] MENDONÇA, Ricardo F.; FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Algorithmic Institutionalism*. The Change Rules of Social and Political Life. United Kingdom: Oxford University Press, 2023. p. 29.
[38] Como afirma Mariateresa Maggiolino: "For mathematicians and computer scientists an algorithm is a compound control structure, finite, abstract, effective, imperatively given, and accomplishing a given purpose under given provisions. In other words, an algorithm is a set of precise rules describing a computation process that, when executed, proceeds from an input, goes through a finite number of well-defined steps, and eventually produces an output. Thus, even before the advent of the data economy, an algorithm has always consisted in a sequence of orders and instructions, called to detail a procedure or a decision process meant to realize a given task. However, with the flourishing of firms collecting big data, the word "algorithm" has acquired a more specific – to some extent, narrower – nuance. It does not indicate any mathematical construct that describes the operations to follow to achieve a given objective. It refers to how the said orders and commands are practically implemented and combined into a particular program, software, or information system, with the ultimate goal of inferring from data the answers to be given to a specific set of questions" [Para matemáticos e cientistas da computação, um algoritmo é uma estrutura de controle composta, finita, abstrata, efetiva, dada imperativamente e que realiza um propósito específico sob determinadas condições. Em outras palavras, um algoritmo é um conjunto de regras precisas descrevendo um processo de computação que, quando executado, procede a partir de uma entrada, passa por um número finito de etapas bem definidas e eventualmente produz uma saída. Logo, mesmo antes do advento da economia de dados, um algoritmo sempre consistiu em uma sequência de ordens e instruções, chamadas

Os dois elementos em conjunto – dados pessoais e tecnologia – marcam as mudanças que começaram a ocorrer com a Terceira Revolução Industrial, quando máquinas passaram a desenvolver tarefas autônomas em escala verdadeiramente impossível analogicamente[39]; quando as experiências humanas migraram para o mundo virtual e a sociedade se reorganizou a partir de novas dinâmicas de interação; quando surgiram plataformas digitais para intermediação de interações no mundo virtual a partir de (i) elementos computacionais[40]; (ii) arquitetura[41]; (iii) elementos figurativos[42]; e (iv) interesses políticos[43].

Nesse processo, a experiência humana passou a ter sentido somente quando compartilhada na internet. Trata-se de um fenômeno de plataformização das interações e a virtualização da experiência[44], que fez com que variados tipos de conteúdo, comportamentos e interações fossem transformados em matéria-prima para serem exploradas pelos agentes de mercado[45].

Surgiu simultaneamente um processo de datificação (ou de extrativismo de dados[46]), normalizando o fato de que as informações pessoais agora existiam em

---

para detalhar um procedimento ou um processo de decisão destinado a realizar uma tarefa específica. No entanto, com o florescimento das empresas que coletam *big data*, a palavra 'algoritmo' adquiriu uma nuance mais específica - até certo ponto, mais estreita. Não indica qualquer construção matemática que descreva as operações a serem seguidas para alcançar um objetivo dado. Diz respeito a como as referidas ordens e comandos são implementados e combinados praticamente em um programa, software ou sistema de informação específico, com o objetivo final de inferir a partir de dados as respostas a serem dadas a um conjunto específico de perguntas] (MAGIOLINO, Mariateresa. EU Trade Secret Law and Algorithmic Transparency. *Bocconi Legal Studies Research Paper, n. 3363178,* 2019. p. 3, tradução livre. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363178. Acesso em: 04 abr. 2024).

[39] SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016. Tradução de Daniel Moreira Miranda.

[40] Os elementos computacionais dizem sobre os elementos *online* que descrevem o ambiente. Trata-se do *design* combinado com o uso específico de determinados dispositivos — como *hardware*, sistemas operacionais, computadores, celulares, dentre outros (GILLESPIE, Tarleton. The Politics of "Platforms". *New Media & Society*, vol 12, n. 3, 2010. p. 3, tradução livre. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1601487. Acesso em: 11 nov. 23).

[41] A arquitetura diz sobre a estrutura, o local propriamente onde as interações acontecem, que é viabilizada pelos sistemas algorítmicos (GILLESPIE, *op. cit*., p. 3).

[42] Os elementos figurativos constituem o material metafísico para a indústria física constituir oportunidades: são as ações e *insights* muitas vezes obtidos através de dados comportamentais ou de estudos de mercado, e que permitem fazer com que o processo de intermediação seja perfeito (GILLESPIE, *op. cit*., p. 4).

[43] Os aspectos políticos, por fim, são as escolhas feitas pelos agentes para organizarem a arquitetura e os elementos figurativos, e efetivamente articulam suas opiniões para endereçá-las ao público (GILLESPIE, *op. cit*., p. 4).

[44] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 39.

[45] O termo *datificação* foi primeiro utilizado em 2013, para dizer sobre o processo de transformação dos fenômenos em "formas quantificáveis", para que eles pudessem ser categorizados e analisados, conforme dizem MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data*: A Revolution That Will Transform How We Live, Work and Think. London: John Murray, 2013. p. 78.

[46] O termo extrativismo de dados caracteriza a situação de dependência, a subordinação, a exploração e a relação colonial entre países que apenas fornecem dados para serem explorados, em relação aos países que

ambientes virtuais administrados exclusivamente por agentes privados, através de suas regras próprias e utilizando esses conteúdos em favor de seus interesses capitalistas, ainda que isso possa interferir nos modelos de construção e interação social[47].

Passou a existir um ostensivo processo de substituição da ação humana por sistemas autônomos de leitura de dados pessoais, retirando do indivíduo a sua autonomia e a capacidade de controle sobre aspectos decisórios importantes para o desenvolvimento social[48]. Amplificam-se os sentimentos de solidão e falta de liberdade decorrentes das interações intermediadas por terceiros[49]; de mal-estar relacional e de frustração em razão das conexões artificiais e frágeis estabelecidas pela rede[50]. As interações deixam de ser baseadas no afeto e passam a ser lastreadas em métricas de engajamento que alimentam a riqueza dos agentes de tratamento[51]. Não só, são tomadas decisões em nome do ser humano que determinam fortemente sua personalidade e a forma como ele se insere no mundo[52].

---

efetivamente produzem a tecnologia e vivem a Quarta Revolução Industrial (GIL, Gabriel de Siqueira; HIRSCHFELD, María Noel C. Extrativismo hi-tech e expansão capitalista no século XXI: uma breve contribuição para a crítica latino-americana na era do colonialismo de dados. *In*: PARANÁ, Edemilson; KAMINSKI, Ricardo S. (org.). *Tecnologia e Desenvolvimento nas Américas*: novas fronteiras e dilemas do capitalismo contemporâneo. Curitiba, 2021. p. 186). O resgate às referências coloniais é proposital, para resgatar um regime de exploração e extração abusiva dos recursos dentro de um contexto de subalternização de determinados grupos em prol do crescimento econômico e dos lucros de agentes localizados em países desenvolvidos (COULDRY, Nick; MEJIAS, Ulisses Ali. *The costs of connection*: how data is colonizing human life and appropriating it for capitalism. Stanford, California: Stanford University Press, 2019. p. 53).

[47] MOROZOV, Evgeny. *Big Tech*: A ascensão dos dados e a morte da política. UBU Editora, 2018. p. 165. A palavra extrativismo, é importante lembrar, é um paralelo com os modelos de exploração dos recursos naturais em prol de grandes lucros.

[48] Cabe mencionar as considerações de Nicholas Carr, de que o uso constante das redes e a exposição continuada à internet, por si só, têm trazido mudanças no cérebro humano que podem ser prejudiciais ao desenvolvimento da espécie: são mensuráveis as perdas nas habilidades de comunicação pela fala, memória e concentração. Ver: CARR, Nicholas G. *What the Internet is Doing to Our Brains*. Nova York: Norton, 2010. Bruno Latour igualmente tem considerações relevantes sobre o tema, especialmente no campo da sociologia, ao destacar como atores não humanos estão sempre presentes no processo de conformação do ser humano, e como a vivência hoje não pode mais se isolar de tecnologias e de processos de rede. Suas contribuições integram esforços da sociologia para compreender como as plataformas interferem na experiência humana e no fenômeno digital como um todo. Sobre isso, ver: LATOUR, Bruno. *Reassembling the Social*: An Introduction to Actor-Network-Theory. Oxford: Clarendon, 2005.

[49] DENEEN, Patrick J. *Por que o liberalismo fracassou?* Editora Âyiné, 2020. p. 144-146. Tradução de Rogério W. Galindo.

[50] TURKLE, Sherry. *Alone Together*. Why We Expect More From Technology and Less from Each Other. New York: Basic, 2011.

[51] FISHER, Max. *The Caos Machine*. The inside story of how social media rewired our minds and our world. New York: Little, Brown and Company, 2022.

[52] KOTLIAR, Dan M. The Return of the Social: Algorithmic Identity in an Age of Symbolic demise. *New Media Society,* v. 22, n. 7. p. 1154.

A relação crescente de dependência cega da sociedade[53] com as tecnologias que tratam dados pessoais em massa[54] cria então diferentes dinâmicas de mercantilização da vida humana, de vigilância e de exploração da força produtiva para lucro[55] e de influência na percepção do usuário sobre a realidade[56].

Trata-se de um círculo vicioso, no qual são fornecidos e coletados cada vez mais dados, e expandidas as possibilidades de uso dessas informações. Isso trouxe novas percepções sobre o que são esses conteúdos: no lugar de informações privadas, passaram a ser tratados como se fossem simples elementos de troca (*commodity*), incorporados aos fatores de produção[57]. Sua percepção como capital[58] acabou até sendo legitimada por meio de leis de proteção de dados pessoais no mundo todo, que mesmo demonstrando

---

[53] Dentro da obra Os Saltimbancos, de 1977, já dizia Chico Buarque: "Todos. Proibida a Entrada. Exijo gravata e dados pessoais". A letra retratava, já naquela época, como a expressão do acesso aos dados é determinante para o desempenho de praticamente qualquer atividade social, até mesmo para "[...] tratar uma hospedagem. Para descansar e seguir viagem" (A POUSADA do Bom Barão. Intérprete: Os Saltimbancos. Compositores: Chico Buarque, Luis Bacalov, Sergio Bardotti. *In*: Os Saltimbancos. Intérprete: Os Saltimbancos. [*S. l*] Universal Music Ltd., 1977. 1 CD: faixa 8).

[54] "Existe uma certa relação inseparável entre as plataformas online e as estruturas sociais, mas uma relação na qual as plataformas online não somente espelham o mundo off-line, mas constantemente coproduzem novas estruturas sociais. Esta performatividade através da mediação é um aspecto importante da plataforma de toda a Internet. A plataformização neste sentido significa que uma codificação contínua das integrações humanas e institucionais não se baseia mais nos mecanismos tradicionais de proteção do mercado ou do Estado, mas em novas estruturas e modelos de negócios focados nos efeitos de rede de acumulação e processamento de dados como algoritmos. Neste contexto, a sociabilidade é codificada de uma forma abrangente pela tecnologia" CAMPOS, Ricardo. *Metamorfoses do direito global*: Sobre a interação entre direito, tempo e tecnologia. São Paulo: Editora Contracorrente, 2022. p. 280. Também sobre o tema: VALENTE, Jonas C. L. O poder das plataformas digitais e impactos econômicos e políticos sobre a América Latina. *In*: PARANÁ, Edemilson; KAMINSKI, Ricardo S. *Tecnologia e Desenvolvimento nas Américas*. Novas Fronteiras e Dilemas do Capitalismo Contemporâneo. Curitiba: CRV, 2021. p. 109-110.

[55] FAUSTINO, Deivison; LIPPOLD, Walter. *Colonialismo Digital*: por uma crítica hacker-fanoniana. São Paulo: Boitempo, 2023. p. 46.

[56] MENDONÇA, Ricardo F.; FILGEURIAS, Fernando; ALMEIDA, Virgílio. *Algorithmic Institutionalism*. The Change Rules of Social and Political Life. United Kingdom: Oxford University Press, 2023. p. 30.

[57] MEJIAS, Ulises A.; COULDRY, Nick. Datafication. *Internet Policy Review*, 8 (4), 2019. p. 5. Disponível em: https://doi.org/10.14763/2019.4.1428. Acesso em: 11 nov. 2023.

[58] O capital é um conceito mutável e político que reflete o que o atual momento do capitalismo considera como conjunto de ativos "que podem ser adquiridos, vendidos e comprados em algum mercado" (PIKETTY, Thomas. *O Capital no Século XXI.* Rio de Janeiro: Intrínseca, 2014. p. 51). Há significativa controvérsia sobre o que é considerado capital, especialmente quando se fala em ativos humanos. Thomas Piketty, por exemplo, expressamente exclui ativos humanos do conceito, na medida em que o ser humano não pode pertencer a outra pessoa, "tampouco pode ser comprado e vendido num mercado, ao menos não de modo permanente" (p. 51). Katharina Pistor, cujas conclusões se adotam neste trabalho, entende que o ativo humano pode sim ser enquadrado como capital, na medida em que é possível construir uma estruturação jurídica que permita o enquadramento da mão de obra como capital. Diz Pistor que a mão de obra humana consegue ser convertida em capital por meio de livres associações às empresas. Ainda afirma que bens imateriais, como o *know-how* e a propriedade intelectual seriam também formas de codificação do ser humano e sua *ingenuidade*. Suas conclusões sobre a definição de capital acabam sendo de que qualquer ativo ou bem pode ser transformado em capital, pois isso depende apenas do enquadramento jurídico que se escolhe dar. Ver: PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. pp. 11-12. (PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. p. 11).

preocupações sobre as operações, acabaram autorizando a exploração das informações privadas a partir de uma série de bases legais.

Os dados até têm uma expressão de propriedade[59], mas se consolidou no Brasil o entendimento de que a sua natureza jurídica deveria ser de extensão da personalidade individual[60], por reunirem eles os elementos caracterizadores do indivíduo e determinarem sua essencialidade e seus atributos no mundo virtual[61]. Sendo desdobramentos da personalidade, os dados pessoais gozam de tutela jurídica mais ampla do que aquela atribuída aos direitos reais, além de atrair o regime dos direitos fundamentais na hipótese de uso indevido ou ilegal dos conteúdos[62].

Além de desdobramentos nítidos na esfera individual, dados pessoais também possuem importante dimensão coletiva[63]: conteúdos compartilhados em rede dificilmente

---

[59] Conforme defende LESSIG, Lawrence. The architecture of Privacy. *Taiwan Net '98 conference*, in Taipei, March, 1998. p. 17. Disponível em: https://cs.wellesley.edu/~cs342/fall10/papers/LessigArchitectureOfPrivacy.pdf. Acesso em: 19 jul. 2023.

[60] MAIA, Roberta Mauro Medina. A natureza jurídica da titularidade dos dados pessoais. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 191-192.

[61] TEPEDINO, Gustavo. *A Tutela da Personalidade no Ordenamento Civil-Constitucional Brasileiro*. Temas de Direito Civil. 3. ed. São Paulo: Renovar, 2004. p. 27.

[62] Novamente, cabe destacar o que foi apontado em oportunidade anterior: "Entendendo que os dados pessoais são apenas bem jurídicos, não seria possível deduzir que a divulgação indevida e não autorizada de um dado pessoal estaria violando, também, a privacidade de um usuário. Seria, nessa circunstância, uma discussão restrita apenas ao âmbito do direito de propriedade, envolvendo o uso indevido de um bem pertencente a terceiro. Nesse aspecto, a proteção assegurada pelo direito possui efeitos apenas na esfera patrimonial. Ou seja, apenas o aumento patrimonial indevido, ou a diminuição de um passivo de forma indevida, através da coleta de dados desautorizada, por exemplo, seria punível. Por outro lado, entendendo que os dados pessoais são projeções da própria personalidade, a difusão desautorizada do conteúdo implica na divulgação desautorizada de informações que são atributos da essência do usuário, de suas características mais íntimas e determinantes, assegurando a proteção do usuário também na esfera extrapatrimonial, decorrente, principalmente, da proteção da privacidade (um direito fundamental e constitucionalmente assegurado). Não se ignora o valor comercial dos dados, porque a atribuição da personalidade aos dados pessoais possui natureza mista e também se torna capaz de proteger o usuário dos reflexos patrimoniais indevidos do uso desautorizado de seus dados, mas associá-los à personalidade confere um status jurídico diferenciado para esse tipo de conteúdo, permitindo a proteção do usuário tanto na esfera patrimonial quanto extrapatrimonial" (LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento automatizado de dados pessoais*. Como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021. p. 35-36). Ainda, cabe destacar que diante da relevância dos dados para a conformação da personalidade, sequer seria possível compreender os dados pessoais como extensões do indivíduo. Conforme preleciona Perlingieri, "a tutela da pessoa não pode ser fracionada em isoladas *fattispecie* concretas, em autônomas hipóteses não comunicáveis entre si, mas deve ser apresentada como problema unitário, dado o seu fundamento representado pela unidade do valor da pessoa" (PERLINGIERI, Pietro. *Perfis do direito civil*: introdução ao direito civil constitucional. 3. ed. Rio de Janeiro: Renovar, 2007. p. 155).

[63] É o que dizem Carissa Véliz (VÉLIZ, Carissa. *Privacidade é poder*. Por que e como você deveria retomar o controle de seus dados. São Paulo: Editora Contracorrente, 2021), Daron Acemoglu (ACEMOGLU, Daron. Harms of AI. *National Bureau of Economic Research*. 2021. Disponível em: https://www.nber.org/papers/w29247. Acesso em: 18 nov. 2023), Anita Allen (ALLEN, Anita L. An Ethical Duty to Protec One's Own Information Privacy Allen, Anita L. *Alabama Law Review*, 845, 2013. Disponível em: https://scholarship.law.upenn.edu/faculty_scholarship/451/. Acesso em: 18 nov. 2023) e outros.

dizem respeito a uma única pessoa e ainda podem, por técnicas sofisticadas de inferências e correlações, denunciar comportamentos e padrões de terceiros. Ou seja, qualquer extração de conteúdo advindo dos dados pessoais pressupõe "práticas de extração ligados aos corpos, objetos, instituições, interações e campos que constituem o espaço social"[64].

Contudo, a dimensão de ativo ou bem jurídico é por vezes imposta pelo capitalismo e se torna soberana. Ignora-se que, ainda que sejam tratados como "o novo petróleo", os dados pessoais não são recursos naturais disponíveis[65], mas sim informações sobre indivíduos que efetivamente existem.

O Direito pode ter tido importante contribuição para esse fenômeno, na medida em que viabilizou a existência das bases legais que autorizam a exploração comercial de um desdobramento da personalidade, legitimando uma atividade econômica que deveria ser muito mais limitada.

Katharina Pistor analisa criticamente processos como esse, refletindo que o Direito fornece o conjunto de ferramentas suficientemente flexíveis para que os agentes econômicos exerçam sua criatividade e consigam transformar em ativo qualquer coisa que gere lucro, incluindo o próprio ser humano[66]. Essas reflexões mostram o imbricamento dos interesses privados dentro da construção e interpretação das normas jurídicas, o que será explorado a seguir no contexto específico do mercado de dados pessoais.

---

[64] GIL, Gabriel de Siqueira; HIRSCHFELD, María Noel C. Extrativismo hi-tech e expansão capitalista no século XXI: uma breve contribuição para a crítica latino-americana na era do colonialismo de dados. *In*: PARANÁ, Edemilson; KAMINSKI, Ricardo S. (org.). *Tecnologia e Desenvolvimento nas Américas*: novas fronteiras e dilemas do capitalismo contemporâneo. Curitiba, 2021. p. 178.

[65] COULDRY, Nick; MEJIAS, Ulisses A. A Data Colonialism: rethinking big data's relation to contemporary subject. *Television & New Media*, v. 20, n. 4. p. 336-349, 2019.

[66] PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. p. 12.

I.1.2 As manifestações de poder dos agentes de tratamento de dados pessoais

Os impactos da interação entre os dados pessoais e tecnologias são estudados em vários campos[67][68], que mapearam como impactos (i) a plataformização das interações, (ii) a datificação da experiência humana e (iii) a percepção dos dados pessoais como bens jurídicos que abastecem atividades econômicas muito lucrativas.

Dentre os teóricos que abordam a questão, alguns se destacam por trazerem perspectivas mais críticas sobre como os dados interferiram no desenvolvimento do capitalismo. É o caso de Shoshana Zuboff, que sustenta a ideia de que se vive em uma nova era, chamada de capitalismo de vigilância, na qual os dados pessoais constituem a matéria prima necessária para que os agentes econômicos exerçam o controle social sobre a população[69].

Apesar da relevância de seus estudos em ressaltar diferentes aspectos do atual contexto capitalista, especialmente em razão das diferenças criadas pela exploração massiva dos dados e pela incorporação da tecnologia na vivência humana, não existem alterações estruturais nas características centrais do capitalismo a ponto de justificar que

---

[67] A presença da tecnologia e dos dados igualmente é analisada a partir de seus impactos econômicos. Segundo os estudos desenvolvidos pela chamada Nova Economia, o ambiente econômico se caracteriza também pela intangibilidade das coisas que caracterizam a experiência social e pela interconexão intensa. Nesse contexto, em que setores como de produção de softwares, computadores e de negócios digitais são protagonistas do desenvolvimento econômico, o mercado de dados acaba sendo um grande guarda-chuva para tratar de uma atividade econômica mais ampla, que envolve vários setores de tecnologia, e tem por objetivo final a exploração econômica de dados pessoais. Sobre o tema, ver: KELLY, Kevin. *New Rules for the New Economy*: 10 radical strategies for a connected world. New York: Viking Penguin, 1998 e POSNER, Richard. Antitrust in the New Economy. *Antitrust Law Journal*, v. 68, 2001. p. 926. Disponível em: https://www.jstor.org/stable/40843502. Acesso em: 03 fev. 2024.

[68] A ideia de que o mercado de dados pessoais impacta vários mercados diferentes pode ser analisada sob a perspectiva da teoria dos campos de Bourdieu, que estudou o desenvolvimento da sociedade a partir da concepção de que existem campos de desenvolvimento isolados, regulados por seus próprios conjuntos de regras, sistemas e formas de operação. Dentro de cada campo, determinados agentes são os detentores do capital, ou seja, são os detentores da capacidade de exercer dominância de diferentes formas: econômica, cultural, social ou simbólica. Essa dominância também pode ser exercida fora dos campos, de modo que existem agentes específicos que possuem a capacidade não só de interferir dentro de seus próprios campos, como também dentro de outros campos, a despeito das diferenças de regras e organizações existentes. Essa interferência (que é a detenção do capital) foi chamada de meta-capital, e inicialmente trabalhada por Bourdieu para descrever o papel do Estado, que detém a capacidade de criar regras e interferir em todos os campos. Mas trabalhos recentes também desenvolveram a ideia de que o exercício do meta-capital também é feito pelos agentes que tratam dados pessoais, pois são eles que detêm, através dos algoritmos, o conhecimento necessário para efetivamente impactar em todos os outros campos. Ver: BOURDIEU, Pierre; WACQUANT, Loic. *An invitation to reflexive sociology*. Cambridge: Polity Press, 1992 e LUNDAHL, O. Algorithmic meta-capital: Bourdieusian analysis of social power through algorithms in media consumption. *Information, Communication & Society*, v. 25 (10), 2022. Disponível em: https://research.rug.nl/files/232459855/1369118X.2020.pdf. Acesso em: 10 mar. 2024.

[69] ZUBOFF, Shoshana. *The age of surveillance capitalism.* The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.

se chame o atual momento de uma nova era[70]. Mas existem complexidades adicionais do atual sistema econômico que merecem ser avaliadas. Essas complexidades decorrem do poder que é conferido aos agentes de tratamento por meio dos dados pessoais e das tecnologias.

Foi a coleta e o tratamento de dados em níveis muito elevados que permitiu aos agentes de tratamento adotar novos padrões de monitoramento individual, criando um sistema de vigilância constante de todas as características, desejos e comportamentos dos titulares de dados. O conhecimento reunido sobre os potenciais consumidores e contratantes empoderou os agentes a gerirem e direcionarem o fluxo de informações, realizando nítida interferência nos mais variados processos de tomada de decisão individual[71].

Os agentes se tornaram intermediadores da experiência humana, direcionando opiniões e criando relações que estão cada vez dependentes da tecnologia[72]. Eles conseguem moldar a organização social, institucional, comercial e governamental[73] porque têm conhecimento prévio sobre os fatos, e assim conseguem associar essa informação à venda das certezas obtidas por predições algorítmicas e dados pessoais[74].

É fato que o Direito legitimou esse mercado, mas não se pode ignorar que parte significativa do poder angariado pelos agentes é resultado de longos anos de coleta de dados não regulada e não fiscalizada. Sem dispensar a relevância dos dados coletados

---

[70] "No primeiro caso, tende-se a ignorar, por exemplo, que a coleta, o registro e a análise de dados – à revelia ou não de seus 'proprietários'- bem como as formas de comunicação e controles daí decorrentes, não são exatamente novidade na história do capitalismo. Em alguns desses estudos, o emprego de expressões como 'sociedade da informação', 'capitalismo de plataforma' ou 'capitalismo de vigilância' acaba por sugerir a existência de um 'novo' tipo de sistema social, essencialmente distinto do que havia algumas décadas antes. Essa posição, por vezes, ignora, secundariza ou refuta algumas categorias e conceitos que poderiam auxiliar numa análise histórica do problema (como mais-valor, valor de uso e valor, mercantilização da vida; produção, circulação e consumo; indústria cultural; sociedade do espetáculo; entre outros) fragilizando o debate e a percepção daquilo que permanece do período anterior, embora intensificado ou reconfigurado diante de novas possibilidades tecnológicas FAUSTINO, Deivison; LIPPOLD, Walter. *Colonialismo Digital*: por uma crítica hacker-fanoniana. São Paulo: Boitempo, 2023. p. 46.

[71] KITCHIN, Rob. Thinking critically about and researching algorithms. *Information, Communication & Society*, *20:*1, p. 15, 2016. Disponível em: https://doi.org/10.1080/1369118X.2016.1154087. Acesso em: 03 jan. 2024.

[72] PETERS, Michael A. Algorithmic Capitalism in the Epoch of Digital Reason. *Fast Capitalism*, vol. 14, n. 1, 2017. Disponível em: https://doi.org/10.32855/fcapital.201701.012. Acesso em: 10 mar. 2024.

[73] BEER, David. The social power of algorithms. *Information, communication & society*, 20:1, 1-13, 2016. p. 5. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2016.1216147?needAccess=true. Acesso em: 08 abr. 2022.

[74] ZUBOFF, Shoshana. Caveat Usor: Surveillance Capitalism as Epistemic Inequality. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020. p. 185.

ilegalmente nos dias de hoje, esses momentos históricos anteriores abriram espaço para que as tecnologias se inserissem na vida humana de forma ubíqua e imperceptível[75].

Foi quando os agentes começaram a se valer de uma retórica de eficiência, neutralidade, imparcialidade e isonomia[76], simplesmente por estarem lastreadas em códigos matemáticos[77], apropriando-se de um discurso que cria um suposto senso de superioridade das ciências exatas em razão de critérios que, supostamente, seriam mais objetivos. Mas a retórica é falsa porque a migração de importantes interações entre os cidadãos para um mundo virtual ignora que (i) esses espaços online são administrados e controlados pelos próprios agente e (ii) os próprios códigos carregam elementos subjetivos em sua estruturação.

Ainda assim, surgiu uma autorização implícita para que as tecnologias passassem a substituir a tomada de decisão[78], suprimindo o devido processo legal. As subjetividades inerentes à existência humana[79] foram substituídas pelos vieses e pelas intenções que são

---

[75] De acordo com a Frazão: "O chamado fenômeno de viés da automação (automation bias) sugere que ferramentas de automação influenciam decisões humanas de forma significativas e geralmente ruins. Dois tipos de erros são particularmente comuns: (i) erros de omissão, nos quais as pessoas não reconhecem quando os sistemas automatizados erram e (ii) erros comissivos, nos quais as pessoas seguem os sistemas automatizados sem considerar suas informações contraditórias" (FRAZÃO, Ana. Obstáculos para a consideração de questões éticas nos julgamentos algorítmicos. *In*: FEFERBAUM, Marina *et al*. (coord.). *Ética, Governança e Inteligência Artificial*. São Paulo: Almedina, 2023. p. 45).

[76] Tarleton Gillespie fala que esse discurso veio como estabilizador da confiança social, na tentativa de assegurar "garantias práticas e simbólicas de que suas avaliações são justas e precisas, livres de subjetividade, erro ou tentativa de influência" (GILLESPIE, Tarleton. The relevance of algorithms. *In*: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo J.; FOOT, Kirsten A. Media Technologies: Essays on Communication, Materiality, and Society. MIT Press, 2014. p. 107. Traduzido por Amanda Jurno mediante autorização do autor e da editora. Revisão: Carlos d'Andréa. *§ Parágrafo*, São Paulo, Brasil, v. 6, n. 1. p. 95-121, jan./abr. 2018. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5971548/mod_resource/content/1/722-2195-1-PB.pdf. Acesso em: 25 dez. 2023).

[77] FRAZÃO, Ana. Obstáculos para a consideração de questões éticas nos julgamentos algorítmicos. *In*: FEFERBAUM, Marina *et al*. (coord.). *Ética, Governança e Inteligência Artificial*. São Paulo: Almedina, 2023. p. 38. Ver também: FEENBERG, Andrew. Critical Theory of Technology: An Overview. *Tailoring Biotechnologies*, vol. 1, Issue 1, Winter 2005. p. 52. Disponível em: https://www.sfu.ca/~andrewf/books/critbio.pdf. Acesso em: 09 out. 2023.

[78] "In subjecting human beings to technical control at the expense of traditional modes of life while sharply restricting participation in design, technocracy perpetuates elite power structures inherited from the past in technically rational forms. In the process it mutilates not just human beings and nature, but technology as well. A different power structure would innovate a different technology with different consequences" [Ao submeter os seres humanos ao controle técnico em detrimento dos modos tradicionais de vida, ao mesmo tempo em que restringe fortemente a participação no design, a tecnocracia perpetua estruturas de poder elitistas herdadas do passado em formas tecnicamente racionais. Nesse processo, ela mutila não apenas os seres humanos e a natureza, mas também a própria tecnologia. Uma estrutura de poder diferente inovaria uma tecnologia diferente com consequências diferentes] (FEENBERG, Andrew. Critical Theory of Technology: An Overview. *Tailoring Biotechnologies*, vol. 1, Issue 1, Winter 2005. p. 47-64. Disponível em: https://www.sfu.ca/~andrewf/books/critbio.pdf. Acesso em: 09 out. 2023. p. 54, tradução livre).

[79] CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, 85, 1249, 2008. Disponível em: https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2. Acesso em: 02 mar. 2024.

transportados para os sistemas de tratamento de dados desenvolvidos pelos entes privados[80]. Isso ocorreu, contudo, sem que fosse dada transparência e ciência ampla sobre os direcionamentos que os agentes poderiam fazer na vida de cada pessoa.

O capitalismo conseguiu alienar a população sobre os contextos sociais que impactam no desenvolvimento tecnológico[81]. Também conseguiu suprimir importantes informações sobre como são feitas categorizações de indivíduos a partir de dados pessoais e outras informações que não necessariamente são verdadeiras[82], travestindo os interesses políticos que a vigilância poderia trazer à iniciativa privada de otimização de resultados e melhorias para a população. Não que esses benefícios não tenham sido auferidos, mas isso ocorreu às custas de impactos que sequer são de amplo conhecimento por parte da população.

Os agentes do mercado de dados pessoais hoje realizam interferência direta sobre os titulares, o que se dá de forma cada vez mais imperceptível. Os dados e as tecnologias disponíveis (*big data*, inteligências artificiais, algoritmos preditivos, dentre outros) constituem fontes de poder que são utilizados para vincular a constituição do ser humano aos interesses dos agentes[83]. A possibilidade de criar perfis individuais para trabalhar predições e induções do comportamento individual; de construir formas de direcionamento e manipulação de vontades; influenciar na tomada de decisão e na construção do desejo; e de moldar a personalidade individual, são apenas alguns exemplos de como essa interferência acontece.

---

[80] Sobre o tema, ver: O'NEIL, Cathy. *Weapons of math destruction*. How big data increases inequality and threatens democracy. New York: Crown Publishers, 2016; DONEDA, Danilo; ALMEIDA, Virgílio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20. p. 60-63, 2016. p. 60. Disponível em: https://www.researchgate.net/publication/305801954_What_Is_Algorithm_Governance. Acesso em: 12 nov. 2023; MAGER, Astrid. Algorithmic Ideology. How capitalist society shapes search engines. *Information, Communication & Society*, 15:5, 1-19, 2012. Disponível em: http://dx.doi.org/10.1080/1369118X.2012.676056. Acesso em: 11 nov. 2023.

[81] JOH, Elizabeth E. Feeding the Machine: Policing, Crime, Data & Algorithms. *J. Willians & Marry Bill of Rights Journal*, vol. 26, issue 2, article 3, 2017. p. 292. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3020259. Acesso em: 11 dez. 2023.

[82] Sobre o tema, ver: O'NEIL, Cathy. *Weapons of math destruction*. How big data increases inequality and threatens democracy. New York: Crown Publishers, 2016; DONEDA, Danilo; ALMEIDA, Virgílio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20. p. 60-63, 2016. p. 60. Disponível em: https://www.researchgate.net/publication/305801954_What_Is_Algorithm_Governance. Acesso em: 12 nov. 2023; JOH, Elizabeth E. Feeding the Machine: Policing, Crime, Data & Algorithms. *J. Willians & Marry Bill of Rights Journal*, vol. 26, issue 2, article 3, 2017. p. 292. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3020259. Acesso em: 11 dez. 2023.

[83] WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, n. 2, 2019. p. 13-17; 120. Disponível em: https://ssrn.com/abstract=3248829. Acesso em: 6 abr. 2024.

Com a concentração desse poder nas mãos de poucos agentes, o mercado de dados torna-se um importante meio pelo qual se perpetuam as desigualdades[84] características do capitalismo[85]. Primeiro, porque modifica as condições de acesso aos meios de comunicação e controlam o fluxo informacional a partir de critérios obscuros que são controlados exclusivamente pelos agentes que detêm essas estruturas[86]. Segundo, porque substitui mercados tradicionais, exclui concorrentes[87] e modifica as estruturas de preço com base em métricas que decorrem da sua posição de poder, e não de demandas legítimas de consumidores[88]. Terceiro, porque reestrutura as forças de trabalho, mantendo dinâmicas de exploração de determinadas classes sociais, mas com substituição da mão de obra para aumento dos lucros[89].

As técnicas de coleta e tratamento de dados se tornam, portanto, significativas a ponto de permitirem a construção de um histórico do pensamento humano[90], sendo o insumo necessário para que os agentes de tratamento controlem e orientem o pensamento

---

[84] Desigualdade é um termo genérico para avaliar vários tipos de disparidades e assimetrias que existem na organização social. Sua medição é uma escolha política, que pode refletir escolhas ideológicas muito distintas entre si, constituindo não só um desafio técnico, como também político e filosófico (MEDEIROS, Marcelo. *Os ricos e os pobres*. O brasil e a desigualdade. São Paulo: Companhia das Letras, 2023. p. 50). Não é objetivo do presente trabalho desenvolver esse aspecto específico, mas pretende-se demonstrar como o mercado de dados acentua as diferenças que existem entre os agentes de tratamento e os titulares de dados, gerando maior concentração de riqueza e de poder que trazem, como consequência, impactos sociais relevantes. É isso que será tratado como desigualdade.

[85] ZUBOFF, Shoshana. Caveat Usor: Surveillance Capitalism as Epistemic Inequality. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020. p. 183-195.

[86] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 39. A autora afirma que quando os meios de comunicação ocorriam por mídias tradicionais o dinheiro era a única barreira de acesso a quem quisesse fazer um anúncio, pois pagando, ele seria veiculado para todo o público que tinha acesso àquele meio. Com as plataformas, mesmo pagando, não se tem clareza sobre quem terá acesso ao anúncio e com base em quais critérios.

[87] Existem importantes exemplos sobre como plataformas de busca utilizam de sua capacidade de ranking de resultados para interferir no mercado, prestigiar links patrocinados e até prejudicar concorrentes que não quiseram pagar para serem prestigiados. Isso causa concentração de mercado e interferência nas condições de competição a partir do exercício não transparente de poder pelas plataformas. Sobre o tema, ver: PASQUALE, Frank. The troubling consequences of trade secret protection of search engine rankings. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 385-386; TSCHANG, Hi-Chu. The Squeeze at China's Baidu. *Businessweek*, 2009. Disponível em: https://www.bloomberg.com/news/articles/2008-12-30/the-squeeze-at-chinas-baidu. Acesso em: 23 abr. 24.

[88] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 42.

[89] ACEMOGLU, Daron; RESTREPO, Pascual. The Race between Man and Machine: Implications of Technology for Growth, Factor Shares, and Employment. *American Economic Review*, v. 108, n. 6. p. 1488-1542, 2018. Disponível em: https://www.aeaweb.org/articles?id=10.1257/aer.20160696. Acesso em: 10 fev. 2024.

[90] ZUBOFF, Shoshana. Big Other: Capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda *et al*. *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 40.

individual em prol de seus interesses particulares[91]. E os algoritmos, por serem o elemento essencial de composição da infraestrutura que permite a exploração econômica desses dados, são o instrumento que permite o exercício desse controle[92].

Falar de poder dos dados e das tecnologias é reconhecer que esses elementos fornecem aos agentes que os possuem a capacidade de interferência, de direcionamento e até de construção das opiniões e vontades políticas e individuais. É reconhecer que, legitimada a apropriação desse poder por agentes econômicos, o Direito assume para si a responsabilidade de conseguir limitar seu exercício em prol de um resguardo dos interesses mais amplos que são protegidos pela sociedade.

Isso é o que pretendeu, em certa medida, a Lei Geral de Proteção de Dados.

I.2 A LEI GERAL DE PROTEÇÃO DE DADOS E A TRANSPARÊNCIA NO CONTROLE DE PODER DENTRO DO MERCADO DE DADOS PESSOAIS

I.2.1 Entre poder e privacidade: o uso do Direito como expressão de poder na regulação do mercado de dados pessoais

Diante da capacidade que os dados pessoais e os algoritmos fornecem aos agentes de tratamento, devem existir esforços regulatórios para limitar a forma como o mercado se desenvolve. Esses esforços, é importante destacar, não são resultado de processos apolíticos e voltados exclusivamente para a proteção de garantias fundamentais dos titulares.

Segundo Maria Rosária Ferrarese, existem significativos fenômenos de interferência dos interesses dos agentes privados na construção de modelos do governança. Um desses processos tenta tratar o Direito como uma técnica de aplicação de normas em busca de uma única solução correta, em prol da eficiência e do melhor resultado. Mas o processo de construção das leis e das regulações deve ser visto dentro

---

[91] VÉLIZ, Carissa. *Privacidade é poder*. Por que e como você deveria retomar o controle de seus dados. São Paulo: Editora Contracorrente, 2021. p. 85. Mais recentemente: VÉLIZ, Carissa. *The Ethics of Privacy and Surveillance.* Oxford: Oxford University Press, 2024. p. 149-165; p. 222.

[92] BEER, David. The social power of algorithms. *Information, communication & society*, 20:1, 1-13, 2016. p. 4. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2016.1216147?needAccess=true. Acesso em: 08 abr. 2022.

de sua substância política e ideológica[93], havendo que se ter a necessária preocupação sobre como os fenômenos de poder e os interesses privados são inseridos no Direito[94]. Como também entendem outros autores, o Direito não consiste em um conjunto normativo neutro e objetivo, dissociado de fenômenos sociais e políticos[95].

No processo de construção e interpretação das leis, existem importantes situações que podem reproduzir relações de desigualdade características do capitalismo[96], transformando o Direito em instrumento para atender a determinados interesses. Em um contexto mais amplo, Katharina Pistor trouxe considerações sobre a possível distorção que pode ser promovida pelos agentes a partir de desequilíbrio normativo que por eles é estimulado: seja tentando interferir na edição das leis, seja contratando advogados para atuarem em prol de precedentes judicias, ou seja, ainda, explorando lacunas normativas que favorecem interpretações excessivamente amplas sobre suas atividades, os agentes podem conseguir transformar o Direito em um instrumento de consolidação de seus interesses particulares[97].

De diferentes formas, os agentes tentam se apropriar do Direito para tratá-lo como um instrumento que busca atender a seus interesses, a fim de preservar suas posições de

---

[93] FERRARESE, Maria Rosaria. Europe and institutional change. Law: from science to "fit for purpose"? *Économie et institutions.* v. 23, p. 1-12, 2015. p. 1-2. Disponível em: https://doi.org/10.4000/ei.5718. Acesso em: 02 jun. 2024. Também dizem Hugo Mattei e Laura Nader que "the law (no matter its local style and form) is part of the intimate political and social structure of any society" [a lei (independentemente de seu estilo e forma locais) é parte da estrutura política e social íntima de qualquer sociedade] (MATTEI, Ugo; NADER, Laura. *Plunder*: When the rule of law is illegal. Blackwell Publishing Ltd., 2008. p. 200, tradução livre).

[94] FERRARESE, Maria Rosaria. Governance: a soft revolution with hard political and legal effects. *Soft Power*, [S. l.], v. 1, n. 1. p. 34–56, 2014. p. 55. Disponível em: https://editorial.ucatolica.edu.co/index.php/SoftP/article/view/1765. Acesso em: 2 jun. 2024.

[95] Essas são reflexões interessantes trazidas, desde os anos noventa, por Roberto Mangabeira Unger sobre a teoria crítica dos estudos do Direito. Segundo o autor, o pensamento tradicional do Direito se consolidou ao longo dos anos com base em premissas de objetividade e neutralidade que ignoravam as limitações doutrinárias e interpretativas intimamente influenciadas por ideologias e instrumentos de poder. Mangabeira Unger tem um importante papel para elucidar como o Direito, como instituição, não pode ser visto como apolítico e prático, sendo necessário realizar uma abordagem crítica para melhor compreender seu papel na sociedade. UNGER, Roberto Mangabeira. *The Critical Legal Studies Movement*. Cambridge, Massachusetts: Harvard University Press, 1986. p. 16-39.

[96] Como afirma Pachukanis, as "definições abstratas da forma jurídica não se referem somente a processos psicológicos, mas representam também conceitos que exprimem relações sociais objetivas" (PACHUKANIS, Evguiéni B. *Teoria Geral do Direito e Marxismo.* São Paulo: Editora Acadêmica, 1988. p. 41).

[97] PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. p. 158-180.

poder[98]. Ou seja, o Direito pode assumir um papel de fornecedor da tecnologia de organização social necessária para que os agentes econômicos persigam seus interesses[99].

No mercado de dados pessoais, as preocupações com essas possibilidades devem ser ampliadas, pois se viu que os dados e as tecnologias oferecem um poder de interferência concreto, capaz de modificar e influenciar na forma como se constroem as relações[100]. Se em outros contextos os agentes econômicos precisam se valer de instrumentos indiretos para participarem da conformação do Direito, no mercado de dados pessoais eles conseguem atuar diretamente no processo político, moldando a forma como a opinião pública percebe os fatos e direcionando informações de seu interesse para construção da convicção política dos legisladores.

E os agentes de tratamento têm absoluta ciência do poder que eles possuem, tanto que empenham esforços para interferirem na forma como o Direito será criado[101] e aplicado[102], a fim de ampliarem as possibilidades de coleta de informação e flexibilizarem/dificultarem regras de proteção à privacidade e garantias individuais dos titulares[103]. Exemplos recentes na história mostram que essas tentativas são, inclusive,

---

[98] As críticas de Katharina Pistor merecem ser transcritas sobre esse ponto: "The law is a powerful tool for social ordering and, if used wisely, has the potential to serve a broad range of social objectives; yet, for reasons and with implications that I attempt to explain, the law has been placed firmly in the service of capital" [A lei é uma ferramenta poderosa para a ordenação social e, se utilizada sabiamente, tem o potencial de servir a uma ampla gama de objetivos sociais; no entanto, por razões e com implicações que tento explicar, a lei foi firmemente colocada a serviço do capital] (PISTOR, Katharina. *The Code of Capital. How the Law Creates Wealth and Inequality*. Princeton University Press, 2019. p. xi, tradução livre).

[99] ALAPANIAN, Silvia. A crítica marxista do Direito: um olhar sobre as posições de Evgeni Pachukanis. *Semina*: *Ciências Sociais e Humanas*, Londrina, v. 26. p. 15- 26, set. 2005. p. 17. Disponível em: https://ojs.uel.br/revistas/uel/index.php/seminasoc/article/view/3794/3050. Acesso em: 04 maio 2024. Também: NAVES, Márcio Bilharinho. *Marx*: Ciência e Revolução. São Paulo: Moderna, Campinas, SP, Editora da Universidade de Campinas, 2000. p. 40-42. Diz o autor: "Por que o comunismo não pode se identificar com os 'direitos eternos do homem'? Porque esses diretos decorrem das relações de produção e de troca capitalistas; eles fundam a igualdade universal dos sujeitos de direito sob a base do valor de troca, que torna possível a compra e a venda da força de trabalho, a exploração burguesa. O humanismo (direitos do homem) encobre, assim, a dominação de classe" (p. 41).

[100] POWLES, Julia. The Corporate Culpability of Big Tech. *In*: BANT, Elise. (ed.). *The Culpable Corporate Mind*. Hart Publishing, Oxford: 2023. p. 100-101; AUSTIN, Lisa M. *Enough About Me*: Why Privacy is About Power. A World Without Privacy? What Can / Should Law Do. Cambridge, 2014.

[101] Norberto Bobbio faz importantes reflexões sobre a relação entre poder e Direito, diferenciando considerações que há muito orientam o pensamento jurídico. O autor, contudo, não descarta que uma forma de manifestação de poder no Direito é justamente a de produzir normas no ordenamento jurídico, as quais, por sua vez, vão criar regulações para o poder. Sobre o tema: BOBBIO, Norberto. *Contribución a la teoría del derecho*. Madrid: Editorial Debate, 1990. p. 355-358.

[102] VEDDER, Adam. Privacy 3.0. *In*: GROOTHUIS, Marga; HOF, Simone van der. *Innovating Government*. The Hague: Asser Press, 2011.

[103] AUSTIN, Lisa M. *Enough About Me*: Why Privacy is About Power. A World Without Privacy? What Can / Should Law Do. Cambridge, 2014. p. 22-23.

exitosas, e mesmo diante dos riscos que oferecem, trazem o resultado político esperado pelo agente[104].

A possibilidade de interferência tão direta dos agentes de tratamento desloca parte das preocupações sobre as operações para um eixo mais geral, que busca avaliar de que forma o desenvolvimento do mercado de dados transcende os impactos individuais e pode causar prejuízos na coletividade, em processos sociais, políticos e econômicos[105].

Não existem soluções simples sobre como dimensionar e administrar essa capacidade de interferência. Mas existem esforços que tentam controlar o poder exercido pelos agentes, a fim de orientar a atividade econômica no sentido de valores constitucionais que devem ser observados. Esses são esforços feitos, por exemplo, pela LGPD.

I.2.2 A transparência como mecanismo de proteção da privacidade dos titulares de dados

Os esforços para a regulação do mercado de dados vêm ocorrendo em âmbito mundial e têm por objetivo garantir a proteção dos titulares, bem como a legitimação das atividades e operações dos agentes que coletam, armazenam e tratam dados pessoais[106].

---

[104] Exemplos recentes mostram que plataformas de busca que dominam o mercado utilizaram suas estruturas para enviesarem o resultado de pesquisas e produzirem resultados para induzir a opinião pública e interferir no processo político de importantes votações legislativas. Essas votações tinham por objetivo instituir novos marcos regulatórios para punir e diminuir a divulgação de notícias falsas, no que ficou conhecido como PL das Fake News (PL 2.630/2020). Como resultado, a atividade de coleta e tratamento de dados pessoais iria assumir novos contornos para plataformas de conteúdo, e os agentes passariam a assumir diferentes tipos de responsabilidade por postagens de terceiros. A prática foi apurada pela Secretaria Nacional do Consumidor (SENACON) em razão do abuso na transmissão da opinião repassada ao consumidor como se fosse informação neutra, ensejando a aplicação de multa às empresas e até a retirada do conteúdo de circulação. O resultado, contudo, é que o projeto não foi para votação, tendo a empresa alcançado o resultado que era esperado. Sobre o tema: PODER360. Dino aciona Defesa do Consumidor contra o Google por PL das fake news. *Poder 360*. 2023. Disponível em: https://www.poder360.com.br/governo/dino-aciona-defesa-do-consumidor-contra-o-google-por-pl-das-fake-news/. Acesso em: 01 dez. 2023; LESSA, Henrique. Após multa de R$ 1 milhão por hora, Google retira do ar link contrário a PL. *Correio Braziliense*. 2023. Disponível em: https://www.correiobraziliense.com.br/politica/2023/05/5091532-apos-multa-de-rs-1-milhao-por-hora-google-retira-do-ar-link-contrario-a-pl.html. Acesso em: 01 dez. 2023.

[105] AUSTIN, Lisa M. *Enough About Me*: Why Privacy is About Power. A World Without Privacy? What Can / Should Law Do. Cambridge, 2014. p. 22-23.

[106] Diz o saudoso professor Danilo Doneda: "Muito sinteticamente, esses marcos regulatórios [de proteção de dados pessoais] reconhece os dados pessoais e o seu tratamento como fenômenos juridicamente relevantes, estabelecendo direitos e garantias para os cidadãos, limites para a sua utilização por empresas e organizações e mecanismos que procuram reduzir o risco proporcionado pelo tratamento de dados. Esses elementos são organizados de forma a proporcionar maior controle e proteção ao cidadão sobre seus dados, indo além de uma abordagem vinculada meramente à proteção da privacidade e, ainda, têm como uma de suas consequências mais importantes a consolidação de espaços dentro dos quais os dados pessoais podem

Por se tratar de um mercado cuja essência está fundada na globalização[107], as leis envolvendo proteção de dados pessoais mostram como é importante transcender as fronteiras da jurisdição para pensar em soluções mais amplas na regulação das atividades[108]. Por esse motivo, é frequente analisar experiências de outros países e interpretações sobre institutos diferentes, importando-se soluções e reflexões mais avançadas sobre como aprimorar a proteção dos dados pessoais.

Diferentemente de outras experiências internacionais, nas quais as normas de proteção de dados surgiram de iniciativas civis decorrentes da preocupação com a exploração das informações privadas[109], a LGPD brasileira veio de esforços do Governo Federal, a partir de reuniões do Mercosul, para que o Brasil se inserisse em um contexto global de regulação das operações envolvendo dados pessoais[110]. A consequência disso é

---

ser tratados licitamente, proporcionando garantias para utilizações legítimas de dados pessoais e fomentando espaços de tratamento e livre fluxo de dados" (DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo *et al*. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 4).

[107] Diversos são os autores que buscam analisar de que forma os movimentos de globalização impactaram no desenvolvimento tecnológico e vice e versa. É possível dizer que novas formas de comunicação e fluxo de capital impactaram nos níveis de soberania dos Estados, e que o poder privado conseguiu se expandir em âmbito global. Não necessariamente esses são desdobramentos negativos, mas eles mostram de que forma o desenvolvimento tecnológico e o surgimento de um mercado fundado na exploração de dados pessoais demandam novas reflexões sobre as autoridades nacionais e a capacidade institucional de controle de poder e influência na conformação social (EDWARDS, Michael. *Future Positive*: International Co-operation in the 21st Century. London: Earthscan, 1999. p. 5-6; APPADURAI, Arjun. Disjuncture and Difference in the Global Cultural Economy. *Theory, Culture & Society*, v. 7, n. 2-3, 1990. p. 295-310. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/026327690007002017. Acesso em: 04 maio 2024; CASTELLS, Manuel. *The network Society*. A Cross-cultural Perspective. Northampton, MA: Edward Elgar, 2004).

[108] BERMAN, Paul Schiff. *Global Legal Pluralism*. A Jurisprudence of law Beyond Borders. Cambridge University Press, 2012.

[109] O caso famoso frequentemente mencionado diz respeito à primeira iniciativa de normatização da proteção de dados pessoais, do Condado de Hesse, na Alemanha, em 1970. Outro exemplo mais atual diz respeito às movimentações civis que serviram como fagulha para discussões sobre proteção de dados nos Estados Unidos a partir da proposta de criação do *National Data Center*, como um banco de dados administrado pelo governo que iria reunir grandes quantidades de dados pessoais dos indivíduos. Sobre o tema, ver: DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo *et al*. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 7-11.

[110] Diversos autores destacam que vários são os diplomas anteriores à Lei Geral de Proteção de Dados que delineavam importantes aspectos sobre a proteção dos dados pessoais, como a Lei de Acesso à Informação (Lei 12.527/2011); o Marco Civil da Internet (Lei 12.965/2014), regulamentado posteriormente pelo Decreto n. 8.771/2016; o Código de Defesa do Consumidor que disciplinou, em alguma medida, as bases de dados de consumidores; e a Lei do Cadastro Positivo (Lei n. 12.414/2011), que regulamentou o uso de dados pessoais para análises de crédito e formação de históricos (*credit score*). A legislação prévia não diminui a relevância da LGPD de efetivamente concretizar um sistema, inclusive principiológico, de proteção de dados relevante para o país. Sobre o tema, ver: DONEDA*, op. cit*., p. 10-12; OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *A Lei Geral de Proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019; LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento automatizado de dados pessoais*. Como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021. p. 37.

que no Brasil a cultura de proteção de dados não deu origem à lei e até hoje, anos depois de ela estar em vigor, ainda existem esforços importantes que precisam ser empenhados para que a população brasileira compreenda a relevância de suas informações privadas[111].

Posteriormente à edição da LGPD, pode-se dizer que o sistema de proteção de dados pessoais foi complementado pela transformação da proteção de dados em um direito fundamental[112]. Em decisão histórica do Supremo Tribunal Federal[113], a proteção de dados se consolidou como um mecanismo de limitação do poder dos agentes de tratamento. Na tentativa de restringir os instrumentos de vigilância, decidiu-se que a proteção de dados é forma inegociável de proteção às liberdades e aos direitos individuais[114]. Com a edição da EC n. 115, de 2022, esse entendimento foi consolidado e expressamente inserido no texto constitucional (inciso LXXIX do artigo 5º).

Em termos de estrutura do sistema de proteção de dados, a LGPD consolida importantes princípios[115] a partir de *standards* a serem observados nas operações

---

[111] VERONESE, Alexandre. Os direitos de explicação e de oposição diante das decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD Brasileira. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023. p. RB-14-8.

[112] Importante destacar que o direito à proteção de dados como garantia fundamental não necessariamente foi inaugurado somente com a decisão do STF. Como afirma Sarlet: "a condição de direito fundamental autônomo não depende, em si, de tal expediente, porquanto sobejamente demonstrado que se trata de um direito implicitamente positivado, o que é objeto de amplo consenso doutrinário e mesmo acolhido na esfera jurisprudencial"(SARLET, Ingo Wolfgang. Proteção de Dados Pessoais como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo para a Construção de uma Dogmática Constitucionalmente Adequada. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 14, n. 42. p. 179–218, 2020. p. 213. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 26 maio 2024).

[113] Trata-se do julgamento da ADI 6.387 MC-Ref/DF, julgamento em 6 e 7 maio 2020, de relatoria da Ministra Rosa Weber, julgada em conjunto com as ADIs 389, 6.390, 6.393, 6.388 e 6.387.

[114] MENDES, Laura Schertel. Decisão Histórica do STF reconhece direito fundamental à proteção de dados pessoais: Novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. *JOTA*. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 10 mar. 2024.

[115] Princípios são normas imediatamente finalísticas. Pela definição de Humberto Ávila, diferenciam-se de regras nos seguintes termos: "As regras são normas imediatamente descritivas, primariamente retrospectivas e com pretensão de decidibilidade e abrangência, para cuja aplicação se exige a avaliação da correspondência, sempre centrada na finalidade que lhes dá suporte ou nos princípios que lhes são axiologicamente sobrejacentes, entre a construção conceitual da descrição normativa e a construção conceitual dos fatos. Os princípios são normas imediatamente finalísticas, primariamente prospectivas e com pretensão de complementariedade e de parcialidade, para cuja aplicação se demanda uma avaliação da correlação entre o estado de coisas a ser promovido e os efeitos decorrentes da conduta havida como necessária à sua promoção" (ÁVILA, Humberto. *Teoria dos Princípios*: da definição à aplicação dos princípios jurídicos. 4. ed. São Paulo: Editora Malheiros. p. 70). Também sobre o tema, Gilmar Mendes afasta qualquer controvérsia sobre a natureza normativa das regras e dos princípios. Afirma: "tanto a regra como o princípio são vistos como espécies de normas, uma vez que ambos descrevem algo que deve ser. Ambos se valem de categorias deontológicas comuns às normas – o mandado (determina-se algo), a permissão (faculta-se algo) e a proibição (veda-se algo)". Ver: MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito Constitucional*. 9. ed. rev. e atual. São Paulo: Saraiva, 2014. p. 166-167.

realizadas pelos agentes de tratamento[116]. As perspectivas para tanto estão dispostas inicialmente no art. 2º, incorporando preocupações que já são pacíficas dentro do mercado de dados pessoais e que direcionam a regulação no mundo todo. São preocupações com a justiça (*fairness*) envolvida no tratamento dos dados; com a não discriminação; com o controle do fluxo informacional; com a opacidade e a explicabilidade; e com o direcionamento das operações automatizadas para os interesses sociais[117].

Sendo a linguagem matemática o fundamento do tratamento automatizado da informação, as normas de proteção de dados são diplomas interdisciplinares importantes, que trazem também orientações principiológicas e obrigacionais sobre o *design* dos algoritmos, os resultados produzidos por decisões automatizadas e os vetores normativos que devem ser incorporados em qualquer sistema que explora dados pessoais[118].

Os princípios que devem conduzir o tratamento dos dados pessoais estão dispostos no art. 6º, inciso VI, como uma "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"[119].

Diante das preocupações centrais que envolvem o mercado, é possível afirmar que a transparência constitui um eixo central da LGPD, na medida em que se propõe a criar as condições necessárias para perfectibilizar as garantias fundamentais que envolvem os dados pessoais. Por meio da transparência, importantes elementos do direito fundamental à proteção de dados se consolidam, sendo também um princípio importante para concretizar vários outros – como é o caso da finalidade, do livre acesso e da qualidade.

---

[116] ZANATTA, Rafael Augusto Ferreira. O Uso da Lei Geral de Proteção de Dados Pessoais por Gestores Públicos: Origens e Funções Procedimentais em Políticas Públicas no Brasil. *Revista de Estudos em Organizações e Controladoria-REOC*, ISSN 2763-9673, UNICENTRO, Irati-PR, v. 3, n. 2. p. 204- 235, jul./dez., 2023. p. 221. Disponível em: https://revistas.unicentro.br/index.php/reoc/article/view/7614. Acesso em: 08 jun. 2024.

[117] EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, v. 16, maio 2017. p. 18. Disponível em: https://ssrn.com/abstract=2972855. Acesso em: 10 abr. 2024.

[118] Cabe trazer o que afirma Machado: "Dispondo sobre a atividade de tratamento de dados pessoais, a LGPD é a única lei no sistema jurídico brasileiro a diretamente disciplinar a técnica de perfilamento automatizado com preceitos normativos aplicáveis a ambas as etapas de formação e aplicação de perfis. Esse é um aspecto deveras relevante, pois além de significar a existência de vetores normativos a serem obrigatoriamente observados no *design* e construção das tecnologias de perfilamento, reforça certo pendor de instrumentalidade do direito fundamental à proteção de dados pessoais e a sua normativa infraconstitucional" (MACHADO, Diego. *Algoritmos e Proteção de Dados Pessoais*. Tutela de direitos na era dos perfis. São Paulo: Almedina, 2023. p. 186).

[119] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 maio 2023.

Analisando a disposição legal sobre transparência, pode-se dizer que ela tem duas dimensões: uma formal e uma material. A dimensão formal diz respeito à maneira como se comunicam as informações, especialmente quando elas são direcionadas aos titulares de dados: de forma clara, precisa e acessível, para que o titular consiga compreendê-las, mesmo diante de suas limitações técnicas. O legislador reconhece que existe uma significativa assimetria entre o agente e o titular e, por isso, determina uma necessária adequação da linguagem de comunicação, em todos os momentos, para que ela seja compreensível e consiga transmitir o que é necessário e importante sobre as operações[120].

Desdobramento dessa dimensão formal são as exigências que ficaram conhecidas como um dos campos da privacidade por *design*: cabe aos agentes a adoção de práticas específicas para aprimorarem a proteção da privacidade dos usuários de acordo com o serviço prestado. Os agentes têm o dever de darem visibilidade às operações, possibilitando a compreensão do tratamento de dados e os esforços que são empregados em prestígio à privacidade[121]. A comunicação efetiva, além de empoderar os indivíduos em melhores escolhas, ainda pretende criar maior confiança no mercado e na segurança das operações, aproximando o titular das informações necessárias para que ele acredite que o método, o procedimento e a arquitetura do sistema observam os parâmetros legais e atendem às melhores pretensões de proteção à privacidade[122].

A outra dimensão do princípio da transparência é material, e diz respeito à tentativa de se definir qual é a extensão de informações que devem ser prestadas para que o agente de tratamento esteja em conformidade com a lei[123]. Diz respeito à forma como

---

[120] FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 91.

[121] O termo foi primeiramente utilizado por Ann Cavoukian (CAVOUKIAN, Ann. Privacy by Design The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. *Information & Privacy Commissioner*, Ontario, Canada, v. 5, 2009. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Acesso em: 17 dez. 2020), mas também tem sua ideia indicada em estudos feitos por outros autores, como Lessig, para destacar a importância dos códigos como ferramentas para proteção da privacidade. Dentre os princípios norteadores da privacidade por design, estão a visibilidade e a transparência, justamente como formas de se reconhecer que a proteção da privacidade envolve também compreensão dos titulares de dados sobre os métodos de tratamento, e isso só é possível a partir de uma linguagem customizada e direcionada para cada tipo de serviço fornecido pelo agente. Sobre o tema, ver: LINDOSO, Maria Cristine Branco. Igualdade por design: novas formas de pensar o fim da discriminação por algoritmos e data mining. *Revista de Direito e as Novas Tecnologias*. São Paulo, n.13, out./dez. 2021. Disponível em: https://dspace.almg.gov.br/handle/11037/42710. Acesso em: 11 dez. 2023.

[122] LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. *In*: DONEDA, Danilo *et al*. (coord). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 450.

[123] Nas palavras de Humberto Ávila, seria "definir, também para outros casos, quais são os comportamentos necessários para a realização de um princípio" (ÁVILA, Humberto. *Teoria dos Princípios*: da definição à aplicação dos princípios jurídicos. 4. ed. São Paulo: Editora Malheiros, 2022. p. 74).

se deve orientar a atividade econômica e qual o seu nível de aplicação para o propósito que ele pretende cumprir dentro do mercado de dados pessoais[124].

Há controvérsia sobre como essa dimensão se concretiza, pois as inserções feitas sobre ela ao longo do texto legal são genéricas e não deixam clareza suficiente sobre o que exatamente o titular pode esperar receber ou o que o agente deve ser obrigado a compartilhar, seja para o titular dos dados, seja para a autoridade.

Frank Pasquale foi um dos primeiros defensores de que a transparência deveria ser buscada em extensões máximas, eventualmente se concretizando por meio da abertura das caixas-pretas dos algoritmos que tratam dados pessoais, a fim de torná-los livres para inspeção e escrutínio[125].

Outros autores, por sua vez, defendem que a verdadeira transparência não necessariamente precisaria enfrentar o conteúdo do algoritmo para dar conhecimento aos titulares e às autoridades sobre as operações de tratamento de dados[126]. Nesse sentido, defendem que o processo decisório não estaria lastreado somente no código matemático, envolvendo também toda uma estrutura complexa que sequer poderia ser analisada[127]. A partir disso, argumentam, a transparência seria um conjunto de esforços que envolveriam mecanismos de controle de resultados e fornecimento de informações sobre as operações que envolvem seus dados pessoais[128].

A solução dessa controvérsia deve passar pela compreensão sobre qual é o propósito central da transparência. Ela não se presta somente à função de dar ciência sobre como ocorre o tratamento dos dados pessoais, mas também serve para possibilitar o controle sobre como se manifesta o poder obtido por meio dos dados e da tecnologia[129].

---

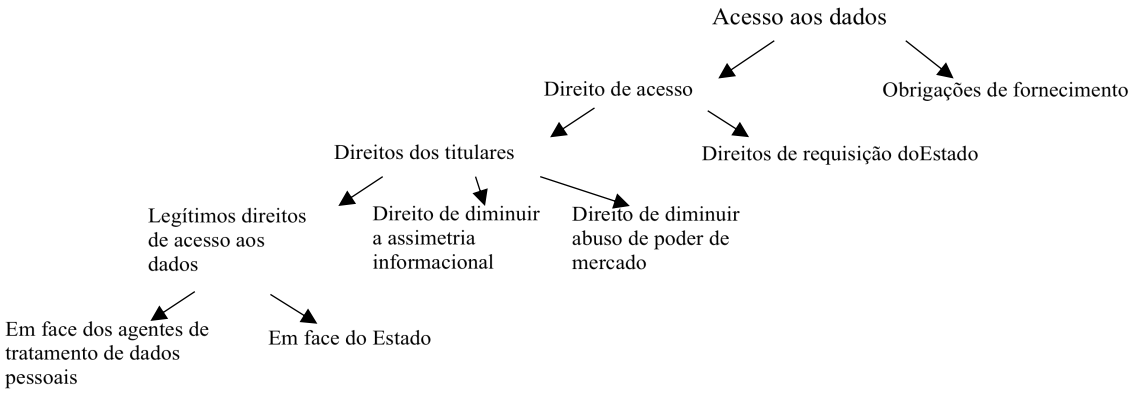
[124] Sobre essa função dos princípios, ver: GRAU, Eros Roberto. *A Ordem econômica da Constituição de 1988* [interpretação crítica]. 14. ed. São Paulo: Editora Malheiros, 2010. p. 73-120.
[125] PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 141.
[126] BUCHER, Taina. *If...Then*: Algorithmic power and politics. Oxford University Press, 2018. p. 45.
[127] BUCHER, *op. cit.*, p. 46.
[128] BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. p. 12. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023.
[129] DIAKOPOULOS, Nicholas. Algorithmic Accountability Reporting: On the Investigation of Black Boxes. *Columbia Journalism School*. 2014. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/D8TT536K/download. Acesso em: 03 nov. 2023.

I.2.3 Os destinatários da transparência e suas formas de materialização

Para melhor refletir sobre transparência, pode-se sistematizá-la em formas de acesso aos dados pessoais e às informações sobre as operações. Através das distintas maneiras de acesso aos conteúdos, fica mais fácil avaliar quem é o destinatário da informação e assim compreender qual o propósito que ela precisa atingir[130].

Considerando o paradigma europeu de proteção de dados, a autora Louisa Specht-Riemenschneider criou uma taxonomia do direito de acesso, a fim de exemplificar a maneira como os dados pessoais devem ser fornecidos:

Figura 1 – Taxonomia dos direitos de acesso aos dados pessoais considerando o paradigma europeu



Fonte: SPECHT-RIEMENSCHNEIDER (2021)[131].

A proposta tem perspectivas interessantes, por mostrar que os dados podem ser acessados não só pelo exercício legítimo de direitos, mas também com o propósito de assegurar o funcionamento do mercado e o controle de poder.

Contudo, pretende-se aprimorar o modelo, inclusive para adequá-lo ao contexto brasileiro, diferenciando os destinatários das informações e as possibilidades de acesso aos dados que estão previstas na LGPD.

---

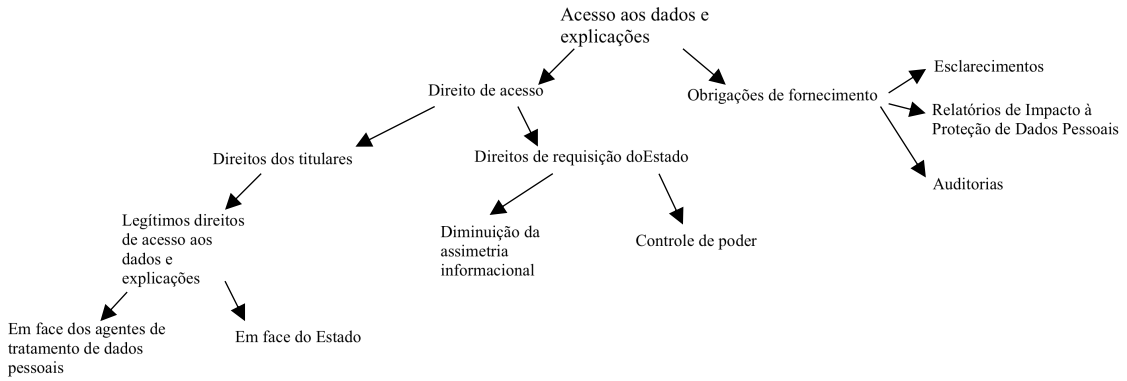
[130] A diferença sobre as expectativas de informações que devem ser fornecidas para os titulares e para as autoridades foi comentada pela Diretora da ANPD, Miriam Wimmer, em seminário (CRUZ, Carolina. Diretora da ANPD aponta limites do segredo comercial. *TeleSíntese*. 2022. Disponível em: https://www.nic.br/noticia/na-midia/diretora-da-anpd-aponta-limites-do-segredo-comercial/. Acesso em: 18 abr. 2024).

[131] SPECHT-RIEMENSCHNEIDER, Louisa. Data access rights – A comparative perspective. *In*: German Federal Ministry of Justice and Consumer Protection | Max Planck Institute for Innovation and Competition (eds.). *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos, 2021. p. 403.

Por exemplo, o direito de acesso aos dados por parte dos titulares não pode ter a pretensão de resolver a assimetria informacional ou corrigir distorções no mercado causadas pelo abuso de poder. Não só o titular não tem acesso às informações suficientes sobre as operações e sobre o mercado para fazer avaliações desse tipo, como também ele tem uma série de dificuldades que impossibilitam um juízo crítico e técnico sobre o tema.

A partir de reflexões desse tipo, propõe-se a seguinte taxonomia, que diferencia o nível de acesso às informações de tratamento de dados a partir da relevância daquele conteúdo para os propósitos a serem desempenhados pelo seu destinatário[132]:

Figura 2 – Diferença do nível de acesso às informações de tratamento de dados



Fonte: Elabora pela autora (2024).

Uma primeira diferença é que, para o que aqui se propõe, o acesso aos dados pode envolver mais informações que não apenas os dados pessoais. O objetivo deve ser materializar a transparência, o que eventualmente implica no acesso não só aos dados em si, mas também a várias outras informações que compõem as operações. A LGPD especifica situações que diferenciam o conteúdo a ser fornecido, mas assegura, como vértice da orientação normativa, que a transparência deve ser perseguida para assegurar a garantia fundamental da proteção de dados, além de outras. Por esse motivo, não se pode entender que o direito de acesso esteja limitado aos dados pessoais.

[132] Como sugerem Maranhão, Junquilho e Tasso, perguntas como "para quem" e "por que" devem ser feitas para avaliar o cumprimento dos propósitos das obrigações de transparência. Os autores falam especificamente sobre inteligências artificiais aplicadas no âmbito do poder judiciário, mas as mesmas perguntas são válidas para se pensar em requisitos de transparência direcionados aos titulares e às autoridades (MARANHÃO, Juliano Souza de Albuquerque; JUNQUILHO, Tainá Aguiar; TASSO, Fernando Antônio. Transparência sobre o emprego de Inteligência Artificial no Judiciário: um modelo de governança. *Suprema - Revista de Estudos Constitucionais*, Distrito Federal, Brasil, v. 3, n. 2. p. 145-187, 2023. p. 154. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/231. Acesso em: 17 maio 2024).

Outra consideração importante sobre o modelo proposto considera, como já mencionado, quem é o destinatário do conteúdo, a fim de avaliar qual o nível de acesso às explicações sobre o tratamento deve ser fornecido[133].

Essas questões serão detalhadas a seguir.

I.2.3.1 *Propósitos da transparência aos titulares de dados: autodeterminação informativa e explicabilidade*

Uma vez que os destinatários são os titulares de dados, é preciso considerar que há uma assimetria informacional significativa, e que as limitações de racionalidade, vieses e heurísticas compõem um conjunto de subjetividades que dificultam (ou até impossibilitam) a compreensão[134].

Por isso, dentre os princípios que se desdobram a partir da transparência, um dos mais significativos em relação aos titulares é o da explicabilidade[135]: um direito de acesso[136], para constituir uma forma de o indivíduo (i) confirmar se há processamento de seus dados ou não; (ii) acessar os dados pessoais que são objeto de operação; e (iii) acessar informações mais gerais sobre o processamento dos dados, como finalidade, duração das operações, compartilhamentos com terceiros, dentre outros[137].

---

[133] A avaliação de como se dá a comunicação da transparência vem sendo estudada no âmbito de processos mais sofisticados, de inteligência artificial, mas é aplicável também para operações de tratamento de dados. Nesse sentido: "Como componente de uma atividade de comunicação, a transparência é sempre relacional: o emissor (a organização) fornece informações (i) relevantes e (ii) adequadas ao (iii) receptor sobre (iv) o sistema de IA. Esses quatro elementos formam os pontos cardeais para definir o conteúdo informativo nessa relação comunicativa" (MARANHÃO, Juliano Souza de Albuquerque; JUNQUILHO, Tainá Aguiar; TASSO, Fernando Antônio. Transparência sobre o emprego de Inteligência Artificial no Judiciário: um modelo de governança. *Suprema - Revista de Estudos Constitucionais*, Distrito Federal, Brasil, v. 3, n. 2. p. 145–187, 2023. p. 153. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/231. Acesso em: 17 maio 2024).

[134] MENDES, Laura Schertel; FONSECA, Gabriel Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista de Estudos Institucionais*, v. 6, n. 2, p-507-533, maio/ago 2020. p. 515. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 11 mar. 2023.

[135] Apesar de ser um requisito frequentemente associado às operações mais complexas de inteligência artificial, nas quais os algoritmos possuem capacidade de aprendizado autônomo, a explicabilidade é aplicável para quaisquer operações algorítmicas em geral, como as que tradicionalmente acontecem no mercado de dados pessoais.

[136] KAMINSKI, Margot E. The Right to Explanation, Explained. *University of Colorado Law Legal Studies Research Paper*, n. 18-24, 15 de junho de 2018. p. 194. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985. Acesso em: 06 jan. 2024.

[137] European Data Protection Board (EDPB). Diretrizes do EDPB sobre o direito de Acesso em conformidade com o Regulamento Geral de Proteção de Dados (GDPR). *EDPB*. 2022. p. 2. Disponível em: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf. Acesso em: 27 fev. 2024; FERRARI, Isabela; BECKER, Daniel. O direito à explicação sobre decisões automatizadas: uma análise comparativa entre a União Europeia e o Brasil. *Revista de Direito e as Novas Tecnologias*, vol.

Essas informações devem respeitar os requisitos formais que estão expressos em lei, a fim de garantir que as limitações do titular não sejam obstáculo à sua compreensão sobre como seus dados são utilizados. O acesso não implica um escrutínio do processo decisório por parte do titular[138], mas deve representar uma possibilidade concreta de conhecimento dos resultados produzidos em um nível de explicação simplificado, porém suficiente, sobre como os modelos foram estruturados.

O objetivo da transparência através da explicabilidade deve ser possibilitar o exercício da autodeterminação informativa: um conceito de origem na jurisprudência alemã, que tenta transcender as preocupações essencialmente patrimonialistas sobre privacidade[139] para refletir uma dimensão existencial desse direito, especialmente frente ao mercado de dados[140].

A ideia é que a proteção da privacidade não deve mais ser percebida como a busca por espaços de isolamento egoístico entre o indivíduo e a sociedade[141]. Ela deve se tornar um mecanismo para assegurar a cada um o direito de desenvolver livremente sua própria personalidade[142], em um esforço que serve, além de tudo, para manter os parâmetros

---

01, out-dez, 2018. p. 7.Disponível em: https://www.oasisbr.ibict.br/vufind/Record/STJ-1_4e5a5817ee8d02db14ed65775a6fce51. Acesso em: 06 jan. 2024.

[138] Em análise sobre o princípio análogo que existe no RGPD, Döhmann detalha que o livre acesso igualmente não permite um escrutínio nas bases de dados e nos *inputs* que são utilizados pelos agentes de tratamento, de modo que até mesmo ele encontra limitações (ainda que elas não sejam claramente definidas pela lei). Ver: DÖHMANN, Indra Spiecker genannt. The legal framework for access to data from a data protection viewpoint – especially under the RGPD. *In*: Bundesministerium Der Justiz Und Für Verbraucherschutz; Max-Planck-Institut Für Innovation Und Wettbewerb. *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos, 2021. p. 189-191.

[139] Bodin de Moares e Quinelato destacam que a origem do direito de privacidade remete "à desagregação da sociedade feudal e a um contexto no qual a privacidade e a intimidade eram privilégios burgueses, a construção de espaços privados acentuou-se com as Revoluções industriais, privilegiando a burguesia que, cada vez mais, se isolaria em relação às demais classes" (BODIN DE MORAES, Maria Celina; QUINELATO, João. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *CADERNOS ADENAUER*, São Paulo, v. 3. p. 1-17, 2019. p. 117).

[140] Diz Albers: "O que caracteriza esse direito à autodeterminação informacional? Seu alcance é maior do que a compreensão clássica do direito à privacidade. Seu elemento central é um direito individual relativamente abstrato e, por isso, amplo de tomar decisões, que se estende desde a divulgação de dados até seu processamento e seu uso"(ALBERS, Marion. A complexidade da proteção de dados. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 10, n. 35. 2016. p. 26. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/93. Acesso em: 4 maio 2024).

[141] COHEN, Julie E. Turning Privacy Inside Out. *Theoretical Inquiries in Law 20.1 (2019 Forthcoming)*, 2018. p. 9. Disponível em: https://ssrn.com/abstract=3162178. Acesso em: 10 out. 2023.

[142] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Revista Pensar*. Fortaleza, v. 25, n. 4. p. 1-18, out./dez. 2020. p. 9-10. Disponível em: https://ojs.unifor.br/rpen/article/view/10828. Acesso em: 23 jun. 2023. Sobre o tema, ver também: PERES FILHO, José Augusto de Souza; TEPEDINO, Gustavo. Autodeterminação informativa e a interseção da proteção de dados com a defesa do consumidor. *In*: MARQUES, Claudia Lima *et al*. (coord). *5 anos de LGPD*: estudos em homenagem a Danilo Doneda [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2023.

democráticos de desenvolvimento social[143]. As possibilidades de exercício podem ir desde a limitação de acesso aos dados até o controle sobre a forma de interferência que as decisões automatizadas podem ter na vida individual[144].

Ou seja, em larga medida, a transparência aos titulares é uma possibilidade de mecanismo de controle, mas com vistas a administrar quais dados sobre si estão sendo utilizados e de que modo[145].

A flexibilidade da autodeterminação informativa faz com que se permita a avaliação de seu cumprimento caso a caso, sendo possível verificar se, nos contextos específicos, os critérios de transparência atendem às necessidades para que o titular compreenda como se dá a operação de dados[146]. Até por isso, o que se tem por privacidade hoje é uma análise contextual de como são utilizadas as informações pessoais[147], fazendo com que esse direito seja tutelado de forma elástica e dinâmica a partir das diferentes relações sociais que existem[148].

Para o exercício completo da autodeterminação informativa, a explicabilidade deve envolver dimensões profundamente amplas. Além da compreensão sobre as operações, ela envolve também a necessidade de o titular entender a importância das operações de dados e qual impacto elas podem ter na vida cotidiana. Em alguma medida,

---

[143] MENDES, *op. cit*., p. 11.

[144] WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, n. 2, 2019. Disponível em: https://ssrn.com/abstract=3248829. Acesso em: 6 abr. 2024.

[145] Os chamados *Fair Information Practice Principles* (FIPPs) foram norteadores da construção de leis de proteção de dados e regulações ao redor de todo o mundo, como destacam Barocas e Nissenbaum (BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. *In*: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. *Privacy, Big Data, and the Public Good*. Frameworks for Engagement. Cambridge University Press, 2014. p. 57.), e demonstram tal dimensão da transparência associada ao controle. Os FIPPs surgiram em 1973 pelo *U.S. Department of Health, Education, and Welfare* (HEW) para endereçar a preocupação que vinha surgindo com o uso de dados. Esses princípios incluem (i) transparência; (ii) direito de saber sobre o uso dos dados e das bases que armazenam conteúdo; (iii) direito de se opor ao uso dos dados sem o consentimento; (iv) direito de correção dos dados; e (v) responsabilização dos agentes que tratarem os dados de forma equivocada. Posteriormente, foram os FIPPs que deram as premissas iniciais para várias leis de proteção de dados e até mesmo para o guia da OCDE de 1980 sobre privacidade. Sobre o tema, ver: SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, v. 126, n. 7, 2013. p. 1882. Disponível em: https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/. Acesso em: 19 maio 2023. A ideia aqui desenvolvida amplia o escopo da discussão proposta, para que o controle possível aos titulares seja aquele direcionado, tão somente, à autodeterminação informativa.

[146] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Revista Pensar*. Fortaleza, v. 25, n. 4. p. 1-18, out./dez. 2020. p. 12. Disponível em: https://ojs.unifor.br/rpen/article/view/10828. Acesso em: 23 jun. 2023.

[147] NISSENBAUM, Helen. *Privacy in context*: technology, policy and the integrity of social life. Palo Alto: Stanford University Press, 2010. p. 2.

[148] NISSENBAUM, *op. cit*., p. 127.

é conseguir ver os agentes de tratamento como atores políticos[149], conseguir retirar um pouco do véu da ubiquidade para enxergar a presença da automatização em importantes escolhas que se desdobram em impactos na personalidade e no desenvolvimento individual[150].

Assim, uma parte importante da transparência também envolve elucidar o poder algorítmico e deixar cristalinas as pretensões nas quais se insere o tratamento de dados pessoais[151].

I.2.3.2 *A transparência direcionada às autoridades: accountability e controle de poder*

Pra as autoridades, a transparência envolve menores dimensões de gestão dos impactos na personalidade individual e maiores aspectos de controle de poder[152].

Dentre os princípios mais relevantes que decorrem da transparência, tem-se o da *accountability* (inciso X, art. 6º): a busca por um sistema de pesos e contrapesos, através de regulações sobre critérios, procedimentos e formas de efetivação de um sistema de proteção e controle dos dados pessoais[153]. Trata-se de um princípio autônomo da LGPD, mas que está diretamente relacionado com a transparência, na medida em que depende de políticas de visibilidade para ser concretizado.

---

[149] GREEN, Ben. Data Science as Political Action: Grounding Data Science in a Politics of Justice. *Journal of Social Computing*, vol. 2, no. 3. p. 249-265, 2021.Disponível em: https://doi.org/10.23919/JSC.2021.0029. Acesso em: 29 mar. 2023.

[150] Nesse sentido, não se ignora que até mesmo o tratamento de dados feito de forma mais simples pode impactar no desenvolvimento da personalidade individual e na construção coletiva. Decisões algorítmicas tomadas sobre quem aparece primeiro nas redes sociais impactam na forma como cada um constrói relacionamentos interpessoais, desenvolve conexões e cria interesses em relação ao outro (FISHER, Max. *The Caos Machine*. The inside story of how social media rewired our minds and our world. New York: Little, Brown and Company, 2022).

[151] DIAKOPOULOS, Nicholas. Algorithmic Accountability Reporting: On the Investigation of Black Boxes. *Columbia Journalism School*. 2014. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/D8TT536K/download. Acesso em: 03 nov. 2023.

[152] Sabe-se que a ANPD encontra, atualmente, níveis de dificuldade no Brasil para se consolidar em uma posição suficientemente robusta para exercer as funções que são descritas nesse tópico. Sendo recente, não se pode esperar que ela consiga ter um nível de maturidade (técnica e operacional) para conseguir desenvolver essas funções tão rapidamente. Mesmo assim, são importantes as críticas que já existem sobre a posição talvez excessivamente branda da autoridade em relação aos agentes e à dificuldade que tem de exercer todas as competências que lhe foram estabelecidas pela LGPD. Sobre a questão, ver: SARLET, Gabriela B. S.; RODRIGUEZ, Daniel P. A Autoridade Nacional de Proteção de Dados (ANPD): Elementos para uma Estruturação Independente e Democrática na Era da Governança Digital. *Revista Direitos Fundamentais & Democracia*, [S. l.], v. 27, n. 3. p. 217–253, 2022. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285. Acesso em: 14 mar. 2024. O propósito do presente estudo não é focar nessas limitações, mas apenas elucidar que algumas das competências que poderiam ser exercidas pela ANPD são limitadas por outros motivos, conforme será detalhado adiante.

[153] VÉLIZ, Carissa. *The Ethics of Privacy and Surveillance*. Oxford: Oxford University Press. p. 149-165. p. 165.

A *accountability* não está presente somente no mercado de dados pessoais, e é incorporada como um dos vetores que orienta várias outras atividades, como as que conduzem a atuação da administração pública. Sua essência é permitir o exercício de um mecanismo de equilíbrio entre a garantia da legalidade, moralidade e eficiência, além de concretizar o direito de informação e a atuação proba e ética[154].

Assim, até mesmo por ser um princípio condutor das atividades do Estado, para a autoridade no âmbito da proteção de dados, a *accountability* constitui uma via de mão dupla: ela deverá adotar condutas transparentes como um dever em relação aos seus cidadãos e poderá reclamar essa transparência dos agentes, como condição primária para exercer sua competência regulatória e fiscalizatória.

A transparência se mostra então essencial para o exercício das competências da Autoridade Nacional de Proteção de Dados (ANPD), pois constitui um mecanismo de equilíbrio nas relações, uma vez que inexistem limitações técnicas e de racionalidade em relação aos agentes de tratamento. Trata-se de um equilíbrio alcançado pela visibilidade de como se dão as operações e como interage o agente com os titulares de dados.

Essa visibilidade não envolve apenas uma pretensão de controle e ciência de como se dá o fluxo informacional, apesar de esse ser um desdobramento relevante. Ela envolve igualmente um esforço de prestação de contas, para que possa construir uma medida de contingenciamento do poder dos agentes de tratamento através da relação entre partes que buscam estimular comportamentos virtuosos por meio da interação e de um vínculo dinâmico[155].

É preciso ter em mente que somente a autoridade poderá averiguar, de forma técnica, se a finalidade foi observada, se os dados coletados são necessários para as operações, como os códigos são estruturados, se eles possuem vieses ou influenciam de forma indevida nos processos decisórios. Sabendo que os algoritmos não são estruturas neutras e imparciais, compete à autoridade entender a forma como os desejos e intenções dos programadores são incutidos nos sistemas, a fim de avaliar, em seguida, se isso se dá de forma adequada e em atenção aos melhores interesses sociais.

Não só, a autoridade busca visibilidade sobre o uso dos dados, com o objetivo de avaliar seus impactos em relação aos titulares e em uma perspectiva coletiva, que

---

[154] FURTADO, Lucas Rocha. *Curso de Direito Administrativo*. 4. ed. Belo Horizonte: Fórum, 2013. p. 91.
[155] BIONI, Bruno Ricardo. *Regulação e proteção de dados pessoais*. O princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 76-78.

transcende os reflexos individuais[156]. Somente a autoridade conseguirá avaliar de que forma aquelas operações impactam no desenvolvimento de características de categorias ou grupos, de que maneira a sociedade pode ser determinada por uma decisão automatizada[157].

É a autoridade[158] que pode, através da materialização da transparência, buscar um verdadeiro equilíbrio entre a atividade de tratamento automatizado de dados e os direitos sociais, em uma tentativa de diminuir a assimetria informacional que existe em relação aos titulares e tornar obrigatória a prestação de contas sobre as operações[159].

Resgatando a taxonomia de acesso que foi anteriormente proposta, é somente a ANPD que pode ter a pretensão de exercer, então, algum tipo de controle de poder sobre a atuação dos agentes de tratamento.

O controle, através da *accountability*, poderá ser efetivado dentro de uma dimensão técnica, por meio da qual os agentes de tratamento terão que produzir provas suficientes, indicando quando, como, em qual extensão e por qual motivo os dados são tratados, a fim de viabilizar a avaliação e a verificação dos critérios de tomada de

---

[156] VÉLIZ, Carissa. *The Ethics of Privacy and Surveillance*. Oxford: Oxford University Press, 2024. p. 160; ACEMOGLU, Daron. *Harms of AI*. 2021. p. 6. Disponível em: https://www.nber.org/papers/w29247. Acesso em: 04 jun. 2024.

[157] TAYLOR, Linnet; FLORIDI, Luciano; VAN DER SLOOT, Bart. Introduction: A New Perspective on Privacy. *In*: TAYLOR, Linnet; FLORIDI, Luciano; VAN DER SLOOT, Bart. *Group Privacy*. New Challenges of Data Technologies. *Philosophical Studies Series*. Dordrecht: Springer, 2017. p. 5-12.

[158] É interessante notar que a ANPD não replica o modelo de atuação regulatória do comando-controle, mas sim tem por premissa uma atuação baseada na regulação responsiva, respaldada no modelo originário de Ian Ayres e John Braithwaite (AYRES, Ian; BRAITHWAITE, John. *Responsive Regulation*: Transcending the Deregulation Debate. New York: Oxford University Press, 1992), que busca maior interação com os entes regulados, a fim de criar normas efetivamente exequíveis e adequadas à realidade dos agentes. Dizem Miriam Wimmer e Octavio Penna Pieranti sobre o modelo de regulação responsiva: "A característica central ao novo modelo é a construção de saídas dialógicas e pactuadas, pressupondo-se a existência de um fluxo regulatório contínuo ('fluxo institucional'). Assim, a regulação passa a ser responsiva à estrutura da indústria regulada; às motivações que importam aos atores regulados; e ao comportamento do regulado" (WIMMER, Miriam; PIERANTI, Octavio Penna. Programas de compliance e a LGPD: a interação entre autorregulação e a regulação estatal. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021. p. 212). Sobre o tema, ver também: FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 445-446. Também é de se destacar que o modelo proposto tem grande lastro no arcabouço teórico de Julia Black, que, dentro da ideia de regulação responsiva, deveria ser incorporado pela ANPD para pensar em um modelo fragmentado, que considere dinâmicas de poder e envolva uma proposta aberta de governança, com ampla participação dos atores sociais. Sobre a questão, ver: BLACK, Julia. Decentering regulation: Understanding the Role of Regulation and Self-Regulation in a "Post Regulatory" World. *Current Legal Problems*, v. 54, Issue 1, 2001. p. 103-146. Disponível em: http://dx.doi.org/10.1093/clp/54.1.103. Acesso em: 08 maio 2023.

[159] SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. *In*: DONEDA, Danilo *et al*. (coord). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 263.

decisão[160]. Mas há também que se considerar a adoção de valores éticos no design dos algoritmos e dos sistemas de tratamento de dados, que permitam uma fácil compreensão sobre seus propósitos, sendo o mais primordial deles a conformidade com a lei[161].

Dentre as possibilidades expressas em lei para efetivar essa *accountability*, há previsão legal de requerer a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIDPD) ou de auditorias.

O Relatório de Impacto trata de um documento elaborado pelo agente, no qual são descritos e avaliados riscos às garantias individuais e aos direitos fundamentais por meio das operações de tratamento de dados que são realizadas pelo agente. Sua obrigatoriedade por parte dos agentes está vinculada (i) ao tratamento dos dados feito com base no legítimo interesse (conforme art. 10, parágrafo 3º, da LGPD); ou (ii) ao tratamento dos dados que pode apresentar risco a alguma das garantias ou princípios gerais da proteção dos dados (arts. 38 e 55-J, XIII, da LGPD)[162].

No Relatório de Impacto, o agente deve fornecer informações detalhadas sobre os dados coletados, a metodologia de tratamento desses dados, descrição dos processos e análises sobre quais medidas de segurança são utilizadas para preservar a segurança desses dados[163]. Também deve fazer uma análise fundamentada sobre o impacto de suas operações, observando um rigor metodológico para essa análise (que deve ser explicado no documento) e justificando, ainda, de que forma as medidas por ele adotada tornam suas operações suficientemente seguras e conformes em relação à lei[164].

A ideia é que o documento forneça as informações necessárias para que a autoridade possa avaliar as operações da forma mais adequada possível[165]. Por isso, quanto maior o nível de detalhamento e mais específicas forem as informações prestadas sobre o funcionamento das operações, maior a efetividade do Relatório de Impacto.

---

[160] DESAI, Deven R.; KROLL, Joshua A. Trust But Verify: A Guide To Algorithms And The Law. *Harvard Journal Of Law & Technology*, v. 31, 2017. p. 11. Disponível em: https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech1.pdf. Acesso em: 13 fev. 2024.

[161] BEER, David. Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society*, 11(6), 2009. p. 985-1002. Disponível em: https://journals.sagepub.com/doi/10.1177/1461444809336551. Acesso em: 12 ago. 2023.

[162] MACHADO, Diego. *Algoritmos e Proteção de Dados Pessoais*. Tutela de direitos na era dos perfis. São Paulo: Almedina, 2023. p. 324.

[163] FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 264.

[164] KLOZA, Dariusz *et al*. The concept of impact assessment. *In*: KLOZA, Dariusz; BUGRESS, J. Peter (org.) *Border Control and New Technologies*: addressing integrated impact assessment. Brussel: ASP, 2021. p. 32.

[165] KLOZA, *op. cit*., p. 32.

No art. 10º, parágrafo 3º, a previsão legal autoriza à autoridade solicitar o Relatório de Impacto quando o tratamento dos dados estiver fundamentado na base legal do legítimo interesse. A proposta se justifica porque o legítimo interesse é uma base legal aberta[166] que permite ao agente coletar e tratar dados pessoais sem a autorização prévia, desde que eles estejam alinhados aos seus propósitos comerciais à finalidade de suas operações e não esvaziem as garantias dos titulares de dados.

O Relatório de Impacto acaba sendo um mecanismo para assegurar que essa base legal será utilizada dentro dos limites estabelecidos na LGPD – qual seja, a necessidade de um benefício concreto ao agente[167] e de uma finalidade legítima para justificar aquela operação[168]. O documento ainda deve avaliar se foi observado o princípio da minimização de dados, além do balanceamento dos impactos sobre o titular com as legítimas expectativas sobre a operação[169]. Por isso, esse desdobramento da transparência acaba sendo crucial para a avaliação sobre o legítimo interesse, não só para comprovar o cumprimento dos critérios mínimos que justificam a referida base legal, mas também para garantir "que a disparidade que aparta o controlador dos dados do titular dos mesmos possa ser mitigada"[170].

A realização de auditorias, por sua vez, não trata de um documento, mas sim da possibilidade de realização de um tipo de análise técnica que deverá permitir avaliar a

---

[166] Como afirma Roberta Mauro Medina Maia, o legítimo interesse foi construído na LGPD a partir de uma técnica legislativa de cláusula geral, que acaba possuindo grau de vagueza e indeterminação compensados por valoração social e maiores esforços interpretativos para conciliar a norma à estrutura principiológica da lei e do ordenamento jurídico. Segundo a autora, "a cláusula geral não regulamenta de maneira específica e exaustiva as 'condutas e consequências que visa estimular ou evitar, de modo que remete o intérprete a um cenário de elementos que transcendem o conjunto normativo do Código Civil, tornando necessário o recurso a tipologias sociais, usos e costumes objetivamente vigorantes em determinada ambiência social'. Como se pode perceber, foi essa a técnica legislativa adotada no art. 10 da LGPD, embora o próprio dispositivo forneça ao intérprete critérios consistentes capazes de auxiliá-lo a definir, diante do caso concreto, se se está ou não diante da hipótese de legítimo interesse do controlador" (MAIA, Roberta Mauro Medina. O legítimo interesse do controlador e o término do tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 100-101).

[167] COMMISSION européenne/Europese Commissie. ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion on the notion of legitimate interests of the data controller. *Opinion 06/2014*. p. 24. Disponível em: https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf. Acesso em: 17 abr. 2024.

[168] BIONI, Bruno Ricardo. Legítimo Interesse: Aspectos gerais a partir de uma visão obrigacional. *In*: DONEDA, Danilo *et. al.* (coord). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2017. p. 164.

[169] BIONI, *op. cit*., p. 164-166.

[170] MAIA, Roberta Mauro Medina. O legítimo interesse do controlador e o término do tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 108-109.

extensão do tratamento de dados[171]. As auditorias podem ser realizadas dentro do escopo da competência fiscalizatória da ANPD (art. 55-J, XVI) e estão expressamente previstas nos casos em que se apuram potenciais aspectos discriminatórios das operações (art. 20, parágrafo 2º).

I.3 OBSTÁCULOS À MATERIALIZAÇÃO DA TRANSPARÊNCIA PARA GARANTIA DA PROTEÇÃO DE DADOS

I.3.1 Os óbices à transparência relacionados ao titular de dados

Ainda que a transparência seja um eixo central à proteção de dados, persistem óbices significativos à sua materialização. Isso quer dizer que o acesso aos dados e às explicações sobre as operações, apesar dos esforços da LGPD, podem ser insuficientes.

Em relação aos titulares de dados, as dimensões de incompreensão sobre como são tratados os dados pessoais podem surgir de diferentes aspectos. A linguagem é um deles.

Ciente da posição de vulnerabilidade e assimetria do titular, o legislador estabeleceu um formato para a comunicação entre o agente e o titular, criando diferentes requisitos e níveis de direcionamento da informação, com condições adicionais para situações que envolvam dados pessoais sensíveis e menores de idade[172].

Contudo, mesmo com os esforços para tornar mais clara e acessível a linguagem, ainda assim a comunicação sobre as operações de tratamento de dados permanecem extensas e ininteligíveis[173]. Na grande maioria dos serviços, ela segue sendo uma barreira

---

[171] Auditorias, além de serem requeridas pelas autoridades, deveriam também ser adotadas espontaneamente pelas próprias empresas. Elas são mecanismos de controle fiscalizatório e podem também ser ferramentas de demonstração para os titulares de dados de que as políticas de privacidade são cumpridas, em uma sinalização importante ao compromisso de transparência. Auditorias externas também auxiliam na adequação normativa e na diminuição de riscos de segurança ao tratamento dos dados, trazendo benefícios para as próprias operações, além de maior conforto para os titulares. Por isso, deveriam ser medidas que, além da previsão legal, eram estimuladas pelo próprio valor ético a elas agregadas, já que a busca por transparência deve ir além do receio punitivo e verdadeiramente ser incorporada como um compromisso por parte dos agentes. Sobre a questão, ver: VÉLIZ, Carissa. *The Ethics of Privacy and Surveillance*. Oxford: Oxford University Press. p. 164.

[172] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil* – RBDCivil: Belo Horizonte, v. 25. p. 83-116, jul./set. 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521. Acesso em: 13 ago. 2024.

[173] Elena Ferrante, em um de seus romances mais famosos, descreve como "as coisas mais difíceis de falar são as que nós mesmos não conseguimos entender" (FERRANTE, Elena. *A filha perdida*. Intrínseca: São Paulo, 2016). A frase pode ser uma forma de traduzir a complexidade que por vezes envolve o mercado de dados pessoais: espera-se do titular de dados uma compreensão das operações cujas premissas básicas ele é incapaz de compreender. Saber os impactos que o mercado de dados pessoais têm na vida humana torna-

em razão da sua complexidade para cognição da população em geral[174], de modo que importantes termos de uso das plataformas e condições de privacidade simplesmente não são lidas[175].

Além da linguagem, o legislador não conseguiu concretizar na transparência deveres suficientes para endereçar as limitações de racionalidade do titular. São questões que impedem a compreensão das operações pois constituem dificuldades na avaliação de custo-benefício, na compreensão da extensão do tratamento dos dados e nos impactos que as operações podem trazer ao indivíduo[176].

Pela LGPD, o titular segue sem ter acesso ao que seria necessário para que ele pudesse compreender como os seus dados de fato estão inseridos em uma cadeia maior de produção de resultados, perfilamentos e tomada de decisão[177]. Em razão da ubiquidade, é até possível afirmar que o titular sequer enxerga como os dados e a tecnologia interferem na sua vivência, ou qual o nível de dependência que têm em relação ao mercado de dados pessoais[178].

---

se uma das maiores dificuldades da vida moderna, porque a estrutura de funcionamento do mercado está distante da maior parte da população.

[174] SOLVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, v. 126. p. 1880, 2013. Disponível em: https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/. Acesso em: 19 maio 2023.

[175] Estudos mostram que se todos os usuários dedicassem tempo para ler as políticas de privacidade de todos os sites que interagem, haveria um impacto financeiro anual de $ 781 bilhões de dólares na economia. Esse custo poderia ser aprofundado se fossem feitas ainda comparações entre as diferentes políticas, a fim de tentar medir custo-benefício e tomar decisões mais informadas. Ver: MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. *In*: *I/S*: A Journal of Law and Policy. Vol. 4:3, 2008: Privacy Year in a Review Issue. Disponível em: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf. Acesso em: 09 set. 2023.

[176] MENDES, Laura Schertel; FONSECA, Gabriel Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista de Estudos Institucionais*, v. 6, n. 2, p-507-533, maio/ago 2020. p. 515. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 11 mar. 2023.

[177] Afirmam Mendes e Fonseca: "Ademais, o fluxo desses dados perpassa por uma complexa rede de atores que os utilizam por meio de práticas e de operações com fins diversos. É impossível que o titular de dados tenha conhecimento prévio de todos esses elementos, não só por limitações de cognição, mas também por questões estruturais. É dizer: seja pela escala em que a informação é processada, seja pela enorme capacidade de agregação da informação pelas novas tecnologias, é improvável que o indivíduo, no momento da coleta, gerencie plenamente algo que ocorrerá no futuro e que envolve inúmeras incertezas acerca de como todas as informações e dados acerca de um indivíduo serão agregados, cruzados ou utilizados" (MENDES; FONSECA, *op. cit*., p. 518).

[178] A frase de Mark Weiser para falar sobre como a ubiquidade se manifesta é pertinente: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" [As tecnologias mais profundas são aquelas que desaparecem. Elas se diminuem dentro do cotidiano até serem impossíveis de se distinguir dele] (WEISER, Mark. The Computer for the 21st Century. *CalmTechnology* (Originally published 09-91: Scientific Americ), tradução livre. Disponível em: https://calmtech.com/papers/computer-for-the-21st-century. Acesso em: 19 jan. 2024. Nesse mesmo sentido, DEVITO, Michael Ann. Adaptive folk theorization as a path to algorithmic literacy on changing platforms. *Proceedings of the ACM Conference on Human-Computer Interaction*, *5* (CSCW2). 2021. p. 3. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3476080. Acesso em: 20 dez. 2023.

Isso justificaria, por exemplo, o que se chama de paradoxo da privacidade[179], no qual preocupações com a coleta excessiva de dados pessoais se contrapõem à conduta dos titulares de compartilharem cada vez mais conteúdo nas redes sociais. Pode-se falar que esse paradoxo é também uma consequência da assimetria existente em relação aos agentes. Ele decorre do poder exercido por meio dos dados e dos algoritmos, que impõem novos padrões de comportamentos sociais aos titulares, especialmente sobre como interagir e se comunicar, forçando assim novos limites para que os dados sejam fornecidos em extensões maiores e de forma "espontânea"[180].

As dificuldades do titular têm ainda uma dimensão de analfabetismo matemático (*technical illiteracy*)[181], pois falta à população a compreensão crítica dos fundamentos da linguagem matemática e do funcionamento das estruturas algorítmicas[182]. Sabe-se que não é trivial ter acesso à matemática necessária para avaliar algoritmos[183]. Mas em uma sociedade que valoriza as ciências exatas como superiores para diversos aspectos da vida humana; que se estrutura a partir de uma tecnocracia; que cria formas de exploração do capital por meio da tecnologia; e que empenha esforços para matematizar conhecimentos sociais[184], algum nível de compreensão dessa linguagem deve ser imprescindível, sob pena de se excluir a população dos processos decisórios mais importantes para a

---

[179] O termo foi trazido primeiramente em 2006 por BARNES, Susan B. A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 1-10, 2006. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/1394. Acesso em: 11 nov. 2023.

[180] SUÁREZ-GONZALO, Sara. Personal data are political. A feminist view on privacy and big data. *In*: *Recerca*, Revista de Pensament i Anàlisi, n. xx. 2019. p. 176. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 11 nov. 2023.

[181] BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. p. 4. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023.

[182] BURRELL, *op. cit*.

[183]Em verdade, essas avaliações se dificultam pelo fato de os códigos comportarem variações que muitas vezes os tornam incompreensíveis para quem não os desenhou. Também existem variações diversas de linguagens matemáticas que permitem estruturar algoritmos, além de diversos tipos de algoritmos que desempenham inúmeras funções, complexificando aspectos técnicos e inviabilizando sua compreensão (BURRELL, *op. cit*., p. 4). Tanto que até mesmo quem estuda ciência da computação e matemática, e que deveria dominar o funcionamento da linguagem matemática, não consegue ter domínio crítico suficiente para avaliar como funcionam os algoritmos principais inseridos no cotidiano hoje. Estudos produzidos mostram que as escolas e faculdades não conseguem cobrir o nível de sofisticação que o mercado alcançou. Mesmo conhecendo os algoritmos, muitos estudantes não conseguem ter compreensão suficiente de quais podem ser seus impactos e qual a importância deles quando inseridos no cotidiano (OELDORF-HIRSCH, Anne; NEUBAUM, German. What Do We Know About Algorithmic Literacy? the Status Quo and a Research Agenda for a Growing Field. *SocArXiv*. November 18, 2021. p. 13. Disponível em: https://doi.org/10.31235/osf.io/2fd4j. Acesso em: 20 dez. 2023).

[184] NOVAES, Henrique; DAGNINO, Renato. O fetiche da tecnologia. *ORG & DEMO*, v. 5 n. 2. p. 189-210, 2004. p. 193. Disponível em: https://revistas.marilia.unesp.br/index.php/orgdemo/article/view/411. Acesso em: 15 out. 2023; FEENBERG, Andrew. Critical Theory of Technology: An Overview. *Tailoring Biotechnologies*, vol. 1, Issue 1, Winter 2005. p. 54. Disponível em: https://www.sfu.ca/~andrewf/books/critbio.pdf. Acesso em: 09 out. 2023.

organização social. A questão, portanto, não é de domínio técnico, mas sim de um nível de compreensão que não seja equiparado ao analfabetismo.

As limitações do titular como dimensões de opacidade se mostram graves para a efetividade da transparência e acabam caracterizando uma situação de hipervulnerabilidade em razão da extensa assimetria[185]. Os motivos dessa situação podem ter várias origens[186], mas fato é que o titular se insere em posição de fraqueza informacional, técnica e econômica, que não consegue ser superada pela lei[187].

Diante dessa posição, mostram-se preocupantes as escolhas do legislador em colocar o consumidor em posições negociais e de consentimento frente ao agente, já que a discrepância de informações disponíveis impede que qualquer decisão no âmbito de um intenso fluxo de dados pessoais seja tomada de forma devidamente informada[188]. Se as limitações que criam a assimetria informacional ainda não foram superadas (se é que podem ser), a lei sequer deveria considerar a possibilidade de estruturar um regime de proteção de dados a partir da manifestação de vontade de uma parte em situação de extrema vulnerabilidade[189].

---

[185] BIONI, Bruno. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019. p. 222.

[186] Existem divisões de gênero e classe que afastam do conhecimento de grande parte da população o acesso ao ensino matemático mais sofisticado e falta investimento significativo na educação para que compreensões sobre algoritmos e sua presença na vida do cotidiano se tornem um conhecimento comum à população. Sobre a questão, ver: BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023 e OELDORF-HIRSCH, Anne; NEUBAUM, German. What Do We Know About Algorithmic Literacy? the Status Quo and a Research Agenda for a Growing Field. *SocArXiv*. November 18, 2021. p. 13. Disponível em: https://doi.org/10.31235/osf.io/2fd4j. Acesso em: 20 dez. 2023.

[187] BIONI, Bruno. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019. p. 222-223.

[188] Como afirma Bioni, o consentimento é há tempos tratado como uma ficção jurídica (i.e. ficção legal do consentimento, conforme SCHWARTZ, Paul M. Internet privacy and state. *Connecticut Law Review*, v. 32. 2000. p. 825. Disponível em: https://paulschwartz.net/wp-content/uploads/2019/01/SCHWARTZ-CK1A-1.pdf. Acesso em: 27 nov. 2023) incompatível com o modelo normativo de proteção de dados que efetivamente se preocupe com as garantias dos titulares. É necessário pensar então em novas estratégias regulatórias, que considerem inclusive dimensões de poder, para que se possa buscar um cenário de proteção de dados efetivo (BIONI, Bruno. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense. 2019. p. 224). Em trabalhos mais recentes, o autor propôs saídas nesse sentido por meio da *accountability*. Ver: BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022.

[189] A crítica aos modelos de consentimento e legitimação das atividades de tratamento de dados que colocam os titulares de dados em posições de negociações com os agentes não são fundadas somente nas limitações dos titulares, mas também nos riscos à privacidade de terceiros. Por vezes, existem dados que estão contidos nos conteúdos autorizados pelos titulares e que não são sobre si. Não só, deveres de transparência também podem acabar ensejando a divulgação de informações sobre terceiros, criando riscos à privacidade que não envolvem somente o indivíduo que consentiu (*data externalities*). Sobre o tema: MACCARTHY, Mark. New Directions In Privacy: Disclosure, Unfairness and Externalities. *I/S*: A Journal of Law and Policy for the Information Society. 425. 2011. Disponível em: https://ssrn.com/abstract=3093301. Acesso em: 27 nov. 2023; BERGEMANN, Dirk; BONATTI, Alessandro; GAN, Tan. The Economics of Social Data. *Cowles*

Essa preocupação resgata algumas das reflexões trazidas anteriormente, sobre como o Direito pode acabar perpetuando algumas situações que prestigiam os interesses privados. Ao manter uma estrutura relacional entre o agente e o titular de dados, a LGPD pode ter pretendido prestigiar a autodeterminação informativa exercida por cada um, mas acabou desvalorizando o impacto que tem a assimetria existente em relação ao agente, e que impede ao titular o exercício de escolhas efetivas.

De alguma maneira, isso acaba prestigiando a posição de quem trata os dados pessoais com propósitos comerciais, naturalizando que operações desse tipo ocorram sem que haja uma compreensão efetiva do titular quanto a seus impactos. Isso implica reconhecer que o poder adquirido a partir dos dados pessoais não foi corretamente dimensionado pela legislação, favorecendo as operações dos agentes de tratamento e ignorando os impactos sociais tão relevantes que a avalanche informativa vem trazendo.

Ao fim, os esforços legislativos para concretizar a transparência mostram alguma preocupação em assegurar que o titular possa exercer sua autodeterminação informativa. Não são, contudo, suficientes, pois autorizam que o mercado de dados se desenvolva explorando um volume expressivo de dados pessoais sem, em paralelo, criar circunstâncias efetivas para a população compreender como isso ocorre.

I.3.2 A opacidade inerente às operações de tratamento de dados

Além das dificuldades que envolvem a figura pessoal do titular de dados, existem questões estruturantes que igualmente constituem barreiras à compreensão completa de como se dão as operações de tratamento. São as opacidades inerentes às operações, considerando-se aqui opacidade no sentido *stricto sensu*, como uma espécie da opacidade *latu sensu*.

Essa opacidade considera que existe uma extensão que é intangível das operações de tratamento, que nunca poderá ser explicada através de critérios de racionalidade, e que é consequência natural da leitura massiva de dados pessoais feita através de algoritmos[190].

Foundation Discussion Paper No. 2203R4. New Haven, Connecticut. 2019. Disponível em: https://www.mit.edu/~bonatti/social.pdf. Acesso em: 27 nov. 2023; ACEMOGLU, Daron *et al*. Too Much Data: Prices and Inefficiencies in Data Markets. *American Economic Journal*: Microeconomics. v. 14, n. 4, 2022. Disponível em: https://www.aeaweb.org/articles?id=10.1257/mic.20200200. Acesso em: 27 nov. 2023.

[190] BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023.

Isso quer dizer que até mesmo os melhores esforços para efetivação da transparência precisarão reconhecer que existem aspectos das decisões algorítmicas, especialmente que envolvem mecanismos de aprendizagem autônoma e *deep learning*, que são inexplicáveis[191].

Não se trata, portanto, de um tipo de assimetria informacional. Independentemente da capacidade racional do ser humano ou dos esforços empenhados para a compreensão dos processos, haverá, ainda assim, uma dimensão intangível cuja compreensão é impossível sobre como os algoritmos leram determinados dados pessoais e produziram aquele resultado.

A opacidade inerente ocorre por diferentes motivos: a complexidade dos algoritmos[192] e sistemas de aprendizado autônomo que tornam mais difícil rastrear os caminhos do processo decisório[193]; o fluxo informacional é cada vez mais volátil, "de difícil determinação, interminável e imprevisível"[194]; além dos processos de coleta de dados que extrapolam a finalidade e a necessidade, dificultando a compreensão de quais são os *inputs* que verdadeiramente contribuíram para o resultado[195]. As expectativas de explicação das decisões algorítmicas também são um elemento já mencionado, pois estão fundadas em critérios de racionalidade humana, ao passo que as associações feitas durante o tratamento de dados observam outra lógica[196].

---

[191] BUSUIOC, Madalina. Accountable artificial intelligence: holding algorithms to account. *Public Administration Review*, v. 81, n. 5. p. 825-836, Sept./Oct. 2021. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293. Acesso em: 18 abr. 2024.

[192] Autores inclusive dizem, nesse sentido, que algoritmos não são transparentes por natureza. Ver: PEREL, Maayan; ELKIN-KOREN, Niva. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, n. 181, 2017. p. 181. Disponível em: https://scholarship.law.ufl.edu/flr/vol69/iss1/5/. Acesso em: 18 fev. 2024.

[193] Cf. EUROPEAN Parliament. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html. Acesso em: 15 abr. 2024.

[194] BIONI, Bruno Ricardo. *Regulação e proteção de dados pessoais*. O princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 207.

[195] DESAI, Deven R.; KROLL, Joshua A. Trust But Verify: A Guide To Algorithms And The Law. *Harvard Journal Of Law & Technology*, v. 31, 2017. p. 26. Disponível em: https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech1.pdf. Acesso em: 13 fev. 2024.

[196] Inclusive, uma parte importante do poder que se associa ao *big data* é justamente essa capacidade, que transcende critérios de racionalidade, através de mecanismos de correlações e autoaprendizagem que não são lineares ou previsíveis, encontrando caminhos novos para relacionar grandes volumes de informações e produzirem o resultado esperado (COULDRY, Nick; MEJIAS, Ulisses Ali. *The costs of connection*: how data is colonizing human life and appropriating it for capitalism. Stanford, California: Stanford University Press, 2019. p. 310). Ver também: DONEDA, Danilo; ALMEIDA, Virgílio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20. p. 60-63, 2016. p. 60. Disponível em: https://www.researchgate.net/publication/305801954_What_Is_Algorithm_Governance. Acesso em: 12 nov. 2023; BUSUIOC, Madalina. Accountable artificial intelligence: holding algorithms to account. *Public Administration Review*, v. 81, n. 5. p. 825-836, Sept./Oct. 2021. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293. Acesso em: 18 abr. 2024.

Não só, os sistemas de tratamento de dados, em seus diferentes níveis de complexidade, são resultado de diversas camadas de interação. Isso quer dizer que diversos elementos também impactam a performance dos algoritmos e alteram a forma como ele produz resultados[197]. Como exemplo, o ambiente, os dados que são fornecidos, os parâmetros, os métodos, os objetivos, as escolhas de implementação daquele sistema (todos esses, inclusive, controlados por um programador), o programa, a linguagem, o tipo específico de *hardware*, o *feedback* dos usuários, a configuração (como o tipo de processador, as interferências de rede ou a possibilidade de vários programas estarem funcionando simultaneamente), dentre outros[198].

Sistemas mais complexos de inteligências artificiais e internet das coisas, que envolvem aprendizagem autônoma de algoritmos (os quais também são sistemas de leitura de dados[199]), trazem ainda mais dimensões para essa questão. Em razão da grande quantidade de dados coletados[200] e das associações autônomas feitas a partir de redes (em semelhanças cognitivas com o cérebro[201] e em níveis de abstração que transcendem a capacidade humana[202]), torna-se ainda mais difícil fazer qualquer rastreio de como o processo decisório foi tomado. E esse nível de incompreensão não é somente por parte do

---

[197] DESAI, Deven R.; KROLL, Joshua A. Trust But Verify: A Guide To Algorithms And The Law. *Harvard Journal Of Law & Technology*, v. 31, 2017. p. 28. Disponível em: https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech1.pdf. Acesso em: 13 fev. 2024.

[198] De forma sintética, Kartik e Miller definiram que os resultados algorítmicos sofrem interferência de três elementos principais: os dados, as pessoas e os códigos. Com base nessa simplificação, os autores demonstram como é complexo obter respostas ao funcionamento algorítmico e até mesmo identificar qual camada de influência mais interferiu na produção do resultado (KARTIK, Hosanagar; MILLER, Alex P. Who Do We Blame for the Filter Bubble. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020. p. 103-121).

[199] Aqui cabe mencionar que algoritmos em geral podem também ser caracterizados de acordo com a necessidade de serem programados ou não. Apesar de algoritmos programados terem maior grau de rastreabilidade das operações (e que ainda assim pode não ser absoluta), os algoritmos não programados possuem um nível de sofisticação maior. São os chamados *learners*, que consegue descobrir novos inputs a partir dos outputs que ele próprio produziu. O próprio algoritmo faz ajustes nas variáveis para produzir resultados de forma independente. Sobre a diferenciação: FERRARI, Isabela. O emprego de algoritmos para a Tomada de Decisões I – Como funcionam os algoritmos não programados? *In*: FERRARI, Isabela. *Justiça Digital*. São Paulo: Thomson Reuters Brasil, 2020. p. 73.

[200] LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 9-11. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

[201] MEDON, Felipe. *Inteligência Artificial e Responsabilidade Civil*: autonomia, riscos e solidariedade. São Paulo: Editora JusPodivm, 2022. p. 110-112.

[202] KAUFMAN, Dora; JUNQUILHO, Tainá; REIS, Priscila. Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e direitos humanos. *Revista de Direitos e Garantias Fundamentais*, [S. l.], v. 24, n. 3. 2023. p. 52. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/2198. Acesso em: 17 abr. 2024.

usuário do sistema, mas também do desenvolvedor, que muitas vezes não consegue compreender como os resultados chegaram a ser produzidos[203].

Ainda, a opacidade inerente ao tratamento dos dados não diz respeito somente às fórmulas matemáticas complexas, mas também aos elementos laterais. São os vieses cognitivos e as decisões particulares dos desenvolvedores, juntamente com os critérios, métodos e outros elementos do sistema que são igualmente importantes para compreender o funcionamento da estrutura[204]. Assim, fica impossível compreender como a decisão foi tomada pelo algoritmo, já que diferentes elementos contribuíram, em proporções imensuráveis, para o resultado.

É possível dizer então que a opacidade inerente aos sistemas é um óbice à transparência. Há um nível de inexplicabilidade das decisões automatizadas que sempre vai existir, sejam elas mais simples ou mais complexas. E ainda que os agentes sejam obrigados a detalhar como os sistemas funcionam, existirá uma parte das associações, das correlações, da leitura de dados que somente poderá ser avaliada por meio dos resultados. Por esse motivo, é inclusive comum dizer que sistemas algorítmicos não foram construídos com base na transparência, porque por vezes essa busca poderá ser inatingível[205].

A preocupação quando se pensa em transparência é então conseguir compreender exatamente qual é a extensão da opacidade inerente aos algoritmos, e de que forma é possível controlar os resultados produzidos[206].

I.3.3 Deveres decorrentes da transparência quando direcionada à Autoridade Nacional de Proteção de Dados

---

[203] COECKELBERGH, Mark. Artificial intelligence, responsibility attribution, and a relational justification of explainability. *Science and Engineering Ethics*, v. 26, 2020. p. 2060. Disponível em: https://link.springer.com/article/10.1007/s11948-019-00146-8. Acesso em: 12 mar. 2024.

[204] PEREL, Maayan; ELKIN-KOREN, Niva. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, n. 181, 2017, p. 188-189. Disponível em: https://scholarship.law.ufl.edu/flr/vol69/iss1/5/. Acesso em:18 fev. 2024.

[205] PEREL; ELKIN-KOREN, *op. cit*., p. 188-189.

[206] Essa é a diferença epistemológica que alguns autores adotam entre compreensão e explicação, no sentido de que a transparência esperada de sistemas autônomos não necessariamente irá envolver a exata compreensão de como ocorrem as associações entre os dados. Ela irá envolver a explicação, dentro do que é possível, para como os resultados foram produzidos. Sobre o tema, ver: STUEBER, Karsten R. Understanding Versus Explanation? How to Think about the Distinction between the Human and the Natural Sciences. *Inquiry*, v. 55, n. 1. p. 17–32, 2012. Disponível em: https://doi.org/10.1080/0020174X.2012.643621. Acesso em: 12 mar. 2024.

A materialização da transparência em processos mais sofisticados vem por vezes através de deveres que estão expressas na LGPD, e constituem modelos mais formais pelos quais os agentes podem ser compelidos a desnudarem como ocorre o tratamento dos dados pessoais. Como visto, o propósito da transparência quando direcionada à autoridade é assegurar um mecanismo de controle do poder que os agentes têm por meio dos dados pessoais e dos algoritmos, bem como avaliar os impactos daquelas operações em âmbito coletivo.

A atuação da autoridade é que permite assegurar um nível de *accountability* que possibilita o controle, de forma minimamente efetiva, da atuação dos agentes de tratamento. Essa atuação envolve uma série de desdobramentos, podendo ser menos agressivas (como advertências, direcionamentos, definições conjuntas de políticas públicas) ou mais ostensivas (como limitação de algumas atividades dos agentes ou aplicação de multas). Independentemente da forma escolhida para exercer o controle do poder, fato é que a conduta da autoridade depende do acesso às informações relativas às operações para que se possa avaliar a forma como o poder pelos dados pessoais e pelos algoritmos é exercido[207].

No entanto, as limitações de acesso à informação acabam, como consequência, restringindo as possibilidades de atuação da ANPD para cumprir esse propósito de controle de poder.

Uma primeira limitação seria justamente a própria jurisdição[208]. A dimensão global do mercado de dados faz com que as operações que ocorrem em território nacional por vezes sejam controladas por agentes que estão em outros países, submetidos a outros regimes jurídicos. Também podem envolver dados armazenados originariamente em diversos locais, ou operações tratando dados de indivíduos de outras nacionalidades. Isso limita fortemente as possibilidades de rastreio e compreensão das autoridades sobre como se desenvolvem os negócios dos agentes, da mesma forma como limitam o acesso direto às informações sobre as operações.

---

[207] MACCARTHY, Mark. New Directions In Privacy: Disclosure, Unfairness and Externalities. *I/S*: A Journal of Law and Policy for the Information Society. 425. 2011. Disponível em: https://ssrn.com/abstract=3093301. Acesso em: 27 nov. 2023.

[208] É importante frisar que os limites da jurisdição trazem hoje debates que transcendem o mercado de dados. A globalização e seus impactos são debatidos no âmbito da sociologia e da antropologia em diversas perspectivas diferentes, falando sobre aspectos do multiculturalismo, do fluxo de pessoas, mercadorias e informações, das novas dimensões econômicas de interação entre povos, de formações de identidade, e tantas outras questões que fizeram surgir novos sensos de comunidade e novas possibilidades de poder e influência. Sobre o tema, ver: BERMAN, Paul Schiff. *Global Legal Pluralism*. A Jurisprudence of law Beyond Borders. Cambridge University Press, 2012. p. 61-96.

Outra questão é que os deveres de fornecimento de dados para a autoridade estão previstas em lei de forma limitada. São poucas as circunstâncias que criam a possibilidade de a ANPD solicitar esclarecimentos mais amplos sobre o tratamento dos dados que é realizado pelos agentes. Essas circunstâncias estão descritas como possíveis para a apuração de risco discriminatório, incidentes de segurança e averiguação das bases legais, mas não cobrem toda a atuação que é necessária para a autoridade perseguir seus objetivos, não só de tutela de direitos, mas também de promoção de um ambiente e de uma cultura de proteção de dados.

Mesmo desconsiderando esse problema, os deveres legais que existem são por vezes limitados e não conseguem efetivamente elucidar como se dão as operações. Os Relatórios de Impacto, por exemplo, são documentos notadamente enviesados, uma vez que foram produzidos pelos próprios agentes para explicarem suas operações. Apesar da preocupação com a metodologia, o rigor do que está inserido no documento depende de uma escolha feita pelo agente, de modo que essa escolha pode mascarar informações importantes sobre como se dão as operações.

As auditorias igualmente são soluções limitadas para viabilizar a transparência para a autoridade, especialmente em razão da forma como elas estão descritas no texto legal: não existe descrição de que tipo de auditoria pode ser realizada pela autoridade, ou qual será a sua extensão. Ou seja, há pouca clareza se o dispositivo fala em auditoria das bases de dados, dos códigos (ou parte deles), dos resultados produzidos, ou de toda a operação[209]. Até o momento, a ANPD apenas indicou que é dever dos administrados se submeter às auditorias por ela determinadas[210], sem dar maiores detalhes sobre a logística e os procedimentos técnicos envolvidos.

Outro problema envolvendo as auditorias é o que de fato elas podem comprovar. Como se vê da previsão legal, sua possibilidade está relacionada à investigação a ser conduzida pela autoridade para apurar potenciais riscos discriminatórios nas operações

[209] Em pesquisas anteriores (2021), esta autora detalhou diferentes tipos de auditorias e os problemas delas decorrentes. A ideia genérica de auditoria colocada pela LGPD remonta à década de 70, a partir de uma premissa falsa de que todo conteúdo pode ser objeto de teste, o que se mostrou não verdadeiro. Dentre os modelos de auditoria, existe o controle de perfis, o controle de resultados, a revisão dos códigos (total ou parcial) e a pesquisa entre usuários que precisam de nível de detalhamento, inclusive técnico, para se mostrarem minimamente viáveis. Ver: LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento automatizado de dados pessoais*. Como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021. p. 169-171.

[210] Cf. Norma de Fiscalização da ANPD. Disponível em: https://www.gov.br/participamaisbrasil/norma-de-fiscalizacao-da-anpd. Acesso em: 06 jan. 2024.

de tratamento de dados. Contudo, não se sabe até que ponto elas são mecanismos efetivos para comprovação desses riscos.

Como mencionado anteriormente, as operações de tratamento de dados combinam diversos algoritmos diferentes com uma série de interações sociais e dimensões que se modificam constantemente a depender da base de dados e do sistema, das redes e dos *feedbacks*. As auditorias nunca vão conseguir reproduzir esses ambientes para fazer uma avaliação concreta e suficiente. Sequer é possível avaliar quais são os dados mais relevantes para a produção daquele resultado, ou quais *inputs* efetivamente podem conter vieses, em razão do fluxo informacional volumoso e da variedade de dados que compõem as operações[211].

O que se percebe, portanto, é que existem importantes óbices a serem superados para que a transparência, em todas as suas dimensões, mostre-se um mecanismo efetivo para materializar o direito fundamental à proteção de dados, à privacidade e até a não discriminação.

[211] DESAI, Deven R.; KROLL, Joshua A. Trust But Verify: A Guide To Algorithms And The Law. *Harvard Journal Of Law & Technology*, v. 31, 2017. p. 10. Disponível em: https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech1.pdf. Acesso em: 13 fev. 2024.

CAPÍTULO II: OS SEGREDOS DE NEGÓCIO NO CONTEXTO DO TRATAMENTO DE DADOS

Além das dificuldades que foram trazidas anteriormente para materializar a transparência, existem também aquelas que são resultado do comportamento dos agentes de tratamento, e que dificultam o acesso dos titulares e das autoridades às explicações sobre como se dão as operações.

O presente trabalho pretende falar especificamente sobre um desses tipos de opacidade: a que é criada por meio dos segredos de negócio.

Antes, contudo, é importante compreender como a referida categoria jurídica se insere no mercado de dados pessoais.

II.1 A TUTELA DOS SEGREDOS DE NEGÓCIO E A PROTEÇÃO DOS INTERESSES DOS AGENTES ECONÔMICOS

Ao se falar no mercado de dados pessoais, é comum pensar em desdobramentos da privacidade que buscam ser protegidos por meio das leis e regulações da área. Nesse sentido, o que se entende por privacidade hoje possui interpretações diferentes em relação a como ela foi originalmente pensada, justamente para acomodar os variados contextos que ensejam o compartilhamento, a coleta e o tratamento de dados pessoais.

Uma dessas reflexões faz da privacidade uma forma de controle do fluxo informacional, a fim de que o titular tenha a possibilidade de limitar e administrar como e por quem seus dados são explorados[212]. Através da autodeterminação informativa, busca-se acomodar o resguardo à esfera privada frente à avalanche informativa característica do atual capitalismo.

Refletindo sobre privacidade nessa perspectiva, ou seja, como uma maneira de gestão do fluxo informacional, alguns autores e autoras tratam outras categorias do direito, não necessariamente relacionadas às pessoas naturais, como também sendo desdobramentos do direito fundamental à privacidade. Os segredos de negócio, a esse

[212] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Revista Pensar*. Fortaleza, v. 25, n. 4. p. 1-18, out./dez. 2020. p. 9-10. Disponível em: https://ojs.unifor.br/rpen/article/view/10828. Acesso em: 23 jun. 2023; WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, n. 2, 2019. Disponível em: https://ssrn.com/abstract=3248829. Acesso em: 6 abr. 2024.

respeito, são uma categoria jurídica que exemplifica esses esforços: são frequentemente tratados como tentativas do legislador de proteger algum tipo de privacidade da pessoa jurídica (ou daquele que desenvolve alguma atividade comercial), resguardando também algumas de suas repercussões mais diretas, como o direito à inviolabilidade da intimidade, ao sigilo da correspondência e à comunicação[213].

A possibilidade de pessoas jurídicas serem dotadas de direitos de personalidade é questão controvertida e suscita críticas diante do risco de tornar análogas as repercussões dos danos causados à subjetividade humana e os danos patrimoniais sofridos por empresas[214]. Valendo-se de reflexões sobre o papel político do Direito, pode-se até identificar que os esforços de se atribuir à pessoa jurídica os desdobramentos da personalidade (dentre os quais se enquadra o direito de privacidade) são uma tentativa de favorecer os agentes econômicos, a fim de eles conseguirem equiparar os seus interesses econômicos aos interesses existenciais das pessoas naturais.

Por esse motivo, importantes doutrinadores defendem que a tutela dos direitos de personalidade decorre de um desdobramento da dignidade da pessoa humana, que distancia a discussão das pessoas jurídicas[215]. Quando muito, seria possível reconhecer a tutela de alguns interesses específicos que se assemelham à proteção da personalidade, mas que só podem ser aplicados de forma suplementar e sem criar qualquer conflito com a efetiva proteção que se busca assegurar exclusivamente ao indivíduo[216].

---

[213] FEKETE, Elisabeth Kasznar. Segredo de Empresa. *In*: COELHO, Fábio Ulhoa; ALMEIDA, Marcus Elidius Michelli de (coord.). *Enciclopédia Jurídica da PUCSP*, tomo IV [recurso eletrônico]: direito comercial. São Paulo: Pontifícia Universidade Católica de São Paulo, 2018. p. 4. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso em: 13 de maio 2024.

[214] Como bem leciona Gustavo Tepedino: "percebe-se o equívoco de se imaginar os direitos da personalidade e o ressarcimento por danos morais como categorias neutras, tomadas de empréstimo pela pessoa jurídica para a sua tutela (tida como maximização de seu desempenho econômico e de sua lucratividade). Ao revés, o intérprete deve estar atento para a diversidade de princípios e de valores que inspiram a pessoa física e a pessoa jurídica." (TEPEDINO, Gustavo. A pessoa jurídica e os direitos da personalidade. *In*: TEPEDINO, Gustavo. *Temas de direito civil*. Rio de Janeiro: Renovar, 1999. p. 499).

[215] O histórico de proteção aos direitos de personalidade, inclusive, representa a expressão da preponderância dos interesses humanos e do protagonismo que o indivíduo deve ter no ordenamento jurídico. O resgate do tema é feito por: Doneda, e cabe citá-lo: "A fundamentação constitucional dos direitos da personalidade e a elevação da pessoa humana ao valor máximo do ordenamento não deixam dúvidas sobre a preponderância do interesse que a ela se refere, interesse este presente na pessoa jurídica apenas de forma indireta. Uma extensão apriorística dos direitos da personalidade às pessoas jurídicas, o que infelizmente pode ser o resultado do artigo 52, passaria ao largo de qualquer consideração a este respeito, podendo chegar a comprometer a tábua axiológica constitucional" (DONEDA, Danilo. Os Direitos da Personalidade no Código Civil. *Revista da Faculdade de Direito de Campos*, Ano VI, No 6 - Junho de 2005. p. 94. Disponível em: https://egov.ufsc.br/portal/sites/default/files/os_direitos_de_personalidade_no_codigo_civil.pdf. Acesso em: 11 abr. 2022).

[216] DONEDA, *op. cit*., p. 95.

A reflexão é importante para situar em qual categoria se inserem os segredos de negócio no ordenamento. Se forem tratados como desdobramentos da privacidade, poderia ser possível atribuir aos agentes econômicos a possibilidade de invocarem, em seu favor, uma tutela jurídica que deveria ser destinada à proteção exclusiva de pessoas naturais.

Por outro lado, é possível defender que normas cuja disposição central se relaciona à proteção da privacidade buscam igualmente proteger os segredos de negócio. É o caso da própria LGPD, que instituiu como competência da ANPD a tutela dos segredos de negócio (arts. 55-J, II, X e parágrafo 5º)[217]. Ou seja, logo depois da proteção aos dados pessoais, a ANPD assume a responsabilidade de também zelar pela observância dos segredos comercial e industrial.

Apesar de estar inserida na LGPD, talvez até de forma indevida, a tutela dos segredos de negócio não pode ser vista como um desdobramento da proteção à privacidade. Isso porque, para além da problemática envolvida em atribuir às pessoas jurídicas uma tutela que se desdobra da personalidade, é também importante diferenciar o que é a proteção da privacidade do indivíduo no contexto dos dados pessoais. Pensando especificamente no mercado em questão, há grande preocupação em assegurar a preservação dos interesses do titular e não os submeter ao exercício arbitrário do poder que é administrado pelos agentes de tratamento em razão dos dados e das tecnologias.

Se conferido aos agentes a possibilidade adicional de tratarem os segredos de negócio como um desdobramento da privacidade, a situação de assimetria no mercado de dados pessoais pode ser ainda maior e preocupações que vão ser endereçadas posteriormente, sobre a opacidade criada por meio dos segredos, poderão ser insuperáveis.

Não sendo desdobramentos da personalidade, resta então compreender como se definem os segredos de negócio.

---

[217] Na redação original da LGPD, antes do veto presidencial, os segredos de negócio eram mencionados apenas no parágrafo 4º do art. 55-J, estabelecendo que a autoridade deveria preservar os segredos e o sigilo das informações, sob pena de responsabilidade. Essa redação sugeria que, tendo tido acesso a informações que são consideradas como segredos de negócio (novamente reforçando o enquadramento estanque), a autoridade deveria empenhar esforços para evitar que essas informações fossem disponibilizadas a concorrentes ou caíssem em domínio público, o que iria prejudicar sua natureza secreta e sua condição sigilosa. Assim, o risco de responsabilização seria decorrente do não cumprimento de um dever de preservação do sigilo por parte da autoridade. Com a redação trazida pela Lei n. 13.853/2019, a LGPD passou a incorporar novas menções aos segredos de negócio e colocou como competência da ANPD também a proteção desse tipo de conteúdo. Ou seja, surgiu uma competência adicional para a autoridade que não é a de proteção de dados pessoais; é a de proteção dos segredos de negócio quando eles estiverem inseridos dentro do mercado de dados pessoais.

II.1.1 Extensão e efeitos da proteção aos segredos de negócio no Brasil

Os agentes econômicos desenvolvem conteúdos essenciais aos seus negócios, nutridos da expectativa de que estes não vão ser indevidamente utilizados por terceiros em proveito próprio[218]. No mercado de dados, esses conteúdos podem ser muito variados e envolvem dados, fórmulas, tecnologias e outros, cujo domínio os consolida no exercício de posições dominantes no mercado.

Na busca da proteção desses interesses privados, é possível perceber que o Direito fornece uma série de mecanismos jurídicos que objetivam regular o comportamento dentro dos mercados, em prol da proteção a essas inovações[219]. O segredo de negócio é um desses mecanismos. No capitalismo, eles é colocado como ferramenta de gestão da competitividade e da inovação por meio da proteção a uma miríade de conhecimentos valiosos para pequenas, médias e grandes empresas, dos mais variados setores econômicos[220].

Entende-se no presente trabalho os segredos de negócio como gênero do qual são espécies o segredos industrial e comercial[221]. Os segredos industriais seriam conhecimentos específicos relacionados aos processos industriais e produtivos, e que se desejam manter ocultos em razão da sua relevância para a empresa e de seu valor competitivo. Os segredos comerciais, por sua vez, são informações relativas às operações da empresa, aos negócios e suas estruturas, que, se divulgadas, igualmente podem causar

---

[218] BARBOSA, Denis Borges. *Uma introdução à propriedade intelectual*. 2. ed. Lumen Juris, 2010. p. 641. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 21 mar. 2024.

[219] Pode-se dizer que no Direito Civil existem inúmeros outros, como a própria boa-fé objetiva: uma cláusula geral que cria deveres e obrigações transcendentes às relações contratuais, a fim de orientar o comportamento social. Pensando na proteção da inovação e no desenvolvimento das atividades econômicas, é possível afirmar que a boa-fé também serve como um *standard* de comportamento esperado dos agentes econômicos para que eles mantenham suas operações dentro de níveis de probidade esperados; para que eles desenvolvam seus negócios dentro de vetores de confiança, credibilidade e previsibilidade (MARTINS-COSTA, Judith. *A boa-fé objetiva no direito privado* – sistema e tópica no processo obrigacional. São Paulo: RT, 2000. p. 270-290).

[220] CUEVA, Ricardo Villas Bôas. A importância de proteger o segredo de negócio. *In* CALCINI, Ricardo; ANDRADE, Dino (org.). *Reflexões Jurídicas Contemporâneas*. Leme-SP: Mizuno, 2022. p. 264.

[221] FEKETE, Elisabeth Kasznar. *O regime jurídico do segredo de indústria e comércio no direito brasileiro*. Rio de Janeiro: Forense, 2003. p. 45.

prejuízos à atividade produtiva e ao mercado[222]. Em conjunto, as características dos segredos de negócio foram sistematizadas por Elizabeth Fekete[223].

No Brasil, as principais disposições sobre segredos de negócio estão contidas na Lei de Propriedade Intelectual (LPI - Lei Federal n. 9.279/1996) e no Acordo Sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (TRIPS).

Na LPI, o art. 195, XI, caracteriza os segredos como "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", vedando o seu compartilhamento sob risco de se caracterizar crime de concorrência desleal. O art. 206 da mesma lei dispõe ainda que o eventual compartilhamento dessas "informações que se caracterizem como confidenciais" só pode ocorrer em processos tramitando em segredo de justiça, sendo vedado seu uso para outras finalidades.

O TRIPS[224], por sua vez, cria como parâmetro de violação aos segredos de negócio e de deslealdade concorrencial meros atos de divulgação, exploração ou utilização indevida e desautorizada da informação sensível ao agente[225]. Referido acordo consolidou iniciativas de anos em busca do consenso e da cooperação entre vários Estados[226] para criação de premissas mínimas em prol da proteção de direitos de

---

[222] Como exemplo dos segredos industriais e comerciais, discorre Fekete: "O 'segredo de empresa', sinônimo, portanto, de 'segredo de negócio' ou "informação confidencial", representa o gênero agrupante de duas espécies: os segredos industriais, que abrangem, entre muitos outros exemplos possíveis, os processos de fabricação, as fórmulas de produtos, os dados técnicos de P&D e os segredos comerciais, como os projetos de lançamento de novos produtos ou serviços, os estudos de marketing, os resultados de pesquisas de mercado, as listas de clientes ou fornecedores, os métodos internos de trabalho e os estudos financeiros, tais como previsões de lucros, precificação, etc. Para definir o objeto deste verbete, percorro o caminho prévio indispensável de examinar e demarcar os requisitos que devem estar cumulativamente presentes" (FEKETE, Elisabeth Kasznar. Segredo de Empresa. *In*: COELHO, Fábio Ulhoa; ALMEIDA, Marcus Elidius Michelli de (coord.). *Enciclopédia Jurídica da PUCSP*. tomo IV (recurso eletrônico): direito comercial. São Paulo: Pontifícia Universidade Católica de São Paulo, 2018. p. 5. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso em: 13 maio 2024). O presente estudo escolhe adotar a definição trazida por Fekete, pois, como detalhou a autora em obras anteriores, a questão não comporta definições unânimes. Ver: FEKETE, Elisabeth Kasznar. *O regime jurídico do segredo de indústria e comércio no direito brasileiro.* Rio de Janeiro: Forense, 2003. p. 44-45.

[223] "[...] conhecimento utilizável na atividade empresarial, de caráter industrial ou comercial, de acesso restrito, provido de certa originalidade, lícito, transmissível, não protegido por patente, cuja reserva representa valor econômico para o seu possuidor, o qual exterioriza o seu interesse na preservação do sigilo através de providências razoáveis" (FEKETE, *op. cit*., p. 420).

[224] Em países latinos, a sigla adotada também pode ser ADPIC (Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual relacionados com o Comércio).

[225] FEKETE, Elizabeth Kasznar. Segredo de Justiça. *In*: ABBOUD, Georges; BARBOSA, Pedro Marcos Nunes (coord.). *Direito processual da propriedade* intelectual [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2023, RB-14.3.

[226] Diz-se que foi uma iniciativa consolidada ao longo do tempo porque veio depois de outros tratados e acordos internacionais entre vários países que já tentavam criar premissas básicas para a proteção da propriedade intelectual e dos segredos de negócio em um nível global. Nesse aspecto, menciona-se a

propriedade intelectual como um todo[227]. Ele foi incorporado no Brasil por meio do Decreto n. 1.355/1994, mas entrou efetivamente em vigor após um regime transitório nele previsto[228].

Existem, ainda, outras leis que regulam o fluxo de informações consideradas segredos de negócio, especialmente em âmbito setorial. A título de exemplo, a Lei Federal n. 10.603/2002 regula a proteção das informações (dados não divulgados) que devem ser apresentadas às autoridades competentes como condição para aprovação ou manutenção de registro para comercialização de produtos farmacêuticos, de uso veterinário, fertilizantes ou agrotóxicos. A Lei de Acesso à Informação (Lei Federal n. 12.527/2011) exclui de suas disposições a necessidade de divulgação de "segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público".

Em conjunto, as disposições sobre segredos de negócio no ordenamento jurídico brasileiro mostram que a condição subjetiva principal para a proteção desse tipo de informação se extrai da vedação aos atos de concorrência desleal[229].

Convenção da União de Paris, de 1883, que foi um dos primeiros diplomas a tratar da obrigatoriedade de se adotarem normas de repressão à concorrência desleal. Outra iniciativa foi por meio da Convenção de Estocolmo, que instituiu a Organização Mundial da Propriedade Intelectual (OMPI), pós Segunda-Guerra Mundial, com objetivo de fortalecer a proteção da propriedade intelectual. Apesar de ter sido revogada pelo TRIPS, referida convenção teve a importância de unificar conceitos e facilitar o acesso a técnicas e obras literárias, bem como à informação científica técnica contida nas patentes. (BASSO, Maristela. Os fundamentos atuais do direito internacional da propriedade intelectual. *Revista CEJ*. Brasília, v. 7, n. 21, jun. 2003. p. 17. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/541. Acesso em: 22 maio 2024).

[227] BASSO, Maristela. A proteção da propriedade intelectual e o direito internacional atual. *Revista de Informação Legislativa*, Brasília, v. 41, n. 162. p. 287-309, abr./jun. 2004. p. 293-295. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/965. Acesso em: 22 maio 2024.

[228] O TRIPS foi aprovado pelo Congresso por meio do Decreto Legislativo n. 30, de 15 de dezembro de 1994 e promulgado pelo Decreto n. 1.355, de 30 de dezembro de 1994 (BASSO, *op. cit*., p. 305). Ele é considerado um tratado-contrato por criar uma situação jurídica subjetiva que cria "obrigação internacional de conduta na ordem internacional e não na ordem interna dos estados-partes". Por meio do TRIPS, os estados-membros assumem compromissos de implementação das normas ali descritas, podendo determinar a melhor forma de fazê-lo, desde que sejam observados os padrões ali descritos (BASSO, Maristela. Os fundamentos atuais do direito internacional da propriedade intelectual. *Revista CEJ*. Brasília, v. 7, n. 21, jun. 2003. p. 21. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/541. Acesso em: 22 maio 2024).

[229] Diz Pontes de Miranda: "Se há meio ou processo de fabricação, ou de indústria, que alguém conhece em segredo, há segredo de fábrica ou de indústria. Dois direitos de personalidade estão em causa, - o direito autoral de personalidade, pois que alguém descobriu ou inventou, e o direito de velar a intimidade. O direito de exploração existe, mas o segredo funciona como impeditivo do exercício de direito formativo gerador (direito à patente), que implica a revelação do segredo" (PONTES DE MIRANDA, Francisco Cavalcanti. *Tratado de Direito Privado*. Parte Especial. 4. ed. São Paulo: Revista dos Tribunais, 1983, v. 16. p. 654). Sobre a tutela dos segredos de negócio pela concorrência desleal, ver também: SILVEIRA, João Marcos. A proteção jurídica dos segredos industriais e de negócio. *Revista da ABPI*. Vol. 53, jul/ago 2001. p. 18-21. Disponível em: https://abpi.org.br/bfd_download/edicao-53-mes-julho-agosto-ano-2001/. Acesso em: 22 maio 2024; BARBOSA, Denis Borges. *Uma introdução à propriedade intelectual*. 2. ed. Lumen Juris, 2010. p. 641. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em:

A menção à "concorrência desleal" deve ser lida de forma ampla, a fim de conferir à norma a possibilidade de vedação de variados comportamentos de deslealdade no mercado, os quais podem ser praticados por diversos atores – concorrentes entre si, sócios, empregados ou colaboradores[230]. Devem englobar usos abusivos de prerrogativas e relações contratuais estabelecidas entre as partes, com objetivo de prejudicar o fluxo de clientes, o desenvolvimento dos negócios[231]. Ainda, pode ser caracterizada quando da mudanças em políticas públicas, limitações técnicas e de conhecimento, e até da inabilidade legislativa, justamente quando são auferíveis impactos concorrenciais no mercado[232]. Em alguma medida, envolvem, portanto, atos que podem gerar infrações à Ordem Econômica, em uma dimensão mais abrangente que relaciona também os impactos concorrenciais para a coletividade.

Trata-se de uma tutela jurídica diferente das patentes e da propriedade industrial porque não envolve necessariamente um distúrbio da propriedade intelectual, mas sim o exercício de uma atividade econômica e os prejuízos que ela pode ter ocasionado no mercado[233]. A proteção aos segredos de negócio, pode-se dizer então, orienta um comportamento individual de não se apropriar indevidamente, em busca de um proveito próprio, das informações de terceiros.

Quanto à sua natureza jurídica, existem doutrinadores importantes que defendem seu enquadramento jurídico como propriedade[234]. Contudo, é de se reconhecer que os

---

21 mar. 2024; VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual*. 2. ed. São Paulo: Almedina, 2020. p. 369.

[230] Pedro Marcos Nunes Barbosa menciona seis clássicas situações nas quais se observa concorrência desleal: "Neste sentido, é possível observar cinco principais eixos sobre os quais a clássica incidência da concorrência desleal se dá no Direito brasileiro: (a) na tutela reputacional do concorrente; (b) na delimitação da liberdade de expressão na auto adulação; (c) no aliciamento de sujeitos de direito que estejam vinculados à vítima, visando subtrair bens imateriais, acessar conteúdo privado, ou desorganizar o concorrente; (d) na publicização de interdições mercantis que não existem; (e) na adulteração da exposição de signos que possam obscurecer a genuína origem de bens e serviços; e (f) no emprego de quaisquer outros artifícios fraudulentos para o desvio de clientela" (BARBOSA, Pedro Marcos Nunes. *Curso de Concorrência desleal*. Rio de Janeiro: Lumen Juris, 2022. p. 182).

[231] BARBOSA, *op. cit*., p. 199-200.

[232] *Ibid*., 186.

[233] AMORIM, Ana Clara Azevedo de. O regime jurídico dos segredos comerciais no novo Código de Propriedade Industrial. *Revista Electrónica de Direito*, n. 2, v. 19, jun., 2019. p. 15. Disponível em: https://cij.up.pt/client/files/0000000001/2-ana-clara-amorim_927.pdf. Acesso em: 22 maio 2024; LEE, N. Open yet secret - trading of tangible goods and trade secrets. *In*: BRUUN, Niklas; DINWOODIE, Graeme B.; LEVIN, Marianne; OHLY, Ansgar (eds.). *Transition and Coherence In Intellectual Property Law*: Essays in Honour of Annette Kur. Cambridge: Cambridge University Press, 2021. p. 242-253.

[234] Nelson Nery Junior defendeu, em parecer elaborado para um caso específico, que "o segredo do negócio do qual é titular a empresa, [é] bem esse imaterial e que integra o estabelecimento empresarial (CC 1142). Embora existam bens do patrimônio imaterial da empresa que tenham específica proteção jurídica, como é o caso das marcas, patentes, modelos, invenções, software, direitos autorais e nome comercial, o segredo do negócio é direito que tem a proteção geral da propriedade. Merece tutela do ordenamento jurídico porque integra o patrimônio da empresa" (NERY JUNIOR, Nelson. Segredo de Negócio - Livre Iniciativa.

segredos de negócio se aproximam de uma tutela jurídica da exclusividade de fato, e não de uma propriedade oponível *erga omnes*[235]. Também não estão expressamente incluídos na LPI como propriedades intelectuais[236], inexistindo dispositivo legal expresso que os categorize dentro dos regime jurídico de direitos reais[237].

É possível defender também que segredos de negócio podem ser tidos como um direito de posse, de quase propriedade, de direito de personalidade ou tantas outras[238]. No entanto, até mesmo para os propósitos do presente estudo, que consideram a necessidade

---

Soluções Práticas. vol. 1. p. 361-370, set/2010. *Revista dos Tribunais*). Também é possível falar que os segredos de negócio são a tutela jurídica do aviamento, sendo o aviamento um direito real, de modo que também por essa justificativa se teria o enquadramento dos segredos como tutelas ligadas à propriedade. Sobre a questão específica do aviamento, ver: FERREIRA, Waldemar. *Tratado de Direito Comercial*. O estatuto do estabelecimento e a empresa mercantil. vol. 7. Editora Saraiva: São Paulo, 1962. p. 207-225.

[235] SILVEIRA, João Marcos. A proteção jurídica dos segredos industriais e de negócio. *Revista da ABPI*. Vol. 53, jul/ago 2001. p. 20. Disponível em: https://abpi.org.br/bfd_download/edicao-53-mes-julho-agosto-ano-2001/. Acesso em: 22 maio 2024.

[236] FEKETE, Elisabeth Kasznar. Segredo de Empresa. *In*: COELHO, Fábio Ulhoa; ALMEIDA, Marcus Elidius Michelli de (coord.). *Enciclopédia Jurídica da PUCSP*, tomo IV (recurso eletrônico): direito comercial. São Paulo: Pontifícia Universidade Católica de São Paulo, 2018. p. 9. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso em: 13 maio 2024.

[237] Nos Estados Unidos, fala-se da expansão da natureza de propriedade para os direitos de propriedade intelectual em geral, subsistindo ainda significativa controvérsia sobre qual a natureza dos segredos de negócio (BENTLY, Lionel. Trade secrets. 'intellectual property' but not 'property'? *In*: HOWE, Helena R.; GRIFFITHS, Jonathan (eds.). *Concepts of Property in Intellectual Property Law*. Nova York: Cambridge University Press, 2013). Há autores que tentam desenvolver um entendimento conciliatório de que as distintas visões sobre a natureza jurídica dos segredos de negócio podem ser complementares entre si. Enquanto um enquadramento jurídico estimula os agentes a desenvolverem informações valiosas e protegê-las do domínio público e da aquisição imprópria por terceiros, o outro desestimula os indivíduos a acessarem essas informações e a se engajarem em atividades que podem resultar em concorrência desleal (SCHECHTER, Roger E.; THOMAS, John R. *Intellectual Property*: The Law of Copyrights, Patents and Trademarks. United States of America: Hornbook Series, 2003. p. 529). Sobre essa proposta conciliatória, ainda que ela não seja objeto expresso do presente estudo (e nem mesmo se adequem com perfeição à realidade brasileira), vale mencionar Richard Posner, que defende que as duas visões sobre o que são segredos de negócio, em verdade, trazem ênfases distintas a um mesmo instituto jurídico: "It should be apparent that the two different conceptions of trade secret protection are better described as different emphases. The first emphasizes the desirability of deterring efforts that have as their sole purpose and effect the redistribution of wealth from one firm to another. The second emphasizes the desirability of encouraging inventive activity by protecting its fruits from efforts at appropriation that are, indeed, sterile wealth-redistributive -- not productive -- activities. The approaches differ, if at all, only in that the second does not limit the class of improper means to those that fit a preexisting pigeonhole in the law of tort or contract or fiduciary duty -- and it is by no means clear that the first approach assumes a closed class of wrongful acts, either" [É possível ver que as duas diferentes concepções sobre a proteção aos segredos de negócio são melhor descritas como diferentes ênfases. A primeira enfatiza a vontade de impedir esforços cujo único propósito e efeito é o de redistribuição de riqueza de uma firma para a outra. A segunda enfatiza a vontade de encorajar a atividade inovadora por meio da proteção dos seus frutos e esforços da apropriação já que que são, de fato, atividades estéreis de redistribuição de riqueza - não produtivas. As abordagens diferem, se é que diferem, apenas pelo fato de que a segunda não limita a classe de meios impróprios àquelas que se encaixam em um nicho preexistente na lei de delitos civis ou contrato ou dever fiduciário - e tampouco está de alguma forma claro que a primeira abordagem assume uma classe fechada de atos ilícitos] (POSNER, Richard. Intellectual Property. Case Compliments of Versuslaw. *Rockwell Graphic Systems*, Inc. v. Dev Industries, Inc., 925 F.2d 174 (7th Cir. 1991), tradução livre. Disponível em: https://biotech.law.lsu.edu/cases/ip/ts/Rockwell_v_Dev_I.htm. Acesso em: 20 mar. 2024).

[238] As diferentes correntes sobre a natureza jurídica dos segredos foram bem detalhadas por FEKETE, Elisabeth Kasznar. *O regime jurídico do segredo de indústria e comércio no direito brasileiro.* Rio de Janeiro: Forense, 2003. p. 143-171.

de compreender e limitar a forma como os segredos são utilizados pelos agentes do mercado de dados pessoais, entende-se que os segredos de negócio são bens imateriais protegidos essencialmente pela vedação à concorrência desleal[239], considerando como concorrência desleal toda a variedade de condutas já mencionada anteriormente. Nessa opção, não há incompatibilidade de se considerar que a tutela jurídica dos segredos, para evitar atos de concorrência desleal, também decorre de fundamentos constitucionais à privacidade dos agentes econômicos e proteção da inovação. Por outro lado, ela permite construir algumas bases para limitar os casos em que os segredos de negócio são invocados e utilizados pelos agentes econômicos.

II.1.2 O alcance do sigilo conferido aos segredos de negócio

A condição sigilosa das informações que são enquadradas como segredos de negócio é um aspecto importante para a categoria jurídica[240].

Comumente, o sigilo é colocado como uma das principais fontes de valor desse tipo de conteúdo[241]. Nesse sentido, a tutela jurídica dos segredos de negócio só subsiste na medida em que a condição de sigilo permanecer[242], não podendo o conteúdo ser de conhecimento geral ou estar acessível publicamente[243]. Até por isso, o enquadramento de

---

[239] É a opção adotada por SILVEIRA, João Marcos. A proteção jurídica dos segredos industriais e de negócio. *Revista da ABPI*. Vol. 53, jul/ago 2001. p. 81. Disponível em: https://abpi.org.br/bfd_download/edicao-53-mes-julho-agosto-ano-2001/. Acesso em: 22 maio 2024.

[240] Além de ser característica definidora, é defensável que o nível de segredo da informação pode ser um elemento que diferencia os segredos de negócio de outros institutos, com o *know-how*. O *know*-how se define como "o conjunto de conhecimentos disponíveis a respeito do modelo de produção específico de uma empresa, que lhe permite ter acesso a um mercado, manter- se nela, ou nele desfrutar vantagens em relação a seus competidores" (BARBOSA, Denis Borges. *Uma introdução à propriedade intelectual*. 2. ed. Lumen Juris, 2010. p. 627. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 21 mar. 2024). Alguns autores não distinguem a categoria dos segredos de negócio e do *know-how*, na medida em que entendem que o *know-how* também é um conhecimento que se caracteriza pela "falta de acesso por parte do público em geral ao conhecimento do modelo de produção de uma empresa" (BARBOSA, *op. cit*., p. 627). Em sentido similar, ver: KORS, Jorge Alberto. *Los secretos industriales y el know how*. Buenos Ayres: La Ley, 2007). No entanto, cabe destacar as recentes considerações de Alberto Esteves Ferreira Filho, no sentido de que em momento algum o *know-how* se define pela sua condição de sigilo, ao passo que os segredos de negócio pressupõem esse elemento para assim serem caracterizados (FERREIRA FILHO, Alberto Esteves. *Licenciamento de Know-How*: considerações sobre sua legalidade e os atos do INPI. São Paulo: Editora Dialética, 2022. p. 34).

[241] MILLER, Megan Marie. Data as the New Oil: A Slippery Slope of Trade Secret Implications Greased by the California Consumer Privacy Act. *Cybaris*®: Vol. 12: Iss. 1, Article 1, 2021. p. 16. Disponível em: https://open.mitchellhamline.edu/cybaris/vol12/iss1/1/. Acesso em: 08 fev. 2024.

[242] MORATO, Antonio Carlos; CHINELLATO, Silmara Juny Abreu. Direitos Básicos de Proteção de Dados Pessoais, o Princípio da Transparência e a Proteção dos Direitos Intelectuais. *In*: DONEDA, Danilo *et al*. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 658.

[243] GERALDES, João de Oliveira. Sobre a proteção jurídica dos segredos comerciais no espaço digital. *Revista da Faculdade da Universidade de Lisboa*, vol. LXIII, 1 e 2, Lisboa, 2022. p. 425. Disponível em:

informações como segredos de negócio pode envolver, dentre outras questões, a avaliação de quais são os esforços e as diligências empenhados pelo agente para que aquela informação se mantenha longe do domínio público e em condição restrita de acesso[244].

Preservar essa condição de sigilo, portanto, pode se mostrar uma tarefa sofisticada para os agentes[245]: sua relevância para a tutela jurídica é fundamental, mas os riscos de divulgação e popularização indevida de informações são hoje muito mais amplos em razão da globalização e da velocidade com que informações são divulgadas na internet[246].

Por outro lado, existem significativos benefícios em manter determinados conteúdos sob o resguardo dos segredos de negócio. Discussão relevante, contudo, deve

---

https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Joa%CC%83o-de-Oliveira-Geraldes_compressed.pdf. Acesso em: 06 out. 2023.

[244] SCHECHTER, Roger E.; THOMAS, John R. *Intellectual Property*: The Law of Copyrights, Patents and Trademarks. United States of America: Hornbook Series, 2003. p. 531-532; FEKETE, Elisabeth Kasznar. Segredo de Empresa. *In*: COELHO, Fábio Ulhoa; ALMEIDA, Marcus Elidius Michelli de (coord.). *Enciclopédia Jurídica da PUCSP.* tomo IV (recurso eletrônico): direito comercial. São Paulo: Pontifícia Universidade Católica de São Paulo, 2018. p. 6. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso em: 13 maio 2024; GERALDES, *op. cit*., p. 425; KORS, Jorge Alberto. *Los secretos industriales y el know how*. Buenos Aires: La Ley, 2007. p. 108. Também sobre o tema, Bone detalha como esse requisito pode ser considerado ultrapassado e até incompatível com o nível do desenvolvimento tecnológico crescente e com o fluxo informacional decorrente dos mercados atuais: BONE, Robert G. Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions. *In*: DREYFUSS, Rochelle C.; STRANDBERG, Katherine J. (eds.). The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research. Edward Elgar Press, 2010. *Boston Univ. School of Law Working Paper* No. 09-40. Disponível em: https://ssrn.com/abstract=1467723. Acesso em:10 mar. 2024.

[245] Os riscos envolvem a precariedade da proteção jurídica, a não vedação do desenvolvimento do mesmo conhecimento por pesquisas ou engenharia reversa e os riscos de divulgação, que podem acabar esvaziando o valor agregado ao conteúdo. Uma interessante metáfora sobre esses riscos foi trazida por Sir John Donaldson M. R em julgamento no Reino Unido (caso Attorney General v Newspaper Publishing Plc and Others em 1989): "Confidential information is like an ice cube. Give it to the party who undertakes to keep it in his refrigerator and you still have an ice cube by the time the matter comes to trial. Either party may then succeed in obtaining possession of the cube. Give it to the party who has no refrigerator or will not agree to keep it in one, and by the time of the trial you just have a pool of water which neither party wants. It is the inherently perishable nature of confidential information which gives rise to unique problems" [A informação confidencial é como um cubo de gelo. Dê-o à parte que se compromete a mantê-lo em sua geladeira e você ainda terá um cubo de gelo quando o assunto chegar a julgamento. Qualquer uma das partes pode então ter a posse do cubo. Dê-o à parte que não tem geladeira ou não concorda em mantê-lo em uma, e quando chegar o julgamento, você terá apenas uma poça de água que nenhuma das partes deseja. É a natureza inerentemente perecível da informação confidencial que dá origem a problemas únicos" (OCAÑA, Teresa Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020. p. 66, tradução livre).

[246] A questão foi mapeada por OHLY, Ansgar. Jurisdiction and Choice of Law in Trade Secrets Cases: The EU Perspective. *In*: SANDEEN, Sharon K.; RADEMACHER, Christoph; OHLY, Ansgar (eds.). Research Handbook on Information Law and Governance. Edward Elgar, 2021. Disponível em: https://ssrn.com/abstract=4020416. Acesso em: 12 out. 2023. O autor fala sobre riscos de violações de segredos de negócio em múltiplas jurisdições e da dificuldade que inclusive existe para os Tribunais apurarem crimes de concorrência desleal e assegurarem indenizações, quando devidas. Em razão da globalização e da velocidade com que a informação se propaga na internet, cabe aos agentes econômicos, dentre outras medidas, fortalecer seus sistemas de segurança da informação e sofisticar seus mecanismos de interação e compartilhamento de conteúdo com parceiros para evitar o vazamento de seus segredos de negócio.

ser a do alcance dessa condição sigilosa, a fim de se avaliar em qual medida o acesso restrito aos segredos de negócio deve ser preservado. Reconhecer que um conteúdo é protegido por meio do segredo não implica reconhecer que nenhum terceiro terá acesso a ela, ou que ela não será compartilhada com ninguém, ou, ainda, que não poderá ser divulgada em nenhuma circunstância[247]. Até porque algum tipo de acesso controlado é necessário para que as atividades econômicas que exploram esses segredos possam se desenvolver.

Diferentemente do que ocorre com patentes, nada impede que os mesmos segredos sejam desenvolvidos por outros agentes ou por terceiros através de pesquisas próprias[248]. A obrigação legal em relação à informação por vezes se relaciona à indisponibilidade dela ao público, e não à exclusividade sobre a sua exploração – tanto que a engenharia reversa não é expressamente vedada no âmbito dos segredos de negócio[249]. Ou seja, "o parâmetro internacional aplicável não prevê proteção coativa do sigilo, facultando o uso dos dados por terceiros desde que resguardados os princípios da leal concorrência"[250]. Isso faz com que seja possível a dois agentes econômicos concorrentes entre si explorarem os mesmos segredos de negócio de forma legal.

Também se pressupõe que os segredos de negócio são de alguma forma acessíveis a funcionários e fornecedores com quem o agente interage[251], a fim de que se possam

---

[247] Falar em segredos de negócio remonta a ideais literários do que são segredos. Bem retrata Clarice Lispector: "de maneira alguma, pense que aqui escrevo o meu mais íntimo segredo. Na verdade, há segredos que não conto nem a mim mesma" (LISPECTOR, Clarice. Um sopro de vida (pulsações). Rio de Janeiro: Nova Fronteira, 1978). A categoria jurídica, contudo, não é cercada por esse tipo de mistério.

[248] SCHECHTER, Roger E.; THOMAS, John R. *Intellectual Property*: The Law of Copyrights, Patents and Trademarks. United States of America: Hornbook Series, 2003. p. 529.

[249] Sobre a questão, cabe também destacar as palavras de Tullio Ascarelli: "La protezione del segreto permetterà a chi abbia realizzato una creazione intellettuale di essere il solo a goderla o utilizzarla, di comunicarla a titolo oneroso ad altri, di agire per risarcimento o dei danni contro chi abusivamente l'abbia carpita o divulgata o utilizzata in seguito a umma comunicazione fiduciaria, ma non gli permetterà di impedire poi la utilizzazione de parte di quanti, in seguite alla sia pur illecita divulgazione, ne siano venuti a conoscenza, né gli assicurerà nessuna priorità nei confronti di chi autonomamente pervenga alla stessa creazione" [A proteção do segredo permitirá que aquele que tenha criado uma obra intelectual seja o único a desfrutá-la ou usá-la, a comunicá-la com fins lucrativos a outros, a buscar compensação por danos contra quem a tenha indevidamente obtido ou divulgado ou usado após uma comunicação confidencial, mas não lhe permitirá impedir o uso posterior por parte daqueles que, mesmo após a divulgação ilícita, venham a ter conhecimento dela, nem garantirá qualquer prioridade em relação àqueles que cheguem independentemente à mesma criação] (ASCARELLI, Tullio. *Teoria della Concorrenza e dei Beni Immateriali.* Istituzioni di diritto industriale. 3. ed., Milão: Griuffrè.1960. p. 287, tradução livre).

[250] BARBOSA, Denis Borges. Exclusividade de dados sigilosos: agroquímicos. *In*: BARBOSA, Denis Borges. *Da Tecnologia à Cultura*: ensaios e estudos de Propriedade Intelectual. Rio de Janeiro: Lumen Juris, 2011. p. 532. Disponível em: https://www.dbba.com.br/wp-content/uploads/tecnologia_a_cultura.pdf Acesso em: 23 mar. 2024.

[251] Inclui-se nesse grupo também outros tipos de parceiros comerciais que firmam contratos típicos e atípicos com os agentes. É o caso dos franqueados, por exemplo, que precisam das informações consideradas segredos para poderem exercer sua atividade. Nesse caso, o compartilhamento dos segredos de negócio constitui também uma forma de o franqueador exercer controle sobre a qualidade e o padrão

desempenhar as atividades necessárias ao desenvolvimento da empresa[252]. O requisito para se manter a proteção jurídica é que esse acesso seja feito de forma controlada, na medida do necessário e dentro dos interesses empresariais, evitando-se que as informações caiam em domínio público ou sejam utilizadas em práticas comerciais desleais[253]. Daí porque frequentemente são firmados acordos de confidencialidade, que servem não só como garantia da proteção da informação, como também enquanto instrumento que dá ciência a terceiros sobre a condição secreta das informações, deixando claro que elas não devem ser amplamente divulgadas[254].

Externamente à empresa, também é de se considerar que, em determinadas circunstâncias, os segredos de negócio poderão ser compartilhados com quem não compõe a estrutura empresarial. Eles podem ser licenciados e vendidos para terceiros[255], além de poderem ser fornecidos de forma compulsória a autoridades e entes reguladores. Nesse sentido, a própria LPI prevê, em seu art. 206, a possibilidade de os segredos de

---

que quer impor ao franqueado. Considerações sobre o assunto foram tratadas por: LEITE, Márcio Junqueira; ALMEIDA, Marcus Elidius M.; SISTER, Tatiana D. Da Proteção do Know-how nos Contratos de Franquia. *PEER Review*. Vol. 5, n. 15, 2023. Disponível em: https://www.peerw.org/index.php/journals/article/download/733/454. Acesso em: 18 nov. 2023; LA ROSA, Fernanda Carvalho Frustockl; DA SILVA, Silvio Bitencourt. Delimitação e Proteção Jurídica do Know-How nos Contratos de Franquia a Partir da Visão Baseada em Conhecimento. *Revista de Direito, Inovação, Propriedade Intelectual e Concorrência*. v. 6, n. 2. Jul/Dez. 2020. Disponível em: https://www.indexlaw.org/index.php/revistadipic/article/download/7125/pdf. Acesso em: 18 nov. 2023.

[252] FEKETE, Elisabeth Kasznar. Segredo de Empresa. *In*: COELHO, Fábio Ulhoa; ALMEIDA, Marcus Elidius Michelli de (coord.). *Enciclopédia Jurídica da PUCSP*, tomo IV (recurso eletrônico): direito comercial. São Paulo: Pontifícia Universidade Católica de São Paulo, 2018. p. 5. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso em: 13 maio 2024.

[253] BARBOSA, Denis Borges. *Uma introdução à propriedade intelectual*. 2. ed. Lumen Juris, 2010. p. 644. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 21 mar. 2024. Também: VOGT, Sander. Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence—Part II. *The Journal of Robotics, Artificial Intelligence & Law* (Fastcase), Volume 5, No. 5, September–October 2022, Full Court Press, an imprint of Fastcase, Inc. p. 312-312. Disponível em: https://www.crowell.com/en/insights/publications/show-me-your-secrets-how-the-use-of-trade-secrets-relates-to-the-demand-for-transparent-artificial-intelligence-part-ii. Acesso em: 24 mar. 2024.

[254] Sobre esse ponto, é preciso dar ciência ao outro de que determinada informação é considerada segredo de negócio, ainda que de forma tácita, para atrair a ele os deveres de não compartilhar essas informações indevidamente. Tal ressalva se coaduna com o fato de que uma parte do valor agregado aos segredos de negócio advém do conhecimento de terceiros sobre a existência de informações comercialmente relevantes que não estão publicamente disponíveis (MILLER, Megan Marie. Data as the New Oil: A Slippery Slope of Trade Secret Implications Greased by the California Consumer Privacy Act. *Cybaris*: Vol. 12: Iss. 1, Article 1, 2021. p. 26. Disponível em: https://open.mitchellhamline.edu/cybaris/vol12/iss1/1/. Acesso em: 08 fev. 2024. Ver também: KORS, Jorge Alberto. *Los secretos industriales y el know how*. Buenos Aires: La Ley, 2007, p. 107-108).

[255] Pontes de Miranda já dizia que segredos de negócio também são suscetíveis de serem transmitidos, podendo-se até considerar a possibilidade de serem arrendados ou licenciados (PONTES DE MIRANDA, Francisco Cavalcanti. *Tratado de Direito Privado*. Parte Especial. 4. ed. São Paulo: Revista dos Tribunais, 1983, v. 16. p. 661). Também sobre as formas contratuais de transmissão dos segredos, ver: SILVEIRA, João Marcos. A proteção jurídica dos segredos industriais e de negócio. *Revista da ABPI*. Vol. 53, jul/ago 2001. p. 22-23. Disponível em: https://abpi.org.br/bfd_download/edicao-53-mes-julho-agosto-ano-2001/. Acesso em: 22 maio 2024.

negócio serem divulgados em circunstâncias específicas, desde que adotadas as medidas necessárias para que a informação se mantenha fora do domínio público.

Outros diplomas também estabelecem a possibilidade de serem fornecidos segredos de negócio para autoridades públicas no âmbito de suas competências fiscalizatórias. Durante acordos de leniência e termos de ajustamento de conduta, é comum autoridades como o CADE (Conselho Administrativo de Defesa Econômica) ou o Ministério Público Federal terem acesso a informações que são consideradas segredos de negócio em processos nos quais também são partes seus concorrentes diretos.

Há previsão regimental do CADE para que esses feitos tramitem em condição de sigilo e que os acessos sejam restritos especialmente quando relacionados a informações que são segredos de negócio[256]. Nesse caso, é evidente que as autoridades públicas que têm acesso a essas informações assumem o dever de preservá-las em sigilo, devendo empenhar esforços de segurança para que elas não vazem. Mas o fato de serem segredos de negócio não exime o agente econômico de fornecê-las, caso seja requisitado.

A Lei Federal n. 10.603/2002, já mencionada anteriormente, igualmente fala sobre o compartilhamento dos segredos de negócio com a autoridade como uma condição essencial para aprovação do registro, o que mostra que o caráter de sigilo desse tipo de conteúdo não é absoluto[257]. Ou seja, a confidencialidade das informações não necessariamente as mantêm restritas ao âmbito empresarial[258]. Por outro lado, a referida lei concede a essas informações uma proteção contra o uso e a divulgação indevida, mitigando riscos de concorrência desleal e trazendo segurança aos agentes econômicos de que seus segredos de negócio vão permanecer em segredo.

Até mesmo o TRIPS deixa claro que a condição sigilosa conferida aos segredos de negócio não é absoluta. Em seu art. 39.3, o Tratado prevê a possibilidade de divulgação

---

[256] Cf. Art. 52 do Regimento Interno do CADE. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/regimento-interno/Regimento-interno-Cade-versao-05-2021.pdf. Acesso em: 25 mar. 2024. Pela norma, segredos de negócio podem ser, dentre outros, escrituração mercantil, situação econômico-financeira da empresa, sigilo fiscal ou bancário, processos produtivos, fórmulas relativas à fabricação de produtos, faturamento, valores e operações de pagamento, relatórios anuais, demonstrativos financeiros, listas de clientes e fornecedores, capacidade instalada e custos de produção.

[257] Em certa medida, até mesmo a condição sigilosa dessas informações é questionável. Em se tratando de dados não divulgados sobre produtos específicos (fármacos especialmente), essas informações podem ser consideradas de interesse público direto, o que as diferencia de segredos de negócio em geral, já que não dizem respeito somente à empresa e suas atividades. Nesse sentido, ver: BARBOSA, Denis Borges. Exclusividade de dados sigilosos: agroquímicos. *In*: BARBOSA, Denis Borges. *Da Tecnologia à Cultura*: ensaios e estudos de Propriedade Intelectual. Rio de Janeiro: Lumen Juris, 2011. p. 541. Disponível em: https://www.dbba.com.br/wp-content/uploads/tecnologia_a_cultura.pdf Acesso em: 23 mar. 2024.

[258] BARBOSA, *op. cit*., p. 530. Também sobre o entendimento do TRIPS em relação à condição sigilosa dos segredos, ver: BASSO, Maristela. *O direito internacional da propriedade intelectual*. Porto Alegre: Livraria do Advogado, 2000. p. 247-248.

de determinados segredos de negócio a autoridades, estabelecendo como condição de conformidade o empenho de esforços para proteger essas informações de usos desleais e divulgações públicas[259].

O alcance do sigilo conferido aos segredos de negócio, portanto, é relativo[260] e coexiste por meio do paradoxal e necessário balanceamento entre a restrição de acesso e a divulgação necessária ao exercício da atividade empresarial[261]. Por esse motivo, os segredos de negócio podem ser vistos como uma espécie de gestão do fluxo informacional[262] – o que talvez seja o cerne do argumento que tenta os aproximar de um desdobramento do direito de privacidade.

Contudo, descartada a possibilidade de se atribuir esse desdobramento da personalidade aos agentes econômicos, pode-se extrair a proximidade da categoria jurídica, de ser também uma forma de controle sobre como a informação é utilizada no mercado; sobre como um determinado conteúdo é explorado por terceiros. O alcance do sigilo conferido aos segredos pode também ser avaliado contextualmente, de modo que, em determinadas situações, seu compartilhamento será vedado em razão do risco de concorrência desleal, mas em outras, poderá ser permitido, para possibilitar a atividade comercial ou dar cumprimento a uma obrigação legal.

O que se percebe, portanto, é que a previsão de proteção aos segredos de negócio, em nenhuma medida, impõe que eles sejam conteúdos armazenados sob condições absolutas de sigilo, existindo uma série de circunstâncias possíveis que autorizam o seu compartilhamento, especialmente com autoridades. Isso faz com que a tutela jurídica dos segredos seja mais voltada à regulação de um fluxo informacional controlado, dentro das

---

[259] Diz o art. 39.3 do TRIPS: "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".

[260] SANDEEN. Sharon K. The limits of trade secret law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on which it is based. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 555.

[261] MADISON, Michael J. Open Secrets. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 222-224; 234-235.

[262] OCAÑA, Teresa Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020. p. 29.

perspectivas de interesse do agente econômico, do que propriamente para a manutenção de informações completamente inacessíveis por terceiros.

II.2 A PROTEÇÃO DOS SEGREDOS DE NEGÓCIO E O CAPITALISMO: PRESTIGIANDO O ACÚMULO DE RIQUEZA

As reflexões introdutórias sobre a sistemática de proteção dos segredos de negócio e sua condição sigilosa são importantes para compor uma crítica sobre o papel desse tipo de tutela jurídica para o mercado de dados pessoais, especialmente quando se pensa no eixo orientativo central da proteção de dados, que é a transparência.

É fácil concluir que a existência de um modelo de proteção dos segredos de negócio é relevante para o desenvolvimento do capitalismo, especialmente quando se pensa no mercado de dados pessoais e no desenvolvimento de novas tecnologias[263]. Juntamente com a tutela da propriedade intelectual, é comum dizer que os segredos de negócio são responsáveis por proteger e potencializar a inovação, viabilizar a exploração de bens imateriais, promover o estímulo à atividade inventiva e incentivar a competição em nível mais elevado[264]. Diz-se que, em razão desses dois institutos, teriam sido erradicadas inúmeras doenças e permitidas inovações tecnológicas disruptivas, já que o sistema de patentes e a proteção das informações essenciais ao negócio são injeções de incentivo aos agentes econômicos para continuarem promovendo pesquisa e buscando novos conhecimentos[265].

---

[263] O histórico de origem dos segredos de negócio remete à Europa medieval, quando se organizaram corporações de ofícios que controlavam a produção de bens e as regulações de comércio. Naquela época, seus membros se organizaram informalmente em busca de uma proteção orgânica fundada na confidencialidade de importantes aspectos de suas atividades. Mas com o fim do regime feudal e o início dos processos de industrialização, surgiu a necessidade de formalizar algum tipo de proteção aos elementos que se mostravam diferenciais na produção. Uma primeira menção a segredos de fábrica foi identificada no Código Penal francês de 1810, prevendo penas caso os segredos fossem comunicados a terceiros. Sobre o tema, ver: GERALDES, João de Oliveira. Sobre a proteção jurídica dos segredos comerciais no espaço digital. *Revista da Faculdade da Universidade de Lisboa*, vol. LXIII, 1 e 2, Lisboa, 2022. p. 416-417. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Joa%CC%83o-de-Oliveira-Geraldes_compressed.pdf. Acesso em: 06 out. 2023.

[264] VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual.* 2. ed. São Paulo: Almedina, 2020. p. 27; CUEVA, Ricardo Villas Bôas. A importância de proteger o segredo de negócio. *In* CALCINI, Ricardo; ANDRADE, Dino (org.). *Reflexões Jurídicas Contemporâneas*. Leme-SP: Mizuno, 2022. p. 264.

[265] VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual.* 2. ed. São Paulo: Almedina, 2020. p. 28. Teresa Ocaña também destaca como essa retórica foi utilizada em casos julgados pela Suprema Corte nos Estados Unidos, para conferir um regime protetivo maior para as informações consideradas segredos. Segundo a autora, o argumento utilizado é de que segredos de negócio seriam uma tutela jurídica capaz de chegar em dimensões que a propriedade intelectual até então não havia conseguido, o que poderia trazer como consequência o estímulo à criação independente e à inovação nos mercados (OCAÑA, Teresa

A defesa dos segredos de negócio pode ser, nesse aspecto, colocada tanto em dimensão privada quanto em dimensão social. A dimensão privada é evidente e atende aos interesses diretos dos agentes econômicos que querem ter preservadas de seus concorrentes as informações essenciais de seus negócios. Resgata-se, para tanto, uma ideia de ética comercial, de valor do trabalho e da produção individual[266], com objetivo de proteger informações pertinentes ao setor técnico e industrial das empresas (como procedimentos de fábrica, linhas de produção ou práticas manuais); ao setor comercial (como listas de clientes, fornecedores, preços, estudos de mercado); ou ao setor organizacional (estrutura interna da empresa, relação com empregados, balanços financeiros)[267].

Na dimensão chamada social, os segredos de negócio preservariam interesses coletivos relacionados à manutenção de ambientes de livre concorrência, especialmente diante de análises que concluem que os custos para os mercados em geral seriam maiores se não houvesse proteção desses segredos. A ideia, em síntese, é que a proteção dos segredos traz estímulos positivos para a concorrência, prestigiando ambientes de busca por inovação e superação que, ao fim, são revertidos para a população[268].

A narrativa, inserida no contexto do capitalismo, atende fortemente aos interesses dos agentes de mercado e vem sendo questionada por diversos motivos. Primeiro, porque coloca nos agentes privados um protagonismo de inovação que não necessariamente lhes deve ser atribuído. Sabe-se que grande parte da verdadeira disrupção que chega aos mais variados mercados não tem origem nos investimentos dos entes privados, mas sim nas pesquisas financiadas pelo Estado, que assume o risco de protagonizar os estudos científicos de maior risco[269]. Quando maduro, esse conhecimento é apropriado pelos agentes privados e aprimorado de acordo com seus interesses de mercado, sendo então incluído dentro da proteção das patentes e dos segredos de negócio como se tivesse sido, desde o início, desenvolvido por eles[270].

Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020. p. 38).

[266] OCAÑA, *op. cit*., p. 32-35.

[267] FEKETE, Elisabeth Kasznar. *O regime jurídico do segredo de indústria e comércio no direito brasileiro.* Rio de Janeiro: Forense, 2003. p. 22.

[268] VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual.* 2. ed. São Paulo: Almedina, 2020. p. 98.

[269] "o governo não se limitou a criar as 'condições para a inovação', mas financiou ativamente as pesquisas iniciais radicais e criou as redes necessárias entre as agências estatais e o setor privado para facilitar o desenvolvimento comercial" (MAZZUCATO, Mariana. *O estado empreendedor*: desmascarando o mito do setor público vs. setor privado. São Paulo: Portfólio-Pinguim, 2014. p. 121).

[270] MAZZUCATO, *op. cit*., p. 224-225.

Segundo, porque os chamados benefícios coletivos, que prestigiariam a concorrência e trariam vantagens para a população como um todo, tendem a ser pequenos frente aos custos sociais trazidos pela inovação. Novas máquinas, tecnologias e inteligências artificiais prometem aumento da eficiência e maior estabilidade aos mercados, mas, na prática, acabam diminuindo a força de trabalho humana, especialmente aquela menos qualificada, que se encontra na base da pirâmide social [271]. Em prol do aumento de seus lucros, os agentes econômicos se utilizam da inovação para fazerem uma melhor gestão de seus riscos e alocarem capital de forma mais segura, independentemente do impacto disso[272].

Os custos sociais também são percebidos quando o aumento da produção e dos critérios de eficiência acabam não sendo distribuídos para vários agentes econômicos diferentes, e ficam restritos a grandes atores econômicos (que geralmente já exercem algum tipo de monopólio nos mercados), sem que haja democratização desse conhecimento[273]. Aumentam-se então os custos de entrada aos mercados[274] e o valor da informação, sem que aumentem simultaneamente os benefícios para a maior parte da população e até mesmo da indústria, que não desenvolve conhecimento próprio e depende da interação com outros agentes econômicos[275].

Estudos demonstram que as proteções conferidas à propriedade intelectual e aos segredos de negócio são importantes estruturas jurídicas que favorecem a criação e a manutenção de riquezas e, por isso, têm importante impacto no desenvolvimento do capitalismo. A dimensão de proteção dos interesses privados costuma ser a mais prestigiada, fazendo com que o Direito seja um instrumento importante para assegurar a geração de lucro a partir de bens imateriais[276].

---

[271] RODRIK, Dani. *Straight Talk on Trade*. Ideas for a Sane World Economy. New Jersey: Princeton University Press, 2018. p. 260; HASKEL, Jonathan; WESTLAKE, Stian. *Capitalism without capital*. The rise of the intangible economy. Princeton & Oxford: Princeton University Press, 2018. p. 123.
[272] STIGLITZ, Joseph E.; GREENWALD, Bruce C. *Creating a Learning Society*: a new approach to Growth, Development and Social Progress. New York: Columbia University Press, 2015. p. 132.
[273] STIGLITZ; GREENWALD, *op. cit*., p. 135.
[274] *Ibid*., p. 122.
[275] BENKLER, Yochai. *The Wealth of Networks*: How Social Production Transforms Markets and Freedom. Yale University Press, 2006. p. 461.
[276] Nesse sentido, Karl Marx teceu considerações importantes no sentido de que o valor do trabalho decorre também do tempo necessário para a produção. Com a inserção de tecnologias nos meios de produção, o tempo de produção diminui e, por consequência, igualmente diminui o valor do trabalho (MARX, Karl. *O capital*. Livro 1. São Paulo: Boitempo, 2014. p. 482 *et seq*). Reflexões sobre essa afirmação mostram que, por isso, o propósito das tecnologias nunca será de melhorar as condições dos trabalhadores, mas sim de servir como forma de valorização do capital, reduzindo os salários e aumentando os lucros (HARVEY, David. *A loucura da razão econômica*. Marx e o capital no século XXI. São Paulo: Boitempo, 2018. p. 113).

A esse respeito, Katharina Pistor coloca os direitos de propriedade intelectual como uma ferramenta dos agentes econômicos[277], na medida em que asseguraram a possibilidade de exploração de bens imateriais para geração de riqueza[278]. Com isso, os segredos se tornam uma forma de conferir uma série de privilégios aos agentes econômicos, a ponto de colocá-los em posições de vantagens que atendem exclusivamente os seus interesses[279].

Em sentido similar, Ugo Mattei e Laura Neder destacam como os direitos de propriedade intelectual como um todo e a proteção aos segredos de negócio se mostram como ferramentas que perpetuam situações de desequilíbrio de poder entre os atores de um mercado. Seriam instrumentos teoricamente respaldados pelo Estado de Direito, mas que prestigiam e perpetuam monopólios, desigualdades e exploração[280].

Um terceiro motivo que se deve considerar é que estudos mais recentes demonstram a falácia do argumento de que a proteção da inovação somente é possível por meio dos modelos que pretendem garantir algum tipo de exclusividade e sigilo à exploração daquele conteúdo. Para alguns mercados específicos, talvez essa estrutura seja importante, mas o desenvolvimento não necessariamente deve estar vinculado a esse modelo de tutela jurídica.

---

[277] PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. p. 147.

[278] "As they show, about half of the intangible investments are not recognized in national accounts; but law has a label for all of them, called patents, trademarks, property rights, and a catchall category of "other," which can be deciphered as trade secrets as well as business processes. Still, the authors hesitate to draw the obvious conclusion that there is a powerful link between law and intangibles, indeed, that the law is the source code for transforming ideas, skills, know-how, even processes, into capital" [Conforme mostram, cerca de metade dos investimentos intangíveis não são reconhecidos nas contas nacionais; no entanto, a lei tem uma etiqueta para todos eles, chamada patentes, marcas registradas, direitos de propriedade, e uma categoria abrangente de "outros", que podem ser decifrados como segredos comerciais, bem como processos empresariais. Ainda assim, os autores hesitam em tirar a conclusão óbvia de que existe uma ligação poderosa entre a lei e os intangíveis, de fato, que a lei é o código-fonte para transformar ideias, habilidades, know-how, até mesmo processos, em capital] (PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. p. 116, tradução livre).

[279] Afirma Pistor: "This may be dismissed as the typical hyperbole of a lawyer, but it fits squarely the worldview of patent lawyers who have claimed that patents, not humans, were responsible for the Industrial Revolution. Yet, we often celebrate the new discoveries and technical breakthroughs, but ignore the legal work behind the scenes that gives these breakthroughs lasting wealth effects" [Isso pode ser descartado como a hipérbole típica de um advogado, mas se encaixa perfeitamente na visão de mundo dos advogados de patentes que afirmaram que as patentes, não os seres humanos, foram responsáveis pela Revolução Industrial. No entanto, muitas vezes celebramos as novas descobertas e avanços técnicos, mas ignoramos o trabalho jurídico nos bastidores que proporciona a esses avanços e descobertas efeitos longevos na riqueza] (PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. p. 130, tradução livre).

[280] MATTEI, Ugo; NADER, Laura. *Plunder*: When the rule of law is illegal. Blackwell Publishing Ltd., 2008. p. 85; 176-179.

Existem estudos demonstrando que prestigiar a democratização e o compartilhamento do conhecimento tende a ter um potencial de impulsionar criações e adaptações de forma mais célere e positiva para os agentes privados e para a sociedade[281]. Argumenta-se que concepções sobre cópias dos produtos e atividades ignoram que existe maior potencial de criação a partir do que já foi desenvolvido. Não só, manter estruturas patrimoniais de proteção da inovação acabam trazendo custos altos para a concorrência, aumentando as barreiras e os custos de entrada nos mercados[282].

A partir dessas conclusões, existem hoje modelos diferentes, chamados abertos (*open inovation*), que propagam a difusão da informação e o compartilhamento do conhecimento. O lucro viria pela criação de caminhos para o desenvolvimento, pelo compartilhamento de tecnologias entre os mercados, e pela integração de diferentes tipos de atividades que possam promover mudanças concretas e mais significativas[283].

---

[281] KUENZLER, Adrian. *Restoring Consumer Sovereignty*. How Markets Manipulate Us and What the Law Can do About It. New York: Oxford University Press, 2017. p. 204-205.

[282] OCAÑA, Teresa Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020. p. 37.

[283] "The open innovation paradigm as I've defined it is best understood as the antithesis of the traditional vertical integration model in which internal innovation activities lead to internally developed products and services that are distributed by the firm. In a sentence, open innovation is a distributed innovation process that relies on purposively managed knowledge flows across organizational boundaries, using pecuniary and nonpecuniary mechanisms in line with the organization's business model to guide and motivate knowledge sharing (see Chesbrough and Bogers 2015. p. 3). This is an admittedly academic definition. It basically means that innovation is generated by accessing, harnessing, and absorbing flows of knowledge across the firm's boundaries" [O paradigma da inovação aberta, conforme defini, é melhor compreendido como a antítese do modelo tradicional de integração vertical, no qual as atividades de inovação interna resultam em produtos e serviços desenvolvidos internamente que são distribuídos pela empresa. Em uma frase, a inovação aberta é um processo de inovação distribuída que depende de fluxos de conhecimento gerenciados propositalmente através de fronteiras organizacionais, utilizando mecanismos pecuniários e não pecuniários em consonância com o modelo de negócios da organização para orientar e motivar o compartilhamento de conhecimento (ver Chesbrough e Bogers, 2015. p. 3). Esta é uma definição reconhecidamente acadêmica. Basicamente, significa que a inovação é gerada acessando, aproveitando e absorvendo fluxos de conhecimento através das fronteiras da empresa] (CHESBROUGH, Henry. The Future of Open Innovation. The future of open innovation is more extensive, more collaborative, and more engaged with a wider variety of participants. *Research-Technology Management*. 60 (1), 2017. p. 35, tradução livre. Disponível em: https://doi.org/10.1080/08956308.2017.1255054. Acesso em: 12 jan. 2024). Adiante, prossegue o autor: "The new logic will exploit this diffusion of knowledge, rather than ignore it. The new logic turns the old assumptions on their head. Instead of making money by hoarding technology for your own use, you make money by leveraging multiple paths to market for your technology. Instead of restricting the research function exclusively to inventing new knowledge, good research practice also includes accessing and integrating external knowledge. Instead of managing intellectual property (IP) as a way to exclude anyone else from using your technology, you manage IP to advance your own business model and to profit from your rivals' use. Your own R&D strategy should benefit from external start-up companies' abilities to initiate multiple organizational experiments to commercialize technologies. You might even occasionally help fund a young start-up to explore an area of potential future interest" [A nova lógica explorará essa difusão de conhecimento, em vez de ignorá-la. A nova lógica subverte as antigas suposições. Em vez de ganhar dinheiro guardando tecnologia para uso próprio, você ganha dinheiro alavancando múltiplos caminhos para o mercado para sua tecnologia. Em vez de restringir a função de pesquisa exclusivamente à criação de novo conhecimento, uma boa prática de pesquisa também inclui o acesso e a integração de conhecimento externo. Em vez de gerenciar a propriedade intelectual (PI) como uma maneira de excluir

Mesmo fora dos modelos de inovações abertas, já existem importantes reflexões sobre como as leis de proteção dos segredos de negócio deveriam se adaptar para garantir proteção jurídica às informações, sejam elas sigilosas ou não[284]. A ideia é sofisticar o sistema de proteção da propriedade intelectual para que se criem estímulos para a difusão do conhecimento. A proteção das informações valiosas para as empresas não estaria mais associada à sua condição de segredo, mas sim ao seu modelo de exploração, que deve ser legítimo e autorizado[285].

A perspectiva de existir uma proteção da inovação exclusivamente através dos segredos, exercida em termos tão amplos, é também altamente questionada. O alcance do sigilo conferido a essa categoria jurídica pode não oferecer contrapartidas de transparência nem limitações temporais (na maior parte dos casos) que justifiquem os custos sociais desse modelo[286]. É com base nessas distorções que muito se fala sobre os

---

qualquer outra pessoa do uso de sua tecnologia, você gerencia a PI para avançar seu próprio modelo de negócios e lucrar com o uso de seus concorrentes. Sua própria estratégia de pesquisa e desenvolvimento deve se beneficiar das habilidades de empresas iniciantes externas para iniciar múltiplos experimentos organizacionais para comercializar tecnologias. Você até mesmo ocasionalmente pode ajudar a financiar uma jovem empresa iniciante para explorar uma área de interesse futuro potencial] (CHESBROUGH, Henry. The Future of Open Innovation. The future of open innovation is more extensive, more collaborative, and more engaged with a wider variety of participants. *Research-Technology Management*. 60 (1), 2017. p. 51-52, tradução livre. Disponível em: https://doi.org/10.1080/08956308.2017.1255054. Acesso em: 12 jan. 2024).

[284] Autores defendem, inclusive, que a sociedade em redes e as novas dimensões do fluxo informacional prestigiam esses novos modelos, na medida em que diluem a concentração de conteúdo e de informação nas mãos de poucos agentes econômicos. Seriam modelos que não estão baseados propriamente na ideia de uma propriedade intelectual, mas sim na conectividade, no compartilhamento e na troca de conhecimento, na reciprocidade e redistribuição. Sobre o tema, ver: BENKLER, Yochai. *The Wealth of Networks*: How Social Production Transforms Markets and Freedom. Yale University Press, 2006. Apesar da empolgação do autor sobre as possibilidades de interação na rede, não se pode ignorar que a formação de conteúdo e as interações em redes não são espontâneas, mas sim resultados de operações preditivas desenhadas e conduzidas a partir dos interesses de alguns poucos agentes econômicos que intermediam e controlam as relações sociais. Pensar que surgem hoje possibilidades de inovação e autonomia maiores do que antes, simplesmente porque a sociedade em redes permite maiores níveis de conexão, seria ignorar o poder dos algoritmos e o poder dos dados pessoais. Até mesmo o espaço de reconquista da esfera pública que defende o autor já foi refutado em razão dos filtros-bolhas e das intermediações e interferências algorítmicas na formação da convicção política, conforme bem trazido por SUSTEIN, Carl. *Republic*: Divided Democracy in the Age of Social Media. Princeton University Press, 2017.

[285] LEMLEY, Mark A. The Surprising Virtues of Treating Trade Secrets as IP Rights. *Stanford Law Review*, v. 61, 2008. p. 311. Disponível em: https://law.stanford.edu/sites/default/files/publication/258632/doc/slspublic/Lemley%20Surprising.pdf. Acesso em: 03 mar. 2024.

[286] Como diz André R. C. Fontes: "A base da patente é a revelação, a transparência sobre a estrutura da invenção. O inventor põe à disposição da sociedade seu conhecimento mediante a outorga de um prazo de exclusividade. Dessa maneira, a patente qualifica-se como a técnica mais característica de proteger uma invenção, a despeito de alguns setores industriais, como o de alimentos, preferirem manter segredo em sua indústria e não patentear seus produtos" (FONTES, André R. C. Patente, invenção e inovação. *Revista da Escola da Magistratura Regional Federal* / Escola da Magistratura Regional Federal, Tribunal Regional Federal da 2ª Região. Edição Especial de Propriedade Intelectual. Rio de Janeiro, 2011. p. 281. Disponível em: https://emarf.trf2.jus.br/site/documentos/revistapinternet2011.pdf. Acesso em: 12 jan. 2024).

segredos de negócio como um modelo de proteção dos interesses do capital que não equilibram interesses da coletividade[287].

A importância dessa discussão, ao fim, é perceber que existe todo um discurso de valorização da inovação que acaba mascarando a existência de uma estrutura jurídica que serve, antes de tudo, à consolidação de privilégios dos agentes privados[288]. Sendo o Direito construído a partir de forças políticas mutáveis, que favorecem o desenvolvimento dos mercados a partir da preservação dos interesses privados, a construção de uma tutela jurídica dos segredos de negócio não se dá de forma diferente.

As tensões políticas dificultam uma regulação mais concreta dos segredos de negócio, que consiga criar bases claras para equilibrar a proteção aos interesses dos agentes econômicos, os interesses sociais e as perspectivas de transparência. Nesse vácuo regulatório mais nítido, os agentes econômicos se beneficiam, explorando com seus advogados as lacunas legislativas, a fim de criar precedentes judiciais que prestigiem apenas os seus interesses particulares[289].

Reflexões feitas por Julie Cohen reforçam essas conclusões, na medida em que a autora percebe a proteção hoje conferida à propriedade intelectual (em geral) como uma das importantes responsáveis pelas desigualdades causadas no atual contexto do capitalismo. Segundo Cohen, a propriedade intelectual passou por mutações ao longo dos anos com o objetivo de favorecer os interesses privados, a partir de interpretações excessivamente amplas sobre seus fundamentos. As consequências foram barreiras de acesso cada vez mais altas a novos competidores; monopólios de poder para determinados agentes; controle mais intenso do fluxo informacional e dos dados pessoais; disponibilização excessiva de informações sobre os indivíduos; controle de acesso a

---

[287] MOORE, Taylor R. Trade Secrets and Algorithms as Barriers to Social Justice. *CDT Free Expression Fellow*. 2017. p. 10. Disponível em: https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf. Acesso em: 2 maio 2024. A renomada doutrina brasileira também comenta que a limitação temporal das patentes (que inexiste no segredo de negócio) faz delas instrumentos socialmente mais produtivos. Ver: BARBOSA, Denis Borges. *Uma introdução à propriedade intelectual*. 2. ed. Lumen Juris, 2010. p. 644. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 21 mar. 2024. p. 295.

[288] Esse é o movimento identificado por Maria Rosária Ferrarese, de que o direito frequentemente é tratado de forma apolítica, por meio de discursos rasos focados apenas na aplicação das normas e na observância dos precedentes, sem que se percebam os processos políticos de uso do poder para criar imunidades regulatórias e espaços mais vantajosos (para os agentes econômicos) de exploração da atividade comercial. Ver: FERRARESE, Maria Rosaria. Europe and institutional change. Law: from science to "fit for purpose"? *Économie et institutions.* v. 23, p. 1-12, 2015. Disponível em: https://doi.org/10.4000/ei.5718. Acesso em: 02 jun. 2024.

[289] PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. p. 160-167.

dados e tecnologias; e dificuldades para inovação com vistas ao desenvolvimento social[290].

As tensões envolvendo os segredos de negócio e sua tutela jurídica são endereçadas em diversos países, com tradições e modelos regulatórios diferentes. Na Europa, por exemplo, a Diretiva (UE) 2016/943 tentou uniformizar para os Estados-membros os níveis de proteção dos segredos de negócio[291], criando premissas básicas para proteção desse tipo de informação e trazendo certa harmonia para a apuração do uso indevido das informações secretas dos agentes econômicos, especialmente fora de contextos de concorrência desleal[292].

Houve, portanto, uma iniciativa específica para qualificar a natureza do que seriam informações consideradas como segredos[293], detalhar minimamente a extensão de sua proteção e especificar regimes de ressarcimento e punição quando violada a tutela conferida[294]. Mas, ainda assim, permaneceram significativas lacunas que hoje trazem como consequência a possibilidade de os agentes econômicos de ampliarem excessivamente os seus direitos de exploração sobre essas informações[295].

---

[290] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019; BUCHER, Taina. *If...Then*: Algorithmic power and politics. Oxford University Press, 2018.

[291] Até diante da Diretiva, é importante destacar que os países dentro do bloco europeu ainda podem possuir estruturas jurídicas de proteção dos segredos de negócio que mudam muito entre si. Ver: BANTERLE, Francesco. 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. *In*: BAKHOUM, Mor; CONDE GALLEGO, Beatriz; MACKENRODT, Mark-Oliver M.; SURBLYTĖ-NAMAVIČIENĖ, Gintaré (eds.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law*: Towards a Holistic Approach? Springer: Berlin, 2018. p. 6-7.

[292] VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual.* 2. ed. São Paulo: Almedina, 2020. p. 104.

[293] A partir da Diretiva, ficou especificado que a informação comercial não poderia ser protegida em si mesma. Seu valor econômico decorrente de seu sigilo, devendo esse elemento ser alvo de cautelas específicas, materializáveis em esforços ativos por parte do agente de mercado. Ver: VICENTE, *op. cit*., p. 105.

[294] *Ibid*. p. 104-105.

[295] "In this section, we consider what lessons should be taken from our empirical findings when it comes to future EU policymaking for trade secrets protection. In response to the empirical findings, our recommendations relate to three areas: (i) clarification of the definition of trade secret; (ii) complementarity between trade secrets and other protection regimes; and (iii) effective legal enforcement. We argue that, while there are some minor, legislative improvements that could be initiated in relation to trade secrets, for the most part, it is a matter of preserving the status quo and allowing for jurisprudence to develop. Alongside this, information gathering about implementation of the TSD and workshops to increase knowledge and awareness of best practices would be helpful. It will also be important to ensure that the flexibility trade secrets protection allows when it comes to data sharing is not undermined by complementary forms of protection, such as contract, copyright and the sui generis database right. To that end, there needs to be serious consideration of abolition or reform of the database right" [Nesta seção, consideramos quais lições devem ser extraídas de nossas descobertas empíricas quando se trata da formulação futura de políticas da UE para a proteção de segredos comerciais. Em resposta às descobertas empíricas, nossas recomendações se relacionam a três áreas: (i) esclarecimento da definição de segredo comercial; (ii) complementaridade entre segredos comerciais e outros regimes de proteção; e (iii) aplicação legal eficaz. Argumentamos que,

Nos Estados Unidos, a principal proteção dos segredos de negócio vem do *Defend Trade Secrets Act*. Sancionado em 2016, o diploma conseguiu federalizar a matéria e estabelecer um regime preventivo, compensatório e punitivo em relação aos segredos de negócio. Assim, através do *Act*, foi possível nacionalizar a tutela jurídica da matéria (o que é relevante, considerando o federalismo norte-americano) para criar critérios mais amplos não só para a proteção dos segredos, mas também para as punições pela usurpação das informações e uso desautorizado por terceiros[296]. Por outro lado, o país também enfrenta discussões sobre as dificuldades regulatórias que envolvem a definição da natureza jurídica, as limitações temporais da tutela, o enquadramento do que pode ser considerado como segredo de negócio e quais as formas mais concretas de se conciliarem os interesses sociais com os interesses privados[297].

II.3 OS ELEMENTOS DO MERCADO DE DADOS PESSOAIS E SEU ENQUADRAMENTO COMO SEGREDOS DE NEGÓCIO: UMA ESCOLHA POLÍTICA DOS AGENTES DE TRATAMENTO

Como brevemente exposto até aqui, a tutela jurídica dos segredos de negócio traz, por si só, preocupações importantes. São questões sobre o alcance do sigilo conferido às informações, sobre o modelo de proteção da inovação com base no segredo; sobre uma

---

embora existam algumas melhorias legislativas menores que poderiam ser iniciadas em relação aos segredos comerciais, na maior parte, é uma questão de preservar o status quo e permitir o desenvolvimento jurisprudencial. Paralelamente a isso, a coleta de informações sobre a implementação do TSD e workshops para aumentar o conhecimento e a conscientização das melhores práticas seriam úteis. Também será importante garantir que a flexibilidade que a proteção de segredos comerciais permite quando se trata de compartilhamento de dados não seja prejudicada por formas complementares de proteção, como contrato, direitos autorais e o direito sui generis de banco de dados. Para esse fim, é necessário haver uma séria consideração sobre a abolição ou reforma do direito de banco de dados] (APLIN, Tanya; RADAUER, Alfred; BADER, Martin A.; SEARLE, Nicola. The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis. *National Library of Medicine*. 2023, tradução livre. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10170042/#Fn53. Acesso em:10 fev. 2024.

[296] VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual.* 2. ed. São Paulo: Almedina, 2020. p. 101; DESAUNETTES-BARBERO, Luc. *Trade Secrets Legal Protection*. From a Comparative Analysis of US and EU Law to a New Model of Understanding. Switzerland: Springer, 2023. p. 71-73.

[297] JAMAR, Steven D. Trade Secrets from an IP Social Justice Perspective (November 16, 2021). Trade Secrets from an IP Social Justice Perspective, in Cambridge Handbook on IP-SJ (Steven D. Jamar & Lateef Mtima editors (forthcoming Cambridge University Press 2022). *Howard Law Research Paper*. Disponível em: http://dx.doi.org/10.2139/ssrn.3964977. Acesso em: 19 fev. 2024. Ver também: VOGT, Sander. Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence—Part II. *In*: *The Journal of Robotics, Artificial Intelligence & Law* (Fastcase), Volume 5, No. 5, September–October 2022, Full Court Press, an imprint of Fastcase, Inc. p. 305-310. Disponível em: https://www.crowell.com/en/insights/publications/show-me-your-secrets-how-the-use-of-trade-secrets-relates-to-the-demand-for-transparent-artificial-intelligence-part-ii. Acesso em: 24 mar. 2024.

estrutura fornecida pelo Direito que pode trazer custos sociais significativos, dentre outras.

No mercado de dados pessoais, a preocupação sobre os segredos de negócio não é mais simples.

Viu-se que a atividade econômica de exploração dos dados está fortemente associada a dinâmicas de poder que impactam no desenvolvimento da coletividade, na conformação da personalidade individual, nas relações, nos processos democráticos e em várias outras esferas da vida humana. Nos níveis em que existe hoje, o mercado de dados apresenta disfuncionalidades, pois, apesar dos esforços legislativos e regulatórios, não consegue materializar suficientemente a transparência.

Em alguma medida, o Direito pode acabar contribuindo para essa disfuncionalidade, uma vez que fornece alguns instrumentos jurídicos para que os agentes consigam resguardar seus interesses e ampliar as suas possibilidades de lucro. Um desses instrumentos pode ser o dos segredos de negócio.

Ao longo dos últimos anos, foi possível perceber que o uso dos segredos de negócio como instrumento utilizado pelos agentes econômicos para proteção da inovação está em plena expansão[298]. Em mercados disruptivos (como o de dados pessoais), os segredos se mostraram um mecanismo jurídico fortemente vantajoso e preponderante[299], até mesmo quando é utilizado em conjunto com as patentes[300][301].

---

[298] EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE (EUIPO). PROTECTING INNOVATION THROUGH TRADE SECRETS AND PATENTS: DETERMINANTS FOR EUROPEAN UNION FIRMS. p. 23-57. Disponível em: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf. Acesso em: 23 abr. 2024.

[299] Estudos mostram que os segredos de negócio são a principal tutela jurídica utilizada para proteção da inovação em diversos setores diferentes. No Reino Unido, entre 1998 e 2006, apenas 4% das inovações foi protegida pelo regime de patente (HALL, Bronwyn H. *et al*. The importance (or not) of patents to UK Firms. 2013. *NBER Working Paper* No. 19089. Disponível em: http://www.nber.org/papers/w19089. Acesso em: 9 abr. 2024). Nos Estados Unidos, o mesmo padrão é observado (COHEN, Wesley; NELSON, Richard R.; WALSH, John P. Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not). 2000. *National Bureau of Economic Research Working Paper* 7552. Disponível em: http://www.nber.org/papers/w7552. Acesso em: 09 abr. 2024).

[300] EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE (EUIPO). PROTECTING INNOVATION THROUGH TRADE SECRETS AND PATENTS: DETERMINANTS FOR EUROPEAN UNION FIRMS. p. 57. Disponível em: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf. Acesso em: 23 abr. 2024.

[301] Em algumas jurisdições, como no caso da *European Patent Convention*, um dos requisitos para patenteamento de invenções é justamente a possibilidade de explicação suficiente de como aquele sistema funciona (*suficiente-disclosure*). A opacidade inerente às estruturas de tratamento de dados mais sofisticadas, especialmente inteligências artificiais, impedem o cumprimento desse requisito, o que justifica, também sob essa perspectiva, a tutela jurídica através dos segredos de negócio (RUDZITE, Liva. Algorithmic Explainability and the Sufficient-Disclosure Requirement under the European Patent

Vários motivos justificam esse processo: um conjunto distinto de informações e conteúdos pode ser enquadrado como segredos de negócio[302]; a proteção jurídica ampla não prescinde de divulgação ou submissão prévia[303]; trata-se de uma tutela jurídica mais flexível e que permite um enquadramento maior de conteúdos[304]; são menores os custos e burocracias administrativas[305]; e não há, em regra, nenhum tipo de limitação temporal para a proteção[306][307].

Convention. *Juridica International*, [S. l.], v. 31. p. 128, 2022. Disponível em: https://ojs.utlib.ee/index.php/juridica/article/view/19323. Acesso em: 15 abr. 2024).

[302] APLIN, Tanya; RADAUER, Alfred; BADER, Martin A.; SEARLE, Nicola. The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis. *National Library of Medicine*. 2023. p. 11. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10170042/#Fn53. Acesso em:10 fev. 2024.

[303] GERALDES, João de Oliveira. Sobre a proteção jurídica dos segredos comerciais no espaço digital. *Revista da Faculdade da Universidade de Lisboa*, vol. LXIII, 1 e 2, Lisboa, 2022. p. 418- 419. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Joa%CC%83o-de-Oliveira-Geraldes_compressed.pdf. Acesso em: 06 out. 2023. Nesse sentido, Teresa Ocaña também destaca que esse é um dos principais atributos dos segredos de negócio, o que inclusive justifica a mudança que vem ocorrendo com a diminuição dos registros de patentes e aumento do uso dos segredos como instrumento de proteção da inovação (OCAÑA, Teresa Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020. p. 59).

[304] SIEMS, Jasper. Protecting Deep Learning: Could the New EU-Trade Secrets Directive Be an Option for the Legal Protection of Artificial Neural Networks? *In*: EBERS, Martin; GAMITO, Marta Cantero (eds.). *Algorithmic Governance and Governance of Algorithms*. Springer, 2021. p. 153.

[305] Cabe aqui mencionar as conclusões de David D. Friedman, Willian M. Landes e Richard A. Posner sobre os segredos de negócio no sistema do *common law*: "To summarize, trade secret law supplements the patent system. Inventors choose trade secret protection when they believe that patent protection is too costly relative to the value of their invention, or that it will give them a reward substantially less than the benefit of their invention (as reflected, in part, in the length of time before any else will invent it), either because the invention is not patentable or because the length (or other conditions) of patent protection is insufficient" [Para resumir, a lei de segredo comercial complementa o sistema de patentes. Os inventores optam pela proteção de segredo comercial quando acreditam que a proteção por patente é cara em relação ao valor de sua invenção, ou que lhes dará uma recompensa substancialmente menor do que o benefício de sua invenção (como refletido, em parte, no tempo decorrido antes que outra pessoa a invente), seja porque a invenção não é patenteável ou porque o tempo (ou outras condições) de proteção por patente são insuficientes] (FRIEDMAN, David D.; LANDES, William M.; POSNER, Richard A. Some Economics of Trade Secret Law. *Journal of Economic Perspectives*, 5 (1), 1991. p. 64, tradução livre. Disponível em: https://www.aeaweb.org/articles?id=10.1257/jep.5.1.61. Acesso em: 29 jan. 2024).

[306] OCAÑA, Teresa Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020. p. 59.

[307] No Brasil, a Lei n. 10.603/02 estabelece uma previsão setorial específica da indústria de fármacos, produtos veterinários e fertilizantes, sobre dados utilizados em pesquisas de medicamentos e que precisam ser compartilhados com agentes reguladores como requisito para aprovação de novos produtos e comprovação das pesquisas realizadas. Esses dados costumam ser aproveitados por empresas de produtos genéricos para sintetização dos medicamentos, mas há restrição de exclusividade em seu uso por meio de uma limitação temporal significativa (*data exclusivity rights*). Longe de ser uma tentativa de conciliação entre interesses sociais e interesses privados, esse intervalo de tempo durante o qual os dados não podem ser explorados por terceiros acaba constituindo uma verdadeira barreira de acesso para a democratização de determinados medicamentos, que não podem ser sintetizados em sua forma genérica enquanto durar o regime de proteção estabelecido pela lei. Esses dados também podem ser considerados segredos de negócio, ainda que gozem de um regime jurídico diferenciado.

No mercado de dados e de tecnologia, também se argumenta que o sigilo conferido pelos segredos de negócio é medida de segurança: sendo uma atividade de risco, na qual existem possibilidades de desenvolvedores autônomos e *hackers* acessarem os sistemas e os dados que são ali armazenados, proteger o conteúdo por meio dos segredos de negócio ajuda a evitar o acesso[308].

Em uma perspectiva transnacional, pesquisas mostram que as indústrias de tecnologia em geral consideram a tutela jurídica dos segredos de negócio como instrumento mais confiável para proteção da inovação. Os parâmetros de proteção dos segredos de negócio são relativamente compartilhados em muitos países, adotando-se como premissa que o sigilo dos conteúdos tratados dentro dessa categoria jurídica tendem a ser preservados em várias jurisdições diferentes[309]. Por isso, a proteção aos segredos de negócio se mostra como uma técnica de proteção da inovação em âmbito global, que mantém preservados os conteúdos essenciais ao desenvolvimento dos negócios[310].

Explorando essas vantagens, os agentes econômicos conseguem enquadrar vários conteúdos e informações distintos como segredos de negócio, bases de dados, dados pessoais, algoritmos e outros elementos fundamentais ao funcionamento do mercado de dados pessoais.

Por vezes, contudo, o enquadramento pode se mostrar controverso diante da realidade do mercado e dos impactos que os dados pessoais e as tecnologias podem trazer para a coletividade. Essa possível impropriedade da categoria jurídica passa a ser explorada a seguir.

II.3.1 As bases de dados e os segredos de negócio

[308] PASQUALE, Frank A. Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries. *Northwestern University Law Review*. 1 out. 2010. p. 165. Disponível em: https://ssrn.com/abstract=1686043. Acesso em: 22 abr. 2024.

[309] Ver também: VOGT, Sander. Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence—Part II. *In*: *The Journal of Robotics, Artificial Intelligence & Law* (Fastcase), Volume 5, No. 5, September–October 2022, Full Court Press, an imprint of Fastcase, Inc. p. 312-318. Disponível em: https://www.crowell.com/en/insights/publications/show-me-your-secrets-how-the-use-of-trade-secrets-relates-to-the-demand-for-transparent-artificial-intelligence-part-ii. Acesso em: 24 ma. 2024.

[310] GERALDES, João de Oliveira. Sobre a proteção jurídica dos segredos comerciais no espaço digital. *Revista da Faculdade da Universidade de Lisboa*, vol. LXIII, 1 e 2, Lisboa, 2022. p. 418. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Joa%CC%83o-de-Oliveira-Geraldes_compressed.pdf. Acesso em: 06 out. 2023.

Dados pessoais são organizados por meio de grandes bases que são administradas e exploradas pelos agentes de tratamento. Pela LGPD, as bases de dados (ou banco de dados) são conjuntos estruturados de dados, estabelecidos em vários locais, com suporte físico ou eletrônico, conforme redação do art. 5º, IV.

A Lei n. 12.414/2011 também traz uma definição para banco de dados como sendo "conjunto de dados relativo à pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro". A definição da LGPD acaba sendo propositadamente mais genérica por ter como objetivo abranger todos os tipos de bases de dados pessoais e não excluir do regime protetivo aquelas que são estruturadas em meio físico ou utilizadas para as finalidades mais diversas.

Ambas as definições legais, contudo, permitem concluir que as bases de dados são conjuntos estruturados de informações. Pressupõe-se que existe um esforço positivo do agente em criar e organizar esses conteúdos de acordo com uma metodologia e um sistema, físico ou eletrônico, que atenda a seus interesses. O processo de organização da base de dados e sua composição podem ser por vezes elementos diferenciais para uma atividade, seja por causa do processo criativo envolvido naquilo que será *input* para as operações de tratamento; seja por causa do próprio conteúdo que, em conjunto, adquire muito mais valor[311].

Pensando nessas características específicas, na União Europeia, a Diretiva 9/96/EC em 1996[312] afastou a tutela dos segredos de negócio às bases de dados e lhes

[311] Pode-se entender que as bases de dados compõem o aviamento da empresa, especialmente quando se pensa que seu diferencial é incorpóreo e se caracteriza pelo sistema de organização das informações e dados, e não necessariamente do conteúdo que é administrado. O aviamento compõe o estabelecimento comercial, sendo "resultado de organização e particularmente como a cristalização da atividade organizadora da coesão dos diversos elementos componentes do estabelecimento" (FERREIRA, Waldemar. *Tratado de Direito Comercial*. O estatuto do estabelecimento e a empresa mercantil. vol. 7. Editora Saraiva: São Paulo, 1962. p. 217). A organização é apenas um dos componentes do aviamento, e em mercados digitais, as bases de dados são a expressão dessa organização, sendo diferenciais para cada atividade.

[312] A Diretiva está em processo de reforma legislativa e atualização, especialmente para considerar questões específicas mais detalhadas em relação à economia digital e ao uso de bases de dados em inteligências artificiais. Sobre o tema, ver: "The European Commission is about to unveil its Data Act proposal that will also amend the Database Directive. It should also create elaborate (business to business (B2B) and business to government (B2G) access and data-sharing regimes. The goal is to unlock the potential of data for its re-use in the data economy and for artificial intelligence. According to the leaked materials, the European Commission intends to exclude from scope some machine generated-data to allow their free re-use.27 While this step tries to address some of the competition concerns in the digital economy, on its own, it is unlikely to solve broader problems of the sui generis protection. In fact, machine-generated data is a perfect example showing that the intended effects, that is to allow re-usability of such data, can only be achieved by at the same time addressing other remaining problems, namely of pre-emption and standard of protection. While the CV-Online judgment addresses some of the long-standing concerns (competition and

conferiu uma tutela jurídica *sui generis*, a qual considera sua relevância comercial e protege os esforços dos agentes econômicos que as constituíram[313]. A Diretiva inclui as bases de dados[314], mas não se limita a elas, e tem por objetivo principal criar parâmetros mais uniformes de proteção e valorização das bases informacionais e do trabalho de

exceptions), it does not solve other issues" [A Comissão Europeia está prestes a apresentar sua proposta de Lei dos Dados que também irá alterar a Diretiva sobre Bancos de Dados. Também deverá criar regimes elaborados de acesso e compartilhamento de dados (de negócios para negócios (B2B) e de negócios para governo (B2G)). O objetivo é desbloquear o potencial dos dados para sua reutilização na economia de dados e para a inteligência artificial. De acordo com os materiais vazados, a Comissão Europeia pretende excluir do escopo alguns dados gerados por máquina para permitir sua reutilização gratuita. Embora esse passo tente abordar algumas das preocupações de concorrência na economia digital, por si só, é improvável que resolva problemas mais amplos da proteção sui generis. Na verdade, os dados gerados por máquina são um exemplo perfeito que mostra que os efeitos pretendidos, ou seja, permitir a reutilização desses dados, só podem ser alcançados ao mesmo tempo em que se abordam outros problemas remanescentes, ou seja, de preempção e padrão de proteção. Embora a decisão CV-Online aborde algumas das preocupações de longa data (concorrência e exceções), ela não resolve outros problemas] (DERCLAYE, Estelle; HUSOVEC, Martin. Sui Generis Database Protection 2.0: Judicial and Legislative Reforms. *European Intellectual Property Review (EIPR)* – Forthcoming, november 16, 2021. p. 7. Disponível em: http://dx.doi.org/10.2139/ssrn.3964943. Acesso em: 10 fev. 2024). Também são pertinentes as considerações de Matthias Leistner, pois a proteção *sui generis* das bases de dados pode aumentar custos de transação e dificultar direitos como o da portabilidade e o de compartilhamento dos dados. Também por esse motivo, a Diretiva vem sendo revisada, com o propósito central de se adequar à realidade do atual mercado de dados (LEISTNER, Matthias. The existing European IP rights system and the data economy – An overview with particular focus on data access and portability. *In*: German Federal Ministry of Justice and Consumer Protection | Max Planck Institute for Innovation and Competition (eds.). *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos. 2021. p. 228).

[313] Cf. Directiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996 relativa à protecção jurídica das bases de dados. *Jornal Oficial das Comunidades Europeias*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31996L0009. Acesso em: 10 fev. 2024.

[314] Diz a Diretiva: Considerando 17: "Considerando que o termo «base de dados» deverá ser entendido como incluindo quaisquer recolhas de obras literárias, artísticas, musicais ou outras, ou quaisquer outros materiais como textos, sons, imagens, números, factos e dados; que se deverá tratar de recolhas de obras, dados ou outros elementos independentes, ordenados de modo sistemático ou metódico e individualmente acessíveis; que daí decorre que a fixação de uma obra audiovisual, cinematográfica, literária ou musical, como tal, não é abrangida pelo âmbito de aplicação da presente directiva". Cf. Directiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996 relativa à protecção jurídica das bases de dados. *Jornal Oficial das Comunidades Europeias*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31996L0009. Acesso em: 10 fev. 2024.

autoria[315], estruturando um regime normativo que tente coibir a sua exploração indevida por concorrentes ou terceiros[316].

Pela disposição legal, fica claro que o bem jurídico tutelado não é o conteúdo das bases em si, mas sim os esforços e o empenho do agente em organizar e estruturar aquelas informações. Também é estabelecida uma limitação temporal para essa proteção das bases de dados, mas sem que exista a obrigação do agente de abrir o seu conteúdo e sua metodologia de organização para autoridades ou para terceiros, ao menos em um primeiro momento. Os direitos assegurados envolvem a proteção e a exclusividade sobre o método de organização desenvolvido pelo agente. E direitos sociais se conciliam por meio de limitações da proteção *sui generis*, diante de conflitos que venham surgir com eventual interesse público ou com o cumprimento de outros deveres[317].

---

[315] Note-se que a redação da Diretiva, nesse ponto, mostra que não há diferenciação da natureza de investimento, podendo ele ser qualitativo ou quantitativo. Sobre o assunto, ver: "The database right arises if the investment is substantial.68 The "substantial" requirement can be qualitative and/or quantitative.69 "Investment" can be financial or professional and refers to any type of investment, whether in terms of human, technical and financial resources, or expending time, effort and energy.70 The substantial investment can be in obtaining, verifying or presenting the content. "Obtaining" refers to collecting data, "verifying" relates to checking and updating the database, and "presenting" refers to communicating the data, and can involve for instance designing the user interface" [O direito de banco de dados surge se o investimento for substancial. O requisito de substancialidade pode ser qualitativo e/ou quantitativo. "Investimento" pode ser financeiro ou profissional e se refere a qualquer tipo de investimento, seja em termos de recursos humanos, técnicos e financeiros, ou despesas de tempo, esforço e energia. O investimento substancial pode ser na obtenção, verificação ou apresentação do conteúdo. "Obtenção" refere-se à coleta de dados, "verificação" relaciona-se à verificação e atualização do banco de dados, e "apresentação" refere-se à comunicação dos dados e pode envolver, por exemplo, o design da interface do usuário] (BANTERLE, Francesco. 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. *In*: BAKHOUM, Mor; CONDE GALLEGO, Beatriz; MACKENRODT, Mark-Oliver M.; SURBLYTĖ-NAMAVIČIENĖ, Gintaré (eds.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law*: Towards a Holistic Approach? Springer: Berlin, 2018. p. 14, tradução livre).

[316] Considerando 39: "Considerando que, para além da protecção pelo direito de autor da originalidade da selecção ou disposição do conteúdo da base de dados, a presente directiva pretende salvaguardar a posição dos fabricantes de bases de dados relativamente à apropriação abusiva dos resultados do investimento financeiro e profissional realizado para obter e coligir o conteúdo, protegendo o conjunto ou partes substanciais da base de dados de certos actos cometidos pelo utilizador ou por um concorrente".
Considerando 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".
Considerando 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 o risco de efectuar os investimentos; que isso exclui da noção de fabricante nomeadamente os subempreiteiros". Cf. Directiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996 relativa à protecção jurídica das bases de dados. *Jornal Oficial das Comunidades Europeias*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31996L0009. Acesso em: 10 fev. 2024.

[317] BANTERLE, Francesco. 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. *In*: BAKHOUM, Mor; CONDE GALLEGO, Beatriz; MACKENRODT, Mark-Oliver M.;

No Brasil, o enquadramento jurídico acaba ficando a critério do agente. Nesse sentido, existe previsão legal específica (art. 7º, XIII, da Lei N. 9.610/98) para que bases de dados sejam tratadas dentro do regime de direitos autorais, assumindo então garantias de uma exploração comercial exclusiva, desde que providas de originalidade[318]. Se enquadradas como segredos de negócio, uma mesma metodologia de organização da informação pode acabar sendo desenvolvida por outro agente econômico, através de engenharia reversa ou pesquisas próprias. Por outro lado, o agente pode proteger suas bases de dados em níveis maiores de sigilo e sem limitação temporal expressa[319].

No mercado de dados, a opção dos agentes tende a ser a de prestigiar os maiores níveis possíveis de sigilo sobre os aspectos que envolvem suas operações. Pode-se defender que é uma escolha estratégica, que envolve uma análise sobre custos e burocracia e que tem por objetivo manter a discrição máxima sobre as informações que lhes garantem posições de vantagem no mercado[320]. Mas também pode ser uma escolha política, pois os agentes não querem ser compelidos a disponibilizar informações que denunciem a forma como eles exercem o poder que lhes é franqueado pelos dados e pelos algoritmos[321].

Por essa segunda lógica, enquadrar bases de dados como segredos de negócio é então ainda mais vantajoso, uma vez que os agentes conseguem se utilizar de uma categoria jurídica para obstar o acesso dos titulares e das autoridades aos dados pessoais e às explicações sobre como eles são utilizados.

Sabe-se que, em diversas circunstâncias, deve-se viabilizar o acesso aos dados pessoais, seja porque existem obrigações legais nesse sentido; seja porque foram adotadas políticas de compartilhamento de informação, na tentativa de tornar mais competitivo o

---

SURBLYTĖ-NAMAVIČIENĖ, Gintaré (eds.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law*: Towards a Holistic Approach? Springer: Berlin, 2018. p. 15.

[318] COELHO, Fábio Ulhoa. Curso de direito civil: direito das coisas, direito autoral, vol. 4 [livro eletrônico]. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. pp. RB-10.6; RB-11.6.

[319] SAPPA, Cristiana. How data protection fits with the algorithmic society via two intellectual property rights – a comparative analysis. *Journal of Intellectual Property Law & Practice*, Volume 14, Issue 5, May 2019. p. 7. Disponível em: https://academic.oup.com/jiplp/article-abstract/14/5/407/5369198. Acesso em: 19 fev. 2024.

[320] LICHTMAN, Douglas. Property Rights in Emerging Platform Technologies. *The Journal of Legal Studies*, v. 29, n. 2. p. 615–648, 2000. p. 634. Disponível em: https://www.jstor.org/stable/10.1086/468087. Acesso em: 19 fev. 2024. O autor menciona, inclusive, que segredos de negócio, por não assegurarem direitos de exclusividade, fazem com que o desenvolvimento tecnológico se torne mais complexo do que ele precisa ser, a fim de dificultar processos de engenharia reversa e assegurar ainda mais privacidade sobre as criações.

[321] TIMCKE, Scott. *Algorithms and the end of politics*: how technology shapes 21st-century American life. Bristol: Bristol University Press, 2021. p. 21.

mercado[322]. Independente da circunstância, esse processo compreende complexas questões de natureza operacional, que dizem respeito à interoperabilidade e à forma como o conteúdo será disponibilizado[323]. Sem clareza sobre como se resolvem esses problemas, é simples para os agentes afirmarem que, ao franquear acesso aos dados pessoais, poder-se-á denunciar metodologias de organização dos conteúdos e bases de dados que são protegidas pelos segredos de negócio.

A consequência direta é que se tratam bases de dados como segredos de negócio, os agentes podem acabar conseguindo se eximir da obrigação de disponibilizarem o conteúdo e as explicações sobre as operações, ao argumento de que, ao fazê-lo, informações sigilosas poderão ser divulgadas[324]. Valendo-se da tutela jurídica dos segredos de negócio, os agentes podem ter uma maneira de obstar o acesso de terceiros às metodologias e estruturas de organização dos dados pessoais que utilizam em suas atividades.

Casos paradigmáticos elucidam que esse comportamento é adotado na indústria. Julgado pelo Superior Tribunal de Justiça (STJ), informações sobre as metodologias de organização das informações utilizadas na formação de risco de crédito são segredos de negócio e, por isso, não precisam ser fornecidas aos consumidores. Valendo-se de terminologia genérica, a retórica dos agentes de tratamento foi exitosa, pois construiu um precedente que restringiu o consumidor do acesso a tudo aquilo que compunha a tomada de decisão automatizada, mas que não era dado pessoal[325]. Em entendimento sumulado, o consumidor só precisa ter acesso e consentir quanto aos dados pessoais coletados e as

---

[322] Um exemplo interessante é a política de *open finance* no Brasil: desde que autorizado pelo titular, seus dados poderiam integrar uma rede de informação livre entre aqueles agentes econômicos que estivessem cadastrados, compartilhando-se dados pessoais em um fluxo mais aberto para prestigiar a concorrência, a possibilidade de portabilidade e o livre mercado. Cf. Banco Central do Brasil. Open Finance. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/openfinance. Acesso em: 10 fev. 2024. No caso, não houve divulgação entre bancos das bases de dados, mas sim compartilhamento de dados para agentes econômicos específicos, a partir de uma autorização prévia do consumidor, com objetivo de melhorar condições de concorrência no mercado. A partir dos dados compartilhados, cada agente irá se apropriar dos dados que lhes interessam e organizá-los da forma diferencial que faz sentido para suas atividades, retomando o fato de que é o processo criativo e organizacional que torna as bases de dados um projeto autoral, e não o conteúdo dela em si.

[323] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 46.

[324] VAROSANEC, Ida. Silence is golden, or is it? Trade secrets versus transparency in ai systems. *The Digital Constitutionalist*. 2022. Disponível em: https://digi-con.org/silence-is-golden-or-is-it/ Acesso em: 09 mar. 2024.

[325] "De um lado, a metodologia em si de cálculo da nota de risco de crédito ("credit scoring") constitui segredo da atividade empresarial, cujas fórmulas matemáticas e modelos estatísticos naturalmente não precisam ser divulgadas". Cf. REsp 1.419.697, j. 12.11.2014, rel. Min. Paulo de Tarso Sanseverino. Trecho do voto. p. 35. Acesso em: 15 fev. 2024.

fontes de onde foram extraídos[326], como se essas fossem informações suficientes para compreender como é feito o cálculo do *score* de crédito de um consumidor.

Até mesmo no modelo europeu, que possui uma proteção específica para as bases de dados, é frequente que agentes de tratamento explorem uma sobreposição de regimes jurídicos, na medida em que, mesmo diante da proteção *sui generis*, tentam também alocar as bases como segredos de negócio, a fim de gozarem de um modelo mais benéfico e menos regulado[327]. Por isso, inclusive, a Diretiva está em processo de alteração, a fim de tentar se adequar à realidade do mercado de dados pessoais.

Deve-se destacar que se fossem tratados somente como direitos autorais, haveria, ao menos, maior clareza sobre como as informações são organizadas e qual impacto isso pode ter para os resultados produzidos. Contudo, enquadrar bases de dados como segredos de negócio afasta a materialização da transparência e fornece uma alternativa retórica para os agentes de tratamento, que os possibilita criar um óbice adicional ao acesso sobre como os dados pessoais são explorados comercialmente.

A reflexão aqui é compreender que a eleição pelo enquadramento das bases de dados como segredos de negócio é uma decisão política, fruto de possibilidades asseguradas pelo Direito que acabam por proteger os interesses dos agentes de tratamento.

Deve-se considerar que o mercado de dados traz sofisticações próprias que precisam ser consideradas, sob o risco de se conferir aos agentes de tratamento a possibilidade de criarem dificuldades para o acesso aos dados. Por causa disso, ainda que seja possível, o tratamento das bases como segredos de negócio pode não ser ideal ao objetivo de proteção de dados pessoais.

Nesse sentido, pode ser o caso de limitar a possibilidade de escolha do agente, a fim de que se prestigiem tutelas jurídicas mais transparentes, como a dos direitos autorais. Outra possibilidade seria pensar uma categoria jurídica própria para preservar o sigilo e os interesses dos agentes econômicos quanto ao modelo de organização do conteúdo, ao mesmo tempo em que se assegura a transparência necessária para garantir a autodeterminação informativa e o controle de poder.

---

[326] Em sentido similar, cabe destacar a Súmula 550 do STJ: "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo".

[327] Há, inclusive, significativa discussão sobre como a proteção aos segredos de negócio se sobrepõe ao regime jurídico específico das bases de dados. Sobre a questão, ver: OCAÑA, Teresa Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020. p. 77-86.

A preocupação deve ser no sentido de evitar que os segredos de negócio sejam utilizados como um instrumento que, genérico e não desenhado especificamente para uma realidade complexa, possa ser invocado para obstar a materialização da transparência.

II.3.2 A possibilidade de enquadrar os dados pessoais como segredos de negócio

Se as reflexões sobre as bases de dados são complexas, a forma como podem ser tratados os dados pessoais não é mais simples.

Enquadrar dados em geral como segredos de negócio não é uma discussão nova, pois, em variados mercados, eles podem ser o elemento primordial para o desenvolvimento da atividade econômica. Informações armazenadas como dados, como números sobre lucros e rendimentos, informações sobre estratégias, projetos e tantos outros, são exemplos nesse sentido[328].

Apesar de serem desdobramentos da personalidade, dados pessoais igualmente já são tratados como segredos de negócio em outros contextos[329], notadamente quando dizem respeito a informações sobre pessoas físicas que compõem a estrutura empresarial. É o caso de listas de clientes, das informações sobre fornecedores e dos salários de empregados.

Ainda que sejam dados pessoais, tornou-se comum associá-los a segredos de negócio por serem conteúdos que, mesmo se relacionando a uma pessoa natural, são uma consequência do exercício da atividade empresarial. Outro motivo é que, se indevidamente divulgados para os concorrentes, os dados pessoais podem criar impactos concorrenciais e distorções características da concorrência desleal[330]. Assim, para

---

[328] Um exemplo diferente sobre o tema diz respeito à agricultura, especialmente diante do que vem se chamando agricultura 4.0. Sofisticados equipamentos de georreferenciamento e pesquisas envolvendo nanotecnologia vêm permitindo aprimorar o conhecimento sobre o solo, sementes e produtos importantes para o desenvolvimento da agricultura. E os segredos de negócio por vezes são invocados para proteger os dados coletados e os resultados obtidos através dessas pesquisas, buscando-se formas de regular a transferência e a divulgação dessas informações e ainda assim preservar os interesses de certa exclusividade na exploração desse conteúdo. Sobre o tema, ver: RADAUER, Alfred; SEARLE, Nicola; BADER, Martin A. The possibilities and limits of trade secrets to protect data shared between firms in agricultural and food sectors. *World Patent Information*, Volume 73, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S0172219023000133. Acesso em: 28 fev. 2024.

[329] BANTERLE, Francesco. 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. *In*: BAKHOUM, Mor; CONDE GALLEGO, Beatriz; MACKENRODT, Mark-Oliver M.; SURBLYTĖ-NAMAVIČIENĖ, Gintaré (eds.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law*: Towards a Holistic Approach? Springer: Berlin, 2018. p. 8.

[330] Tais informações são consideradas concorrencialmente sensíveis por diversas autoridades de defesa da concorrência ao redor do mundo, justamente porque podem facilitar e viabilizar ocorrência de cartéis, ou mesmo configurar um tipo de ilícito concorrencial autônomo. Isso reforça seu enquadramento como

atividades tradicionais e para uma realidade não movida a dados, as discussões sobre dados pessoais serem tratados como segredos de negócio não se mostram tão complexas.

A questão é diferente quando transportada para o mercado específico dos dados pessoais. Nele, as informações não são coletadas apenas em razão do desenvolvimento da atividade comercial; são também coletadas com insumo para a atividade, que pode ser a venda de dados em si, a venda de produtos, propagandas, anúncios, perfis, e outros, a partir do conhecimento angariado dos dados pessoais.

A fim de não denunciar a ostensividade com a qual os dados são coletados e utilizados, os agentes de tratamento tentam enquadrá-los como segredos de negócio.

A questão é preocupante quando se pensa no volume de dados coletados e na sua íntima relação com a subjetividade dos indivíduos. Viu-se que dados fornecem um grande poder aos agentes de tratamento, de modo que seu enquadramento como segredo pode aumentar esse poder a ponto de torná-lo incontrolável.

Nesse contexto, alguns autores defendem que dados pessoais coletados e explorados não poderiam então ser tratados como segredos de negócio. Os argumentos principais orbitam entre: (i) serem conteúdos de titularidade de um terceiro e não do agente de tratamento[331]; e (ii) em uma perspectiva mais mercadológica, serem de ampla disponibilidade entre concorrentes, com baixo valor agregado quando analisados isoladamente[332][333].

---

segredos de negócio na medida em que seu uso indevido pode trazer repercussões concorrenciais. Ver: GALVÃO, Luiz Antonio. *Troca indireta de informações entre concorrentes*: os limites do ilícito concorrencial. Dissertação de Mestrado. Universidade de São Paulo. Programa de Pós-Graduação em Direito. São Paulo, 2018. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2132/tde-17092020-170014/publico/6487512_Dissertacao_Parcial.pdf. Acesso em: 18 fev. 2024; e OECD. Policy Roundtables. Information Exchanges Between Competitors under Competition Law. *OECD*. 2010. Disponível em: https://www.oecd.org/daf/competition/48379006.pdf. Acesso em: 18 fev. 2024.

[331] Nesse sentido, até argumentam que a proteção dos segredos poderia ser estendida apenas às bases de dados, porque dizem sobre a forma como o conteúdo se organiza e é utilizado, mas não ao conteúdo em si. Ver: MILLER, Megan Marie. Data as the New Oil: A Slippery Slope of Trade Secret Implications Greased by the California Consumer Privacy Act. *Cybaris*®: Vol. 12: Iss. 1, Article 1, 2021. p. 22. Disponível em: https://open.mitchellhamline.edu/cybaris/vol12/iss1/1/. Acesso em: 08 fev. 2024.
Disponível em: https://open.mitchellhamline.edu/cybaris/vol12/iss1/1. Acesso em: 8 fev. 2024.

[332] APLIN, Tanya; RADAUER, Alfred; BADER, Martin A.; SEARLE, Nicola. The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis. *National Library of Medicine*. 2023. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10170042/#Fn53. Acesso em: 10 fev. 2024; LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 19. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

[333] Sobre esse ponto, o argumento também se desenvolve no sentido de que políticas de democratização de acesso (open inovation) afastam qualquer pretensão de sigilo aos dados pessoais, afastando, também por essa perspectiva, o enquadramento como segredos. De fato, existem muitas políticas para horizontalização do acesso aos dados e democratização de bases amplas. Na Europa, existem vários incentivos para compartilhamento de dados, seja entre instituições públicas ou privadas. Sobre o tema, ver: EUROPEAN

Ambos os argumentos podem ser refutados sem maiores problemas. Apesar de serem de titularidade de terceiros, pode-se argumentar que são conteúdos que estão em posse dos agentes de tratamento, e cuja exploração econômica está lastreada em bases legais que legitimam as operações.

Ainda, alguns dados pessoais não possuem baixo valor agregado em sua forma isolada, tampouco se encontram em situação de ampla disponibilidade entre concorrentes. Existem diferentes tipos de dados pessoais, e essa diferença poderia acabar permitindo enquadrar alguns deles como segredos de negócio, explorando a plasticidade da categoria jurídica[334] e as opções tecnológicas que estão disponíveis para criar dados novos ou coletar informações que nem todos os agentes econômicos têm acesso[335].

A questão mais relevante para afastar o tratamento de dados pessoais como segredos de negócio é, no ordenamento brasileiro, relembrar que eles são extensão da personalidade. Autorizar enquadrá-los como segredos de negócio seria fortalecer a sua percepção de que são simples ativos do capital[336], ampliando as dimensões de datificação e colocando os indivíduos na nítida posição de produtos para o lucro das grandes empresas, as quais passam a explorá-los até mesmo de forma sigilosa.

Não só, surge uma preocupação similar ao que pode ocorrer em relação às bases de dados: o enquadramento como segredos de negócio cria a possibilidade de os agentes de tratamento obstarem o acesso dos titulares e das autoridades aos conteúdos explorados.

COMMISSION. Study On The Legal Protection Of Trade Secrets In The Context Of The Data Economy (GRO/SME/20/F/206). *European Commission.* 2022. p. 29. Disponível em: https://research.gold.ac.uk/id/eprint/32803/2/study%20on%20the%20legal%20protection%20of%20trade%20secrets%20in-EA0922449ENN.pdf. Acesso em: 08 fev. 2024.

[334] WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, n. 2, 2019. p. 117-119. Disponível em: https://ssrn.com/abstract=3248829. Acesso em: 6 abr. 2024. Os autores, inclusive, mencionam diversos tipos de dados pessoais que, em contextos de processos judiciais em países da União Europeia, já foram considerados como segredos de negócio.

[335] Um exemplo interessante envolve os estudos que vêm sendo conduzidos sobre *mouse-tracking*: são coletadas cada vez mais informações sobre o cursor do mouse, os principais locais da tela em que ocorrem os clicks, quanto tempo demora para cada click ocorrer, quais os principais movimentos dos usuários em determinadas páginas, dentre outras informações que, segundo especialistas, podem se relacionar com comportamentos individuais, padrões de interesse, dentre outros. Esse é um tipo de dado comportamental que determinadas empresas se empenham para coletar, representando significativa sofisticação tecnológica e criatividade no processo de datificação da experiência humana. Sobre o tema, ver: KIESLICH, Pascal J.; HENNINGERA, Felix; WULFF, Dirk U.; HASLBECKE, Jonas M. B.; SCHULTE-MECKLENBECK, Michael. (in press). Mouse-tracking: A practical guide to implementation and analysis. *In*: SCHULTE-MECKLENBECK, Michael; KÜHBERGER, Anton; JOHNSON, Joseph G. (eds.). *A Handbook of Process Tracing Methods*. New York, NY: Routledge, 2019.

[336] "No âmbito da economia digital, a informação pessoal representa um ativo incorpóreo importante na criação de valor, bem como uma moeda de troca para os serviços on line" (AUTORIDADE Europeia para a Proteção de Dados. *Jornal Oficial da União Europeia*. 2014. Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_ex_sum_pt_0.pdf. Acesso em: 18 fev. 2024.

Isso faria com que não só as metodologias de organização das informações sejam administradas de forma sigilosa, como também os conteúdos que são explorados comercialmente. E existem importantes exemplos de situações nas quais isso ocorreu, tendo grandes agentes de tratamento empenhado significativos esforços para dificultar e obstar o acesso integral dos titulares aos dados pessoais[337].

A situação absurda pode fazer com que agentes de tratamento consigam tratar dados pessoais dos titulares sem que eles venham a ter acesso a esse conteúdo, mas ainda sejam impactados pelos resultados que são por ele produzidos. Viola-se, por essa perspectiva, até mesmo instrumentos constitucionais, como o do *habeas data*, que assegura o acesso aos dados pessoais que são coletados sobre um indivíduo.

Não quer dizer que todos os agentes, em todas as circunstâncias, vão se recusar a assegurar o acesso aos dados pessoais valendo-se dos segredos de negócio. Quer dizer que o direito do titular pode estar condicionado a uma vontade do agente, de garantir ou não o acesso, já que ele passa a ter a possibilidade de se recusar a fazê-lo. Por isso, a possibilidade de legitimar essa escolha por meio do Direito deve ser coibida, pois uma categoria jurídica não pode criar distorções que se sobrepõem às garantias de direitos fundamentais.

Os segredos acabam se mostrando como uma categoria jurídica inadequada para enquadrar dados pessoais, em razão da ampla dimensão existencial que esses conteúdos têm. Isso quer dizer que, ainda que seja possível tratar dados pessoais no mercado em questão como segredos de negócio, esse enquadramento jurídico deve ser afastado, a fim de reforçar a dimensão existencial que existe no conteúdo. Sendo dimensões da personalidade, o livre acesso aos dados deve ser assegurado em todas as circunstâncias, e tratá-los como segredos, ainda que seja possível discutir o alcance desses segredos, pode acabar prejudicando essa necessária transparência.

Assim, ainda que tenham valor comercial expressivo, conferindo vantagens para os agentes ou sendo determinantes para a prestação de um serviço[338], dados pessoais sempre vão ser informações privadas, com desdobramento existencial e forte impacto na

---

[337] O'BRIEN, Kevin J. Austrian Law Student Faces Down Facebook. *The New York Times*. 2012. Disponível em: https://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html. Acesso em: 02 maio 2024; MALGIERI, Gianclaudio. Trade Secrets v Personal Data: A Possible Solution for Balancing Rights. *International Data Privacy Law*, Volume 6, Issue 2. p. 102-116, maio de 2016. Disponível em: https://ssrn.com/abstract=3002685. Acesso em: 02 maio 2024.

[338] SAPPA, Cristiana. How data protection fits with the algorithmic society via two intellectual property rights – a comparative analysis. *Journal of Intellectual Property Law & Practice*, Volume 14, Issue 5, May 2019. p. 8. Disponível em: https://academic.oup.com/jiplp/article-abstract/14/5/407/5369198. Acesso em: 19 fev. 2024.

conformação da subjetividade humana. Seu enquadramento jurídico como segredo de negócio não pode desconsiderar a dimensão de personalidade, que impõe garantias amplas de acesso por parte de seus titulares.

II.3.3 Os códigos e elementos de composição da estrutura algorítmica

Os algoritmos, como já mencionado, são estruturas de linguagem matemática, que possuem por propósito desempenhar uma tarefa a partir dos desejos e intenções de seu programador. O enquadramento desse tipo de conteúdo como segredo de negócio é comum[339] e frequentemente tratado como uma questão pacífica: os códigos representam diferenciais para as atividades de cada agente, possuem significativo valor agregado e trazem vantagens competitivas que, se indevidamente exploradas por terceiros, podem criar impactos concorrenciais[340].

---

[339] Essas conclusões não são novas: em 2015, Frank Pasquale já falava que algoritmos inseridos dentro do mercado de tratamento de dados pessoais são considerados segredos de negócio. PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 193. Outros autores também tratam da questão como sendo pacífica, até mesmo com o objetivo de analisar os impactos desse enquadramento para o sistema de proteção de dados. É o caso de TIMCKE, Scott. *Algorithms and the end of politics*: How Technology Shapes 21st-Century American Life. Bristol University Press, 2021; COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019; BUCHER, Taina. *If...Then*: Algorithmic power and politics. Oxford University Press, 2018.

[340] Sobre a relevância dos algoritmos e seu diferencial nos mercados: "As seen above, in the digital economy, algorithms serve to give sense to (big) data and to infer pieces information from them – pieces of information that, in turn, find manifold profitable usages. For example, they can work to improve firms' decision-making processes and strategies; they can be employed to design customized products or services strengthening the bindings with consumers; or they can be offered to the market as recommendations, search results, rankings, or reviews. Thus, without neglecting the role of raw data, a good share of the competitive advantages that some data companies hold is due to their algorithms' ability to analyze and elaborate data as so to produce innovation. Not by chance, the supporters of the open data movement believe that firms would keep on competing even in a world where all the raw data available were put in common, just because any firm would still use its own algorithms and thus rely on them (and on the added value that they produce) to overcome and defeat rivals" [Como visto acima, na economia digital, os algoritmos servem para dar sentido aos (grandes) dados e inferir informações a partir deles - informações que, por sua vez, encontram múltiplos usos lucrativos. Por exemplo, eles podem trabalhar para melhorar os processos de tomada de decisão e estratégias das empresas; podem ser empregados para projetar produtos ou serviços personalizados, fortalecendo os vínculos com os consumidores; ou podem ser oferecidos ao mercado como recomendações, resultados de busca, classificações ou análises. Assim, sem negligenciar o papel dos dados brutos, uma boa parte das vantagens competitivas que algumas empresas de dados possuem se deve à capacidade de seus algoritmos de analisar e elaborar dados para produzir inovação. Não por acaso, os defensores do movimento de dados abertos acreditam que as empresas continuariam competindo mesmo em um mundo onde todos os dados brutos disponíveis fossem colocados em comum, simplesmente porque cada empresa ainda usaria seus próprios algoritmos e, portanto, confiaria neles (e no valor agregado que produzem) para superar e derrotar os concorrentes] (MAGIOLINO, Mariateresa. EU Trade Secret Law and Algorithmic Transparency. *Bocconi Legal Studies Research Paper* No. 3363178, 2019. p. 8-9, tradução livre. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363178. Acesso em: 04 abr. 2024).

Cada código pode ser desenhado de inúmeras maneiras, a partir de linguagens, modelos e propósitos que são definidos inicialmente por quem os desenvolve[341]. A gama de escolhas no *design* algorítmico é tamanha que, como já dito, os desenvolvedores acabam sendo verdadeiros atores políticos, pois são responsáveis por estruturarem uma ferramenta que possui impacto significativo no cotidiano humano, em diversos aspectos[342].

Programas compostos por códigos e algoritmos também poderiam ser protegidos pela propriedade intelectual e registrados em condições de sigilo, nos termos do art. 3º, III, parágrafo 2º, da Lei n. 9.609/98 e pelo art. 10.1 do TRIPS. É possível, inclusive, que estruturas maiores sejam patenteadas, como os códigos menores ou elementos matemáticos mais específicos sejam tratados como segredos de negócio[343][344].

Algoritmos em específico, podem ser inclusive tidos como simples métodos de resolução de operação e estruturas de linguagem puramente matemática que não demandam qualquer tutela jurídica. Como destacam Tauk e Cueva a partir de conclusões do Instituto Max Planck para Inovação e Concorrência, algoritmos podem ser vistos como problemas abstratos, ideiais gerais e modelos de negócio que não estão inseridos na

---

[341] MAGIOLINO, *op. cit*., p. 5.

[342] GREEN, Ben. Data Science as Political Action: Grounding Data Science in a Politics of Justice. *Journal of Social Computing*, vol. 2, no. 3, 2021. Disponível em: https://doi.org/10.23919/JSC.2021.0029. Acesso em: 29 mar. 2023.

[343] PASQUALE, Frank. The troubling consequences of trade secret protection of search engine rankings. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 386-287. A questão também pode ser diferenciada pelo objeto do que é patenteado e do que é segredo de negócio. Como analisou Denis Borges Barbosa, o sistema de patente, no âmbito dos *softwares*, protege "soluções técnicas construídas através de programas de computador, soluções essas que se voltam a problemas técnicos" (p. 1849). Os elementos do *software* podem ser protegidos por várias outras perspectivas. Novamente citando o professor Denis: "ele ainda poderá ser objeto de registro de desenho industrial, quanto a seus aspectos ornamentais, de modelo de utilidade quanto a aspectos meramente construtivos de menor inventividade, de direito autoral sobre texto ou imagem nele inclusa, etc." (p. 1856). BARBOSA, Denis Borges. Tratado da Propriedade Intelectual: Tomo III. 2. ed. Rio de Janeiro: Lumen Juris, 2017. Em outros países, é importante dizer, pode-se dizer que a possibilidade de patenteamento de *softwares* tem se mostrado cada vez menos provável, e até as cortes acabam direcionando os agentes econômicos para que utilizem a proteção pelos segredos de negócio no lugar das patentes em relação à inovação (o que não necessariamente é positivo, tendo em vista a falta de limitações e a pouca transparência que cercam os segredos de negócio). São conclusões trazidas por RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. 2020. p. 81-87. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 24.

[344] GERALDES, João de Oliveira. Sobre a proteção jurídica dos segredos comerciais no espaço digital. *Revista da Faculdade da Universidade de Lisboa*, vol. LXIII, 1 e 2, Lisboa, 2022. p. 418. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Joa%CC%83o-de-Oliveira-Geraldes_compressed.pdf. Acesso em: 06 out. 2023. Nesse sentido, é comum pensar que os segredos de negócio e as patentes podem ser tutelas jurídicas complementares. Sobre a questão, ver: SAPPA, Cristiana. How data protection fits with the algorithmic society via two intellectual property rights – a comparative analysis. *Journal of Intellectual Property Law & Practice*, Volume 14, Issue 5, May 2019. p. 3. Disponível em: https://academic.oup.com/jiplp/article-abstract/14/5/407/5369198. Acesso em: 19 fev. 2024.

cultura jurídica[345]. Ou podem também ser interpretados como componentes de um sistema maior que, nessas circunstâncias, enseja tutela jurídica específica (inclusive de direito autoral) [346].

Contudo, os algoritmos em geral frequentemente são tratados como segredos pelos agentes de tratamento de dados pessoais. Isso porque se pretende preservar a natureza secreta dos códigos e não abrir nenhuma parte da sua estrutura para o registro[347], não se submetendo os agentes aos limites territoriais da proteção e nem às regras de países específicos que podem ser relativizadas em outros territórios[348]. Não só, argumenta-se que algoritmos são muito dinâmicos e sofrem mudanças estruturais constantes, o que dificulta os esforços para registro da propriedade intelectual até mesmo de forma parcial, em razão das burocracias envolvidas e da dificuldade que seria demandada para que o registro se mantivesse atualizado[349]. Ou seja, há uma escolha política dos agentes de tratamento em considerar os códigos matemáticos como segredos de negócio.

Contudo, essa escolha deveria considerar a sofisticação do mercado de dados e o impacto que as estruturas algorítmicas podem ter na decisão automatizada. Sabe-se que os códigos transportam vieses e intensões[350] e que seu protagonismo e impacto no mercado é tão grande que se discute a necessidade de os desenvolvedores desses códigos serem tratados como atores políticos[351].

---

[345] TAUK, Caroline Somesom; CUEVA, Ricardo Villas Bôas. Propriedade intelectual, segredo do negócio e transparência: a proteção do código-fonte, do algoritmo e do banco de dados. In: CUEVA, Ricardo Villas Bôas ... [et al.]. *Direitos fundamentais e novas tecnologias*: homenagem ao professor Danilo Doneda. 1ª ed. Rio de janeiro: GZ, 2024. p. 103 ; DREXL, Josef; HILTY, Reto M. *et al.* Data Ownership and Access to Data. Position Statement on the Current European Debate. *Max Planck Institute for Innovation and Competition*, 16 August 2016. pp. 4 e 5.

[346] SCHIRRU, Luca. *Direito autoral e inteligência artificial:* autoria e titularidade nos produtos da IA. Orientador: Allan Rocha de Souza. Tese (doutorado) – UFRJ, 2020. p. 135.

[347] Destaca-se que o registro do programa junto ao Instituto Nacional da Propriedade Industrial (INPI) é facultativo, a teor dos arts. 2º e 3º, da lei n. 9.609/98. E mesmo registrado, não há obrigatoriedade de publicizar o código-fonte. Sobre a questão: TAUK, Caroline Somesom; CUEVA, Ricardo Villas Bôas. Propriedade intelectual, segredo do negócio e transparência: a proteção do código-fonte, do algoritmo e do banco de dados. In: CUEVA, Ricardo Villas Bôas ... [et al.]. *Direitos fundamentais e novas tecnologias*: homenagem ao professor Danilo Doneda. 1ª ed. Rio de janeiro: GZ, 2024. p. 100.

[348] GERALDES, João de Oliveira. Sobre a proteção jurídica dos segredos comerciais no espaço digital. *Revista da Faculdade da Universidade de Lisboa*, vol. LXIII, 1 e 2, Lisboa, 2022. p. 418. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Joa%CC%83o-de-Oliveira-Geraldes_compressed.pdf. Acesso em: 06 out. 2023.

[349] JAMAR, Steven D. Trade Secrets from an IP Social Justice Perspective (November 16, 2021). Trade Secrets from an IP Social Justice Perspective, in Cambridge Handbook on IP-SJ (Steven D. Jamar & Lateef Mtima editors (forthcoming Cambridge University Press 2022). *Howard Law Research Paper*. p. 8. Disponível em: http://dx.doi.org/10.2139/ssrn.3964977. Acesso em: 19 fev. 2024.

[350] O tema foi amplamente explorado por O'NEIL, Cathy. *Weapons of math destruction*. How big data increases inequality and threatens democracy. New York: Crown Publishers, 2016.

[351] GREEN, Ben. Data Science as Political Action: Grounding Data Science in a Politics of Justice. *Journal of Social Computing*, vol. 2, no. 3, 2021. Disponível em: https://doi.org/10.23919/JSC.2021.0029. Acesso em: 29 mar. 2023.

Não se pode desconsiderar também que estruturas algorítmicas estão inseridas em espaços importantes, substituindo a ação humana em tomadas de decisões cujos impactos são imediatos na vida da população. Nesses cenários, os códigos deveriam ser passíveis de fácil auditoria e fiscalização, a fim de se garantir *accountability* e se administrar os impactos por ela causada.

Essas reflexões mostram que existem dificuldades em conferir sigilo a estruturas matemáticas que podem ser tão determinantes em processos políticos, sociais e culturais. Ainda que seja possível, os códigos matemáticos deveriam ser protegidos pelo Direito através de categorias jurídicas mais transparentes (como registro pela Lei de Propriedade Intelectual), a fim de viabilizar mecanismos de controle sobre os impactos que essas estruturas podem ter na coletividade.

A questão se complexifica ao pensar que o mercado de dados pessoais, contudo, não pode ser reduzido a algoritmos. Conforme mencionado anteriormente, a sofisticação da produção de resultados a partir de análises preditivas faz com que a tecnologia transcenda aspectos essencialmente ligados aos códigos matemáticos e passe a sofrer interferência também de outros fatores que compõem os complexos e interligados sistemas de tratamento de dados[352].

Elementos laterais aos algoritmos são parte significativa do funcionamento das estruturas e compõem a formação do resultado e interferem no tratamento de dados de forma muitas vezes impossível de dimensionar[353]. É o caso, por exemplo das metodologias e dos critérios utilizados para treinar algoritmos e selecionar dados[354].

Sendo relevantes para a produção do resultado, defende-se que também esses aspectos dos sistemas de tratamento devem ser abordados como segredos de negócio[355].

---

[352] Cabe mencionar: "with the flourishing of firms collecting big data, the word "algorithm" has acquired a more specific – to some extent, narrower – nuance. It does not indicate any mathematical construct that describes the operations to follow to achieve a given objective. It refers to how the said orders and commands are practically implemented and combined into a particular program, software, or information system,15 with the ultimate goal of inferring from data the answers to be given to a specific set of questions" [Com o florescimento de empresas que coletam grandes volumes de dados, a palavra "algoritmo" adquiriu uma nuance mais específica - até certo ponto, mais restrita. Não indica mais qualquer construção matemática que descreve as operações a serem seguidas para alcançar um determinado objetivo. Refere-se a como as ordens e comandos são praticamente implementados e combinados em um programa específico, software ou sistema de informação, com o objetivo final de inferir a partir dos dados as respostas a serem dadas a um conjunto específico de perguntas] (MAGIOLINO, Mariateresa. EU Trade Secret Law and Algorithmic Transparency. *Bocconi Legal Studies Research Paper* No. 3363178, 2019. p. 3, tradução livre. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363178. Acesso em: 04 abr. 2024).

[353] BUCHER, Taina. *If...Then*: Algorithmic power and politics. Oxford University Press, 2018. p. 47-49.

[354] Esses dois elementos, inclusive, foram considerados segredos de negócio em importante precedente que serão detalhados adiante. Contudo, relevante já mencioná-lo: REsp n. 1.419.697/RS.

[355] MAGIOLINO, *op. cit*., p. 7.

Ou seja, o objetivo é tornar sigilosa toda a sintaxe que compõe as operações de tratamento de dados pessoais.

Esse é um entendimento que foi respaldado pela jurisprudência em diferentes circunstâncias, consolidando que critérios de análise de dados pessoais e elementos para além dos códigos matemáticos deveriam ser protegidos sob condições sigilosas e, por isso, não poderiam ser fornecidos aos consumidores, às autoridades ou a quaisquer terceiros. Casos exemplificativos envolvem o uso de algoritmos preditivos para formulação do risco de crédito[356], análises no mercado de seguros[357] e concessão de financiamentos e empréstimos financeiros[358], além de outros.

Tratar todos esses elementos como segredos de negócio parece uma conclusão óbvia sob a ótica dos agentes de tratamento, pois significa preservar as operações e evitar riscos de apropriação indevida dos elementos de tratamento de conteúdo. Mas não é uma conclusão simples pela ótica do titular, a quem o ordenamento jurídico deve buscar assegurar a proteção de direitos fundamentais, como o da privacidade e o da proteção de dados.

A autodeterminação informativa não depende apenas da ciência sobre quais dados são coletados sobre si (o que, como já exposto anteriormente, pode também ser objeto de controvérsia). Envolve também a compreensão correta sobre qual a finalidade de uso dessas informações, por quanto tempo e por quem. Dentro da expectativa de informação que o titular pode ter, entender todos os elementos que contribuem para a produção dos resultados e das decisões automatizadas se torna um aspecto muito relevante.

---

[356] Empresas de formulação de risco de crédito não costumam fornecer seus códigos ou bases de dados nem mesmo para auditorias promovidas por entes regulatórios, ao argumento de que são informações protegidas por segredos de negócio. As informações que são disponibilizadas, especialmente ao público, também não incluem detalhamento sobre como foram obtidos os dados utilizados nas análises, como são administradas as bases, qual o limite temporal de dados utilizados ou qual o nível de acurácia das informações. Nesse sentido, caso recente foi julgado pela Corte alemã sobre o tratamento de dados pessoais e o uso dos segredos de negócio para obstar o acesso à compreensão completa de como é formulado o risco de crédito. Ver: ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Primeira Secção), 7 de dezembro de 2023. InfoCuria. 2023. Disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=24E21076CD678110912F514CAF865B96?text=&docid=280426&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1302015. Acesso em: 25 maio 2024.

[357] Exemplos no mercado de seguros de saúde (GÓMEZ-GONZÁLEZ, Emilio; GÓMEZ, Emilia. *Artificial intelligence in medicine and healthcare*: Applications, availability and societal impact. Luxembourg: Publications Office of the European Union, 2020) são elucidativos de como tecnologias preditivas e inteligências artificiais podem impactar preços por meio de critérios potencialmente discriminatórios.

[358] RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. p. 61-116, 2020. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 2024. p. 92-96. A autora traz o exemplo de como o segredo que envolve os algoritmos que fazem financiamentos e concessões de benefícios de moradia são enviesados sem que esses vieses sejam mapeados adequadamente.

O tratamento de todos esses elementos técnicos como segredos de negócio também pode dificultar, e até inviabilizar, o exercício das competências da autoridade de proteção de dados. É a ANPD a responsável por garantir a efetividade da proteção de dados em um nível que o titular é verdadeiramente incapaz de fazer[359]. Por meio de análises técnicas, é a autoridade que consegue avaliar de que maneira a comunicação com o titular é feita, para então tentar resguardar os direitos individuais[360] e criar parâmetros de comunicação que vão permitir concretizar a autodeterminação informativa[361].

A autoridade ainda é responsável pela proteção de dados pessoais quando se pensa na privacidade em âmbito coletivo, conseguindo avaliar de que maneira as operações daquele agente podem criar impactos transindividuais[362]. Compete à autoridade, ainda, a

[359] Diz Danilo Doneda sobre a importância de ver a ANPD como uma autoridade de garantia para a proteção de dados pessoais: "Para a efetiva proteção dos direitos em questão na amplitude necessária, seja esta individual ou coletiva, cabe a devida consideração das características da matéria de proteção de dados pessoais a partir dos desafios específicos para a implementação de um sistema adequado de tutela. Conforme observamos, trata-se de uma seara na qual os danos de reduzidíssima monta são comuns, o que diminui a propensão para que se postule individualmente a sua reparação a partir dos institutos tradicionais de responsabilidade civil. A utilização de uma tutela baseada na responsabilidade civil não é, por si só, um instrumento que tutele na medida necessária o direito fundamental à proteção de dados pessoais, podendo inclusive vir a incentivar a consolidação de práticas de utilização indevida de dados pessoais. A ação de uma autoridade para a proteção de dados representa, portanto, instrumento necessário para a efetivação de uma garantia fundamental" (DONEDA, Danilo. A Autoridade Nacional de Proteção de Dados. *In*: DONEDA, Danilo *et. al.* (coord). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2017. p. 464).

[360] Existem interessantes paralelos entre o paradigma liberal de proteção à privacidade, que foca apenas no indivíduo como capaz de fazer a gestão da sua privacidade, com a crítica feminista, que compreende as limitações estruturais dos indivíduos em razão de regimes de poder subjacentes. Pensando na atuação da autoridade para também assegurar direitos individuais, esses paralelos ficam ainda mais fortes, pois mostram que as capacidades de manipulação dos indivíduos e todas as dimensões de influência que são vividas pelos titulares fazem com que o controle do uso dos dados não possa ser feito apenas em âmbito individual, mas primeiramente por meio de autoridades com capacidade técnica de fazê-lo. Sobre o tema, ver: BARNES, Susan B. A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 1-10, 2006. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/1394. Acesso em: 11 nov. 2023. Também se alinham com percepções sobre coletivização dos direitos de privacidade e perspectivas de constitucionalização de direitos para uma dimensão que não seja apenas individual. Ver: TEUBNER, Gunther. Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution. *Italian Law Journal*, v. 3, n. 2. p. 485–510, 2017. Disponível em: https://www.jura.uni-frankfurt.de/70299574/InternetHorizontalConstRightsENGItalJ2017.pdf?.%20. Acesso em: 12 abr. 2023.

[361] VEDDER, Adam. Privacy 3.0. *In*: GROOTHUIS, Marga; HOF, Simone van der. *Innovating Government*. The Hague: Asser Press, 2011. p. 19-20.

[362] É a proposta para que a dimensão coletiva da privacidade seja levada cada vez mais a sério. Sobre o tema, ver: KAMMOURIEH, Lenah *et al*. Group Privacy in the Age of Big Data. *In*: TAYLOR, Linnet; FLORIDI, Luciano; VAN DER SLOOT, Bart. *Group Privacy*: New Challenges of Data Technologies. Springer, 2017. p. 58.

análise das operações que não estão lastreadas na base legal do consentimento[363], a fiscalização sobre vieses e a análise de potenciais decisões discriminatórias[364].

Além do âmbito de fiscalização, a autoridade precisa ser munida de informações sobre as operações para construir regulações setoriais específicas sobre a proteção de dados. Diante da perspectiva colaborativa e descentralizada[365], é importante que haja um canal de comunicação transparente entre o agente e a autoridade[366], por meio de um amplo fluxo de informações para assegurar a construção de normas exequíveis, porém justas.

Para o exercício dessas competências, a autoridade depende fortemente de um amplo acesso às informações sobre as operações, o que inclui acesso aos elementos laterais aos códigos matemáticos que compõem o tratamento de conteúdo[367]. Até porque muitas vezes esses elementos podem ser responsáveis por discriminações algorítmicas e análises enviesadas, que somente o rigor técnico da autoridade poderá ser capaz de identificar.

Incluir todos esses elementos das operações de tratamento de dados dentro da proteção dos segredos de negócio é tratar de forma simples um problema muito complexo da tensão existente entre os deveres e as obrigações de transparência em contrapartida ao sigilo que os agentes pretendem conferir às suas operações.

É possível discutir o alcance do sigilo conferido a esses elementos, a teor do art. 206 da LPI, bem como a possibilidade de, mesmo enquadrados como segredos, serem esses conteúdos disponibilizados, quando não houver riscos concorrenciais ou quando a autoridade demandar informações para o exercício de suas funções. Mas a questão não se mostra simples de ser resolvida e casos concretos mostram que o Poder Judiciário não sabe lidar com as possibilidades de divulgação de segredos de negócio.

---

[363] É o caso das análises de crédito, conforme descrito por STINGHEN, João Rodrigo de Morais; ANDRADE, Aline Rodrigues de. *Os riscos à privacidade do novo cadastro positivo e o papel da ANDP*. Revista dos Tribunais. vol. 1025. ano 110. p. 203-223. São Paulo: Ed. RT, março 2021. p. 218-220.

[364] RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. 2020. p. 106. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 2024.

[365] BLACK, Julia. Decentering regulation: Understanding the Role of Regulation and Self-Regulation in a "Post Regulatory" World. *Current Legal Problems*, Volume 54, Issue 1, 2001, Pages 103–146, 01 December 2001. p. 140. Disponível em: https://doi.org/10.1093/clp/54.1.103. Acesso em: 08 maio 2023.

[366] Bioni corretamente pondera que um regime mais robusto de *accountability* pressupõe que o desenvolvimento de regulação envolva também outros atores da sociedade civil em um modelo mais dialógico com audiências públicas, contraditório e ampla defesa. São considerações que reforçam o aspecto colaborativo e a necessidade de um trânsito informacional amplo, em que não existam tantas limitações sobre como de fato se dão as operações de tratamento de dados pessoais (BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 126-129).

[367] MACCARTHY, Mark. New Directions In Privacy: Disclosure, Unfairness and Externalities. *I/S*: A Journal of Law and Policy for the Information Society. 425. 2011. p. 69-72. Disponível em: https://ssrn.com/abstract=3093301. Acesso em: 27 nov. 2023.

A título de exemplo, o Tribunal Superior do Trabalho concedeu tutela provisória de urgência para suspender a realização de prova pericial deferida no âmbito de ação trabalhista, em que se autorizava a perícia do algoritmo do aplicativo de transporte Uber, a fim de apurar potencial vínculo empregatício entre o motorista e a empresa. A decisão não entra em detalhes, mas diz que a realização da perícia poderia acabar revelando segredos comerciais da empresa e que, por isso, a medida deveria ser revogada[368].

Neste precedente, apesar de se tratar de uma decisão precária proferida em tutela provisória, importantes considerações sobre os segredos de negócio também foram ignoradas. O fato de não haver uma pretensão de sigilo absoluto aos segredos de negócio é a mais relevante, mostrando novamente como a simples invocação do instituto jurídico constitui uma saída argumentativa dos agentes de tratamento que os legitima a manifestar recusa no compartilhamento das informações.

No caso específico da relação empregatícia e das condições de trabalho, há ainda toda uma relevante discussão sobre plataformização e controle informacional[369]; sobre como o mercado de dados fez crescer a informalidade; sobre a disposição tecnológica ter passado a permitir jornadas praticamente em tempo integral[370]; e sobre novas práticas de precarização das condições de emprego[371]. Os segredos de negócio foram invocados como um instituto jurídico que acabou servindo para alienar o julgador de todas essas questões.

Por outro lado, e pensando na perspectiva do agente de tratamento, a divulgação de suas informações mais sensíveis para a condução de investigações pode se mostrar preocupante, sob o risco de a autoridade ou do próprio Poder Judiciário não conseguir assegurar a preservação dos segredos de negócio. Em outros países, autoridades públicas (inclusive de proteção de dados) sofreram com incidentes de segurança ocorreram recentemente[372]. Mesmo no Brasil, importantes órgãos da administração federal[373] e do

---

[368] Cf. Tutela Cautelar Antecedente 1000825-67.2021.5.00.0000. Rel. min. Douglas Alencar Ribeiro, j. 28 maio 2021, Tribunal Superior do Trabalho.
[369] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 39.
[370] Etinografia sobre o tema foi desenvolvida no trabalho: SOUZA, Ilan Fonseca. *Dirigindo Uber*: A subordinação jurídica na atividade de um motorista de aplicativo. Curitba: Juruá Editora, 2024.
[371] COHEN, *op. cit*., p. 30-33.
[372] CONVERGÊNCIA Digital. Operadora de telecom sofre mega ataque hacker e governo da Colômbia é obrigado a parar atividades. *Convergência Digital*. 2023. Disponível em: https://encurtador.com.br/C4UWA. Acesso em: 13 jul. 2024.
[373] TUNHOLI, Murilo. Ataque hacker gerou prejuízo de R$ 3,5 milhões ao Governo Federal. *giz_br*. 2024. Disponível em: https://encurtador.com.br/fnM5x. Acesso em: 13 jul. 2024; ANDRADE, Henrique. Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar. *CNN*. 2021. Disponível em:

Poder Judiciário[374] foram vítimas de ataques *hackers* cuja extensão e danos causados nunca foi amplamente divulgada. Se determinados segredos de negócio estivessem disponibilizados para essas autoridades e tivessem sido violados, os danos sofridos pelos agentes econômicos poderiam ser imensuráveis e até irreparáveis.

Portanto, também em relação aos códigos e aos elementos técnicos e subjetivos que compõem o tratamento dos dados, deve-se entender que a proteção pelos segredos de negócio pode acabar significando um entrave importante ao acesso dos titulares e das autoridades. A consequência disso não é apenas deixar de compreender como são tomadas decisões automatizadas. Elas implicam praticamente em desistir de exercer algum tipo de controle efetivo sobre o poder que os dados e as tecnologias conferem aos agentes de tratamento.

Garantias como a autodeterminação informativa se tornam fantasiosas, pois os segredos de negócio viram óbices concretos ao acesso dos titulares às explicações sobre como são tratados os dados, e podem ser também, como já visto, barreiras ao acesso dos dados em si e das metodologias de organização do conteúdo.

O mesmo pode ser dito da *accountability*: é impossível que a ANPD exerça algum controle sobre a legalidade e a extensão das operações de tratamento se não pode acessar os dados pessoais armazenados; os critérios de organização desses dados; os códigos matemáticos que instruem as operações; os sistemas; as subjetividades que são transcritas em linguagem matemática para direcionar os resultados, dentre outros.

Por outro lado, não se sabe em qual extensão os segredos de negócio alcançam os elementos tecnológicos envolvidos na operação, já que o tratamento de dados pessoais é muito mais sofisticado do que simples códigos matemáticos. Há toda uma sofisticação nas operações, fora uma dimensão de opacidade inerente ao funcionamento dos sistemas, que dificulta compreender exatamente quais elementos corroboraram para a produção do resultado e, por isso, quais deveriam ser os elementos essenciais protegidos pelos segredos de negócio ou fornecidos às autoridades para serem objeto de auditorias.

A dificuldade de assegurar a segurança da informação e a preservação do sigilo dos conteúdos fornecidos pelos agentes de tratamento são camadas adicionais de

---

https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/. Acesso em: 13 jul. 2024.

[374] BOSCO, Natália. Ataque de hackers ao STJ é o mais grave da história no país. *Correio Braziliense*. 2020. Disponível em: https://www.correiobraziliense.com.br/brasil/2020/11/4886936-ataque-de-hackers-ao-stf-e-o-mais-grave-da-historia-no-pais.html. Acesso em: 13 jul. 2024.

complexidade, elucidando que não é simples exigir o fornecimento de informações sem uma contrapartida de segurança significativa por parte das autoridades.

CAPÍTULO III: A OPACIDADE CRIADA PELOS AGENTES DE TRATAMENTO E A DIFICULDADE ADICIONAL NA CONCRETIZAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

III.1 O USO DOS SEGREDOS DE NEGÓCIO PARA AUMENTAR A EXTENSÃO DE OPACIDADE NO MERCADO DE DADOS PESSOAIS

As dificuldades de utilizar a categoria jurídica dos segredos de negócio no mercado de dados pessoais são problemas que relacionam a tensão entre sigilo e transparência nas decisões automatizadas. Demonstrou-se que, apesar de possível, o enquadramento jurídico que é feito pelos agentes de tratamento pode ser muito problemático, de modo que os segredos de negócio talvez sejam institutos inapropriados para proteger os elementos do mercado de dados pessoais.

Há uma escolha política por parte dos agentes em optar por tratar bases de dados, dados pessoais e algoritmos como segredos de negócio. Apesar dos argumentos burocráticos que favorecem essa decisão, existem também argumentos políticos, na medida em que, através dos segredos, os agentes podem dificultar o acesso dos titulares e das autoridades sobre como se dão suas operações.

III.1.1 A opacidade criada pelos agentes de tratamento de dados através do uso dos segredos de negócio

A síntese da preocupação sobre segredos de negócio no mercado em questão é que, ao tratar todos como segredos de negócio, as bases de dados, os dados pessoais, os códigos e os elementos de tomada de decisão automatizada, surge a possibilidade de os agentes de tratamento revestirem o tratamento de dados de camadas adicionais de opacidade.

Valendo-se do fato de que a natureza sigilosa é condição essencial para a proteção legal[375], os agentes podem se recusar a fornecer informações, conteúdos ou explicações

[375] GERALDES, João de Oliveira. Sobre a proteção jurídica dos segredos comerciais no espaço digital. *Revista da Faculdade da Universidade de Lisboa*, vol. LXIII, 1 e 2, Lisboa, 2022. p. 425. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Joa%CC%83o-de-Oliveira-Geraldes_compressed.pdf. Acesso em: 06 out. 2023; KORS, Jorge Alberto. *Los secretos industriales y el know how*. Buenos Aires: La Ley, 2007. p. 108.

aos titulares e às autoridades, ao argumento de que estão excepcionados em fazê-lo em razão da proteção que lhes é conferida pelos segredos de negócio.

Exemplos nesse sentido existem em vários cenários diferentes. Alguns deles já foram trazidos ao longo do presente trabalho, mas vale destacar outros: empresas que desenvolveram assistentes virtuais, operando por inteligência artificial, não disponibilizam informações sobre quais dados são coletados dos usuários.[376]. Plataformas de busca não informam como seus algoritmos produzem o resultado a partir dos dados coletados e dos *inputs* de pesquisa fornecidos pelo usuário[377]. Desenvolvedoras de *softwares* de reconhecimento facial utilizados pela administração pública não fornecem informações sobre como são organizadas suas bases de dados, quais dados estão armazenados e como são feitas as análises automatizadas[378]. *Softwares* de tomada de decisão deixam de fornecer esclarecimentos sobre quais os elementos foram considerados no processo[379]. Sistemas de identificação de fraudes em benefícios sociais não explicam

---

[376] Os esclarecimentos que são disponibilizados são genéricos e insuficientes. Não é fornecida a íntegra do conteúdo com a descrição detalhada do que a assistente virtual coleta e armazena em termos de dados pessoais. Ver: LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 3-5. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

[377] Empresas de busca que foram acusadas de misoginia e homofobia argumentaram que a opacidade inerente ao funcionamento de suas operações impediria a modificação dos resultados produzidos. Por esse motivo, recusaram-se a auditar seus códigos em razão dos segredos de negócio. Tempos depois, pressionadas pela opinião pública e por ameaças mais concretas de investigação, realizaram mudanças estruturais para coibir o problema e divulgaram tais fatos na forma de propaganda positiva para a empresa. Ver: NOBLE, Safiya Umoja. Algorithms of Oppression. How Search Engines Reinforce Racism. New York University Press, 2018. p. 58.

[378] PELE, Antônio; MULHOLLAND, Caitlin. On Facial Recognition, Regulation, and 'Data Necropolitics'. *Indiana Journal of Global Legal Studies*, v. 30. p. 173-194, 2023. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2023/07/On-Facial-Recognition-Regulation-and-Data-Necropolitics-Pele-Mulholland.pdf. Acesso em: 02 maio 2024. Os autores comentam casos emblemáticos do uso de tecnologias de reconhecimento facial no âmbito do monitoramento, fazendo um histórico de situações nas quais homens negros foram identificados como gorilas; ou quando jovens foram identificados por falta de dados suficientemente diversos nas bases dos algoritmos (p. 175-176).

[379] MOORE, Taylor R. Trade Secrets and Algorithms as Barriers to Social Justice. *CDT Free Expression Fellow*. 2017. p. 10. Disponível em: https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf. Acesso em: 02 maio 2024. O caso COMPAS ficou famoso por se referir a um algoritmo preditivo utilizado no âmbito do sistema judicial norte-americano, que não foi submetido a auditorias promovidas pelas autoridades ao argumento de que estava protegido por segredos de negócio. Contudo, auditorias independentes (LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren; ANGWIN, Julia. How We Analyzed the COMPAS Recidivism Algorithm. *Pro Publica*. 2016. Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. Acesso em: 12 maio 2024) demonstraram que os algoritmos estavam reproduzindo vieses discriminatórios contra a população negra, calculando de forma racista a probabilidade de reincidência que era utilizada pelos juízes como fundamento para negar liberdades condicionais e outros benefícios. Sobre o caso, ver: CARLSON, Alyssa M. The Need for Transparency in the Age of Predictive Sentencing Algorithms. *Iowa Law Review*, Vol. 103, 2017. p. 319-321. Disponível em: https://ilr.law.uiowa.edu/print/volume-103-issue-1/the-need-for-transparency-in-the-age-of-predictive-sentencing-algorithms. Acesso em: 12 maio 2024. Ver também: PASQUALE, Frank. Secret Algorithms Threaten the Rule of Law. *MIT Technology Review*. 2017.

como foram feitas as análises de condutas fraudulentas e quais dados foram levados em consideração para a produção dos resultados[380].

Em todos esses casos, os titulares de dados tiveram informações pessoais coletadas e utilizadas sem que soubessem quais eram essas informações e de que forma elas contribuíam para os resultados. Em alguns, foram identificados padrões discriminatórios, de modo que os resultados reproduziam vieses preconceituosos contra grupos minoritários. Em todos eles, os agentes se recusaram a fornecer esclarecimentos sobre suas operações, ao argumento de que eles eram protegidos pelos segredos de negócio[381].

Casos mais graves envolvem também a administração pública, que utiliza sistemas automatizados e inteligências artificiais para o desempenho de suas funções[382]. São casos de tomada de decisões judiciais[383], execução de políticas públicas[384], políticas

Disponível em: https://www.technologyreview.com/2017/06/01/151447/secret-algorithms-threaten-the-rule-of-law/. Acesso em: 12 maio 2024.

[380] O SRI era um sistema utilizado pelo governo alemão para auxiliar na identificação de fraudes no sistema de benefícios sociais e impostos. Contudo, foram identificados padrões discriminatórios incorporados no sistema preditivo da inteligência artificial, além de riscos de proteção à privacidade dos cidadãos que tinham seus dados analisados por ela. Estima-se que mais de 20.000 famílias foram identificadas como fraudulentas de forma indevida em razão da incorporação de vieses discriminatórios lastreados, dentre outros, em dados de imigração (SELDAM, Björn tem; BRENNINKMEIJER, Alex. The Dutch benefits scandal: a cautionary tale for algorithmic enforcement. EU Law Enforcement.2021. Disponível em: https://eulawenforcement.com/?p=7941. Acesso em: 12 maio 2024). Um dos fundamentos decisórios é que o sistema não tinha instrumentos de transparência suficientemente compatíveis com o que era exigido do ente público. Ver: UITSPRAKEN. *Rechtbank Den Haag*. 2020. Disponível em: https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878. Acesso em: 12 maio 2024.

[381] Como afirmam Danielle Keats Citron e Frank Pasquale: "That is a trade secret; a designation offering powerful legal protections to companies that want to keep their business practices a secret" [Isso é um segredo de negócio; uma designação que oferece uma poderosa proteção jurídica para empresas que querem manter seus modelos de negócio secretos] (CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, Vol. 89, 2014, p. 1-, U of Maryland Legal Studies Research Paper No. 2014-8. p. 17, tradução livre. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 12 maio 2024).

[382] LEVINE, David S. The impact of trade secrecy on public transparency. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 409.

[383] A inteligência artificial do *software* Victor foi uma das primeiras a ser desenvolvida pelo STF, em parceria com a Universidade de Brasília, para auxiliar na identificação de repercussão geral (MAIA FILHO, Mamede S.; JUNQUILHO, Tainá A. Projeto Victor: perspectivas de aplicação da inteligência artificial ao direito. *Revista de Direitos e Garantias Fundamentais*, [S. l.], v. 19, n. 3. p. 218–237, 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1587. Acesso em: 25 abr. 2024). Desde então, o poder judiciário já incorporou mais de 100 sistemas privados de automação decisória (KAUFMAN, Dora; JUNQUILHO, Tainá; REIS, Priscila. Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e direitos humanos. *Revista de Direitos e Garantias Fundamentais*, [S. l.], v. 24, n. 3. p. 43–71, 2023. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/2198. Acesso em: 17 abr. 2024. p. 51-52).

[384] RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. p. 61-116, 2020. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 24. p. 92.

vigilância[385], dentre outros, que preocupam por utilizarem tecnologias privadas que, protegidas pelos segredos de negócio, não fornecem níveis de transparência e explicabilidade compatíveis com a atividade pública[386]. Em casos como esses, também não são poucas as denúncias sobre decisões incorretas e discriminatórias[387] que causam prejuízos imensuráveis aos administrados[388] e que não podem ser amplamente investigadas porque a administração não tem acesso amplo aos elementos que compõem o resultado[389].

---

[385] Para persecução penal, tecnologias de identificação facial são amplamente utilizadas no Brasil. Sobre o tema, ver: MILANEZ, Giovanna. A utilização de tecnologias de reconhecimento facial para fins de segurança pública e persecução penal no Brasil: mapeando discussões e possíveis caminhos regulatórios. *In*: MENDES, Gilmar; FREITAS, Matheus Pimenta (org.). *Constituição, Direito Penal e Novas Tecnologias*. São Paulo: Almedina, 2023. p. 91-126; INSTITUTO Igarapé. Infográfico: Reconhecimento Facial no Brasil. *Igarapé*. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 25 abr. 24; Instituto Igarapé. Mais Câmeras, Mais Segurança. Disponível em: https://igarape.org.br/mais-cameras-mais-seguranca/. Acesso em: 25 abr. 2024.

[386] LEVINE, David S. Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure. *Florida Law Review*. 2007. p. 158. Disponível em: https://ssrn.com/abstract=900929. Acesso em: 26 maio 2024.

[387] Resgata-se a ideia trabalhada por Pele e Mulholland: "Our discussion on data necropolitics intersects these debates and is also more ambitious since we argue that the current production and exploitation of digital data can produce a novel production of death targeting growing, vulnerable populations. [...] First, data can produce and normalize the vulnerabilities that given populations have been facing (i.e., racial bias). Second, it can legitimize and turn invisible the violence and death those same populations have been suffering. Violence should not be understood as "mere" physical aggression or violation of private property rights. It is also socioeconomic and symbolic. When we refer to data necropolitics, we have in mind not only the physical elimination of certain individuals but also a predatory/digital form of governance that exposes and produces social violence, vulnerability, and, eventually, (social) death" [Nossa discussão sobre a necropolítica de dados intersecta esses debates e também é mais ambiciosa, pois argumentamos que a produção e exploração atuais de dados digitais podem gerar uma nova produção de morte direcionada a populações crescentes e vulneráveis. [...] Primeiro, os dados podem produzir e normalizar as vulnerabilidades que determinadas populações têm enfrentado (ou seja, preconceito racial). Segundo, podem legitimar e tornar invisível a violência e a morte que essas mesmas populações têm sofrido. A violência não deve ser entendida como uma simples agressão física ou violação de direitos de propriedade privada. Ela também é socioeconômica e simbólica. Quando nos referimos à necropolítica de dados, temos em mente não apenas a eliminação física de determinados indivíduos, mas também uma forma predatória/digital de governança que expõe e produz violência social, vulnerabilidade e, eventualmente, a morte (social)] (PELE, Antônio; MULHOLLAND, Caitlin. On Facial Recognition, Regulation, and 'Data Necropolitics'. *Indiana Journal of Global Legal Studies*, v. 30. 2023. p. 185, tradução livre. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2023/07/On-Facial-Recognition-Regulation-and-Data-Necropolitics-Pele-Mulholland.pdf. Acesso em: 02 maio 2024).

[388] Alguns desses riscos foram mapeados por esta autora em outras oportunidades. Ver: LINDOSO, Maria Cristine. Automatização na justiça criminal: Mapeamento dos riscos e considerações sobre o aspecto político da automatização. *In*: MENDES, Gilmar; FREITAS, Matheus Pimenta (org.). *Constituição, Direito Penal e Novas Tecnologias*. São Paulo: Almedina, 2023. p. 221-242; LINDOSO, Maria Cristine; DE MATOS, Amanda Visoto. O risco discriminatório da automatização decisória no poder judiciário: perspectivas e horizontes. *In*: PINHO, Anna Carolina (coord.). *Manual de Direito na Era Digital*. Processual. Indaiatuba, SP: Foco, 2023. p. 137-168. Também foi objeto de estudo por outros autores, destacando-se: SOUZA, Michel R. O; ZANATTA, Rafael A. F. The Problem of Automated Facial Recognition Technologies in Brazil: Social Countermovements and the New Frontiers of Fundamental Rights. *Latin American Human Rights Studies*, v. 1, 2021. Disponível em: https://revistas.ufg.br/lahrs/article/view/69423. Acesso em: 01 maio 2024.

[389] CARLSON, Alyssa M. The Need for Transparency in the Age of Predictive Sentencing Algorithms. *Iowa Law Review*, Vol. 103, 2017. p. 322-329. Disponível em: https://ilr.law.uiowa.edu/print/volume-103-issue-1/the-need-for-transparency-in-the-age-of-predictive-sentencing-algorithms. Acesso em: 12 maio 2024; CITRON, Danielle Keats. Open Code Governance. *University of Chicago Legal Forum*, vol. 2008,

Há, portanto, um nível de opacidade que envolve escolhas deliberadas dos agentes de tratamento em não fornecerem esclarecimentos, informações ou conteúdos sobre suas operações[390], ao argumento de que estão protegidos de fazê-lo em razão dos segredos de negócio[391]. Quando isso ocorre, amplia-se também a assimetria informacional, porque elementos de explicabilidade que poderiam ser disponibilizados, não o são[392].

As autoridades e os titulares nem mesmo poderiam tentar alcançar os níveis de explicabilidade pretendidos por meio de engenharia reversa, em razão da quantidade de dados coletados e da sofisticação dos sistemas que, em outras oportunidades ao longo deste trabalho, já foram detalhadas[393]. Ou seja, torna-se verdadeiramente impossível a compreensão mínima sobre o uso dos dados[394].

Não se ignora, por óbvio, que os níveis de explicabilidade nem sempre são atingidos dentro dos vários mercados em razão dos segredos de negócio. Há uma opacidade que é inerente ao funcionamento das operações e isso não é objeto de debate. A questão, contudo, é saber em que medida, no âmbito do tratamento de dados pessoais, os agentes podem criar outras camadas de opacidade sobre suas operações, apropriando-se de categorias jurídicas existentes para distanciar ainda mais os usuários e as autoridades de um conhecimento que eles poderiam ter sobre como se dão as operações.

---

n. 1, 2008, Artigo 9. Disponível em: http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/9. Acesso em: 27 abr. 2024. p. 357.

[390] CARLSON, Alyssa M. The Need for Transparency in the Age of Predictive Sentencing Algorithms. *Iowa Law Review*, Vol. 103, 2017. p. 322-329. Disponível em: https://ilr.law.uiowa.edu/print/volume-103-issue-1/the-need-for-transparency-in-the-age-of-predictive-sentencing-algorithms. Acesso em: 12 maio 2024.

[391] BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. p. 3. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023.

[392] Por outro lado, quando a opacidade é inerente ao funcionamento das operações, a questão deixa de ser propriamente de assimetria informacional, uma vez que se trata de uma dimensão intangível das operações e que não pode ser explicada nem mesmo pelo agente.

[393] MAGIOLINO, Mariateresa. EU Trade Secret Law and Algorithmic Transparency. *Bocconi Legal Studies Research Paper*, n. 3363178, 2019. p. 2. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363178. Acesso em: 04 abr. 2024; LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 8. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

[394] O funcionamento de mecanismos de busca elucida essa dificuldade. Em estudo feito sobre o Page Rank, sistema utilizado pela plataforma Google, apurou-se que os resultados produzidos podem envolver mais de 200 tipos de informações diferentes para serem produzidos, dentre palavras, links, imagens, dados comportamentais e outros. Alguns desses sinais são padrões revelados a partir de trilhões de pesquisas que o Google desenvolveu ao longo dos anos, o que torna impossível realizar engenharia reversa e descobrir como o algoritmo funciona. Sobre o tema, ver: GRIMMELMANN, James. The Structure of Search Engine Law. *Iowa Law Review*, v. 93, n. 1, 2007. NYLS Legal Studies Research Paper No. 06/07-23.Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=979568. Acesso em: 01 maio 2024.

Nesse cenário, o uso dos segredos de negócio se torna uma importante ferramenta para impedir o acesso às caixas-pretas que compõem os algoritmos[395]. A partir deles, cria-se uma ilusão de que a explicação sobre o funcionamento dos sistemas é inatingível quando o desconhecimento sobre o mercado de dados está, em sua maior extensão, sendo criado a serviço dos interesses dos agentes.

Scott Timcke chamou esse processo de opacidade capitalista: um tipo de incompreensão sobre o tratamento dos dados que é criada dentro do sistema com o objetivo de proteger os interesses de quem controla o capital[396]. Nessa visão, o Direito é reafirmado na posição de instrumento utilizado pelos agentes para proteção de seus interesses próprios, independentemente de outras garantias que possam existir aos indivíduos e à coletividade. Outros autores chamaram o mesmo fenômeno de *black box* jurídico (tradução livre de *legal black box*), igualmente referenciando a extensão de opacidade que vem dos modelos e códigos, mas não pode ser acessada em razão da proteção pelos segredos de negócio[397].

Independente do nome, os agentes ganham a possibilidade de utilizar uma categoria jurídica para obstar o acesso às operações de tratamento de dados pessoais. Como consequência, garantias fundamentais associadas à privacidade e à proteção de dados ficam prejudicadas, pois é subtraída do titular a possibilidade de ele conhecer como suas informações privadas são exploradas comercialmente (muitas vezes em decisões que vão lhe criar um impacto direto). O controle da legalidade das operações e do poder que é exercido pelos agentes também é diminuído, esvaziando importantes funções da autoridade.

III.2 UMA DIFICULDADE ADICIONAL: A LGPD CRIANDO CAMINHOS PARA OS AGENTES CRIAREM A OPACIDADE

A preocupação exposta até aqui relaciona a possibilidade de se enquadrarem como segredos de negócio alguns dos elementos essenciais do mercado de dados pessoais. Os

---

[395] PASQUALE, Frank A. Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries. *Northwestern University Law Review*. 1 out. 2010. p. 170. Disponível em: https://ssrn.com/abstract=1686043. Acesso em: 22 abr. 2024.

[396] TIMCKE, Scott. *Algorithms and the end of politics*: how technology shapes 21st-century American life. Bristol: Bristol University Press, 2021. p. 27.

[397] LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. *International Journal of Law and Information Technology*, Vol. 27, Issue 2, 2019. p. 122-141. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313916. Acesso em: 10 jan. 2024.

agentes adquirem argumentos, com suposto respaldo jurídico, para manifestarem recusa no fornecimento de esclarecimentos e no acesso das informações sobre como se dão suas operações.

Para além disso, há que se considerar que, no contexto brasileiro, a LGPD criou caminhos adicionais que podem ser utilizados para legitimar essa conduta dos agentes. Analisando o texto da lei, percebe-se que ele adota uma redação genérica que, em variadas circunstâncias, pode criar a impressão de que os direitos e as garantias dos titulares, bem como as competências da ANPD, estão vinculados a uma proteção anterior dos segredos de negócio.

A fim de analisar esse argumento, foram analisadas as 13 (treze) menções que a LGPD faz aos segredos de negócio[398], que podem ser categorizadas nos seguintes grupos: (i) acesso aos dados para portabilidade; (ii) acesso aos dados e explicações destinadas ao titular; (iii) acesso aos dados e explicações destinadas à autoridade regulatória; e (iv) acesso às explicações na comunicação de incidentes de segurança.

III.2.1 Acesso aos dados pessoais para portabilidade

O direito à portabilidade está descrito na LGPD por meio dos arts. 18, V e 19, parágrafo 3º. No primeiro dispositivo, fala-se da portabilidade feita diretamente entre agentes de tratamento, que constitui um direito exercível a qualquer momento, mediante requisição expressa. Nesse caso, o titular faz o pedido e os dados pessoais objeto do tratamento devem ser transferidos de um fornecedor de serviço para o outro, sem custos e de forma célere.

O segundo artigo, por sua vez, dispõe sobre a possibilidade de o titular ter cópia dos dados pessoais que foram coletados a partir da base legal do consentimento. Essa cópia deverá ser disponibilizada em formato que possibilite seu uso posterior, observados os segredos de negócio. Por isso, tal dispositivo acaba abordando também de uma hipótese de portabilidade, mas dessa vez intermediada pelo titular de dados, na medida em que ele que poderá acessar a cópia de suas informações pessoais em um formato reutilizável, para posterior compartilhamento com outros fornecedores.

A portabilidade de dados, exercida diretamente ou através do acesso, constitui um direito dos titulares de dados em relação aos agentes de tratamento. Trata-se de uma forma

[398] Aqui se consideram as menções feitas em dispositivos legais que não foram vetados e que estão vigentes na LGPD.

de assegurar o acesso aos dados até mesmo quando ela envolver a troca de prestadores de serviço.

A portabilidade como direito não foi inaugurada pela LGPD[399]. Contudo, o diploma trouxe a possibilidade de transferência, entre agentes econômicos, de dados pessoais, regulamentando novas operações para intercâmbio de conteúdo e possibilitando outras dimensões de interoperabilidade a partir da complementação de disposições setoriais específicas preexistentes.

Nesse sentido, a portabilidade de dados possui inúmeros aspectos positivos. Do ponto de vista do titular, ela reforça o compromisso com a transparência ao criar a possibilidade de acessar os dados e migrá-los de um fornecedor para o outro. Trata-se de um mecanismo de gestão informacional[400] e exercício da autodeterminação informativa[401], que viabiliza a escolha de prestadores de serviço sem que eventual troca cause prejuízos[402]. Assim, além de uma ferramenta de acesso aos dados, a portabilidade permite ao titular ter escolhas.

Do ponto de vista coletivo, a portabilidade também indica uma preocupação da LGPD com a concentração do mercado. Trata-se de um dispositivo que evita que a relação se torne uma prisão ao consumidor, sem que ele consiga trocar de fornecedor (efeito *lock in*[403]). O consumidor passa a ser resguardado pelo direito de mudar suas relações comerciais sem se prejudicar por essa escolha, levando consigo os dados pessoais que são essenciais para a prestação de um serviço. Esse direito reduz os custos de troca de fornecedores e reforça a possibilidade de o titular dos dados ter o direito de desenvolver

---

[399] A título de exemplo, a ANATEL regulamentou critérios gerais de portabilidade dentro das empresas prestadoras de serviços de telecomunicações ainda em 2007 (Regulamento Geral de Portabilidade (RGP) – Resolução nº 460, de 19 de março de 2007, da Agência Nacional de Telecomunicações (ANATEL)) e o BACEN regulamentou, em 2013, a portabilidade de operações de crédito entre pessoas naturais (Resolução 4.292, de 20 de dezembro de 2013, do Banco Central do Brasil (BACEN).

[400] Como afirma Daniela Cravo: "não há como deixar de reconhecer que a portabilidade de dados, além dos seus potenciais efeitos ao mercado e ao bem-estar do consumidor, é um direito individual, permitindo não só uma maior gestão e controle dos dados pelo titular, mas também que esse usufrua do ecossistema de dados" (CRAVO, Daniela. O direito à portabilidade na Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023. p. RB-12.2.

[401] SILVA, Priscila Regina. Os Direitos dos Titulares de Dados. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 203.

[402] CRAVO, *op. cit*., p. RB-12.2.

[403] De acordo com Daniela Cravo: "o *lock-in* é o efeito de permanência do consumidor ao fornecedor originário mesmo quando haja um desejo pela mudança, que pode ser proveniente do aumento de preços, falhas, vícios ou defeitos no fornecimento do produto ou serviço, vazamento de dados ou falta de privacidade. No entanto, quando esse consumidor faz um cálculo do custo-benefício de uma eventual troca, percebe que será mais custoso, seja monetariamente, seja emocionalmente, seja em termos de conforto, trocar para um fornecedor alternativo" (*Ibid*., p. RB-12.3).

sua identidade digital. Com isso, também possibilita novos entrantes no mercado, pois autoriza que concorrentes estejam em posição negocial competitiva para atrair novos consumidores[404].

A portabilidade marca então um esforço legal para promover o exercício da autodeterminação informativa e um ambiente menos concentrado, no qual as barreiras de acesso são menores e novos competidores podem igualmente tentar conquistar os consumidores.

A regulação da portabilidade, contudo, deve ser feita de forma cuidadosa, e envolve aspectos técnicos sofisticados, bem como esforços para que a promoção de um ambiente concorrencial mais arejado não acabe criando distorções concorrenciais prejudiciais. A esse respeito, já foi dito que a concorrência desleal é multifacetada e não pode ser tida apenas como o vazamento ilegal de informações. Além das condutas clássica que se caracterizam como concorrência desleal, é preciso também considerar que outras circunstâncias – até mesmo previstas em lei – podem gerar vantagens indevidas que favorecem determinado agente na disputa pela clientela[405], ou que viabilizam o acesso impróprio de terceiros a informações essenciais e economicamente relevantes de outros agentes[406].

---

[404] Aqui cabem destacar as considerações de Frazão, Prata de Carvalho e Milanez sobre o tema: "Com isso, evita-se que os consumidores fiquem presos a determinado ofertante (efeito *lock in*) em virtude das dificuldades da 'perda' dos dados. Daí a ideia de que o direito à portabilidade, para atingir tais propósitos, deve ser fácil, gratuito e assegurado de modo a permitir a usabilidade dos dados com eficiência e segurança. Além da proteção ao titular dos dados, o direito à portabilidade tem também importantes implicações concorrenciais, pois, partindo da premissa de que os dados são os mais importantes insumos da economia movida a dados – até mesmo *essential facilities*, isto é, infraestruturas essenciais para o acesso de determinados mercados -, a portabilidade pode facilitar a transferência dos dados para fins de ingresso de novos entrantes ou *startups* no mercado ou mesmo para estimular a competição entre rivais já existentes, evitando que o acúmulo de dados por apenas um ou determinados *players* possa ser uma verdadeira barreira a entrar ou fator que comprometa a rivalidade com agentes menores. Além dos desdobramentos concorrenciais, o direito à portabilidade ainda pode gerar diversos benefícios ao mercado, já que pode também ser utilizado para a troca de dados entre serviços complementares, facilitando a vida dos interessados" (FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022, p. 319-320.

[405] BARBOSA, Pedro Marcos Nunes. *Curso de Concorrência desleal*. Rio de Janeiro: Lumen Juris, 2022. p. 231.

[406] Cabe trazer novamente as considerações de Pedro Marcos Nunes Barbosa sobre as diferentes facetas da concorrência desleal, especialmente quando se pensam em novas tecnologias: "a concorrência desleal é, em geral, abrangida por atos de (a) usurpação de distintividade; (b) danos reputacionais; (c) apropriação de dados sensíveis do concorrente através de meios ilegítimos; (d) práxis de conduta danosa e incalculável pelos parâmetros do setor; enfim, (e) abusivos da liberdade de competir que não sejam prescritos e proscritos nas regras sobre concorrência ilegal ou interdita. São infinitas as combinações de criatividade malévola com a qual se pode lesar, diretamente, o concorrente, e, indiretamente, o consumidor, o Estado, o meio ambiente, enfim, externalidades negativas aos demais núcleos de interesses que participem da relação jurídica poliédrica" (BARBOSA, *op. cit*., p. 230).

No caso da portabilidade, essa é uma possibilidade concreta, na medida em que diz respeito a uma interação entre concorrentes diretos: um agente é compelido a fornecer os dados que coletou para outro agente, porque o titular quer mudar o fornecedor do serviço.

Diante da complexidade da situação, surgem duas questões centrais. A primeira delas é de natureza operacional: não há clareza sobre como será executada a portabilidade; qual agente será responsável por desenvolver o sistema no qual os dados vão ser compartilhados; e de que forma vão ser preservados os segredos de negócio envolvidos no desenvolvimento do sistema que irá viabilizar a interoperabilidade[407].

A questão está em processo de regulamentação pela ANPD porque, além de uma interface para viabilizar a portabilidade, os agentes precisam organizar a forma como isso será feito e dimensionar os custos da operação. Os dados são explorados em diversos padrões diferentes – dados crus, agregados, inseridos em bases, dentre outros – e a obrigação de portabilidade pode demandar dificuldades técnicas e investimentos elevados que precisam ser programados.

Inexistindo resolução quanto à forma como será assegurada a portabilidade, é possível concluir que o direito do titular não é assegurado, pois não há disposição sobre o sistema e os elementos técnicos que vão viabilizá-lo.

A segunda questão é justamente que, ao que se percebe da redação da norma, alguns dados pessoais podem ser considerados segredos de negócio, tornando-se necessário avaliar se eles poderiam, ou não, ser objeto de compartilhamento entre concorrentes.

O enquadramento de dados pessoais como segredo, nesse contexto do mercado de dados, mostra-se problemático de início, porque coloca como ativo um conteúdo que é, antes de tudo, um desdobramento da personalidade individual. Por esse motivo, existem dúvidas se deveria existir algum tipo de limitação ao direito de o titular migrar todas as informações sobre si para um concorrente. E não necessariamente seria preciso enquadrar dados pessoais como segredos de negócio para que os riscos concorrenciais fossem mitigados. A lei ou a regulação específica poderiam simplesmente dispor expressamente quais dados podem ser objeto ou não de compartilhamento entre agentes.

Esse ponto, inclusive, elucida um problema adicional na redação da norma, porque inexiste detalhamento de quais são os dados que são considerados segredos de negócio, a

---

[407] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 46.

fim de que se saiba qual conteúdo poderá ou não ser objeto de portabilidade. Até o momento não há regulação específica sobre isso, de modo que não há clareza, seja para o titular, seja para o agente, sobre o que deve ou não ser disponibilizado.

Os titulares podem nem ter acesso a quais dados não foram disponibilizados, e não se sabe se essas informações são apagadas ou anonimizadas depois da portabilidade[408]. Assim, há pouca transparência sobre como de fato se efetiva a portabilidade e quais são os dados que estão envolvidos no processo.

Ao fim, e como já antecipado anteriormente, o enquadramento de dados pessoais como segredos de negócio cria espaço para que os agentes de tratamento possam exercer um juízo discricionário sobre como assegurar o acesso aos dados pessoais, ainda que para fins de portabilidade. Surge uma possibilidade de escolha que não está lastreada em nenhuma obrigação específica de se justificar quais dados não estão sendo fornecidos, ou de fornecer detalhamentos maiores sobre o que justificaria a recusa. Pela redação da LGPD, a exceção de compartilhamento dos segredos de negócio é taxativa e sequer precisa ser fundamentada.

Se o objetivo é assegurar a autodeterminação informativa e criar um ambiente mais competitivo, a limitação no compartilhamento dos conteúdos inviabiliza grande parte dessas pretensões. Quanto ao titular dos dados, o direito de controle do fluxo informacional passa a ser limitado ao que o agente escolhe compartilhar. E quanto ao mercado, a recusa no fornecimento de dados pode ser tamanha que a troca de fornecedores passa a se tornar custosa e trabalhosa para o titular, retirando dele o direito de escolha. Não só, é possível que dados essenciais para a prestação dos serviços não sejam fornecidos por serem considerados segredos de negócio, e isso acabaria reforçando a concentração do mercado e a dificuldade de operacionalizar a portabilidade[409].

Há, portanto, uma possibilidade de uso dos segredos de negócio para que o agente dificulte a materialização da transparência nessa dimensão de acesso aos dados. O agente utiliza os segredos de negócio para aumentar a distância do titular sobre suas operações,

---

[408] SILVA, Priscila Regina. Os Direitos dos Titulares de Dados. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 205.

[409] Essa dificuldade fica clara quando se pensa no âmbito da internet das coisas, onde grande parte dos dados pessoais coletados não são diretamente relacionados àquela atividade, mas prestigiam a operacionalização e o funcionamento dos serviços. Sobre o tema, ver: LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

fazendo isso pela recusa no fornecimento de dados, seja para o concorrente direto (na portabilidade direta), seja para o próprio titular (na portabilidade indireta).

III.2.2 Acesso aos dados pessoais e explicações sobre as operações destinadas ao titular

A LGPD também estabelece possibilidades por meio das quais os titulares podem ter acesso aos dados pessoais e às explicações sobre as operações. Diferentemente do direito de portabilidade, essas circunstâncias não demandam a interação direta de agentes econômicos concorrentes entre si. São formas legítimas pelas quais os titulares podem conhecer sobre como seus dados são utilizados e obter informações sobre os processos de coleta, armazenamento e tratamento, a fim de que seja empoderado a exercer sua autodeterminação informativa.

Exemplos desses dispositivos são os artigos que delimitam o que é transparência (art. 6º, VI); que possibilitam o livre acesso aos dados (9, II); que criam o dever de informar a forma e o tempo de duração das operações de tratamento (19, II); ou que estabelecem a possibilidade de ter explicações sobre decisões automatizadas, para que se possa pedir, então, a sua revisão (20, parágrafo 1º).

Apesar do esforço em detalhar dimensões de explicabilidade que são direcionadas aos titulares, em todas as circunstâncias que a LGPD trata da questão, o alcance dos esclarecimentos sofre uma limitação objetiva: ele não precisa envolver o compartilhamento de informações que sejam consideradas segredos de negócio.

Há uma primeira questão que diz respeito justamente à dificuldade de se enquadrar os elementos do mercado de dados como segredos de negócio. Foi exposto anteriormente que, apesar de ser possível tratar bases de dados, dados, códigos e outros elementos como segredos, existem complexidades que transcendem a categorização jurídica e que deveriam ser consideradas em razão das especificidades do mercado. A lei não faz qualquer diferenciação nesse sentido, e a redação dos dispositivos parece ser excessivamente aberta para não explicar, sequer, quais são os conteúdos que são segredos e que, por isso, não deveriam ser fornecidos.

Outra questão importante é perceber que a redação das normas cria uma ideia de que segredos de negócio são protegidos por um tipo absoluto de sigilo, como se fossem conteúdos que em nenhuma circunstância precisam ser fornecidos aos titulares. A forma como se excepcionam as obrigações de transparência sugere que a categoria jurídica dos

segredos é quase um salvo-conduto para que o agente não precise assegurar os direitos dos titulares de dados.

Sabe-se que os segredos de negócio limitam obrigações de transparência em vários outros cenários[410]. A tensão entre o sigilo e a explicabilidade não é exclusiva ao mercado de dados pessoais e por vezes são necessários esforços para conciliar os interesses privados e os interesses coletivos. A questão é que, especificamente para o mercado de dados pessoais, o conflito entre transparência e segredos é muito maior, e pode trazer impactos muito mais significativos.

Não é excessivo rememorar o poder que os dados pessoais e as tecnologias franqueiam aos agentes de tratamento, nem resgatar o tamanho dos impactos sociais, culturais e políticos que uma grande empresa de tecnologia pode criar ao influenciar ou direcionar comportamentos através de suas plataformas.

No mercado de dados, esses resultados não são produzidos apenas por um único elemento essencial e que poderia, então, ser protegido pelos segredos de negócio em razão do grande diferencial que ele apresenta à empresa. Os resultados são produzidos por uma convergência de fatores e interações que, individualmente, podem não ter impacto significativo, mas em conjunto adquirem significativo potencial. O esforço dos agentes de tratamento é então para que todos esses elementos sejam protegidos pelos segredos, revestindo assim as operações de um nível de sigilo que torna praticamente impossível compreender como a análise automatizada de conteúdo funciona[411].

O esforço parece ter sido acolhido pela LGPD, porque a ressalva dos segredos de negócio é feita em diferentes contextos, para diferentes conteúdos, de forma a limitar o acesso do titular[412]. Se os segredos de negócio estão excluídos dos conteúdos que devem

---

[410] Outras leis específicas também criam limitações similares à transparência por meio dos segredos de negócio. É o caso da Lei do Cadastro Positivo (Lei n. 12.414/2011), que em seu art.5º, IV, assegura como direito do consumidor cadastrado o conhecimento sobre os elementos principais considerados na análise do risco de crédito, resguardando o segredo industrial. Na visão de Leonardo Roscoe Bessa, trata-se de um entendimento acertado. Ver: BESSA, Leonardo Roscoe. *Nova Lei de Cadastro Positivo*: comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2019. p. RL 1.9.

[411] Um paralelo interessante para exemplificar a questão seria pensar na receita de um famoso refrigerante. A receita é protegida por segredos de negócio e os agentes não são obrigados a fornecê-la. Contudo, não é necessário manter sob a proteção dos segredos de negócio quais são os ingredientes que compõem aquela receita – ao contrário, a divulgação deles constitui, em muitos países, um dever legal em relação ao consumidor. No mercado de dados pessoais, é como se os agentes quisessem manter sob sigilo a receita (que talvez seriam, analogamente, os códigos matemáticos) e os ingredientes (os dados, as bases, os elementos que compõem o sistema).

[412] Diferentemente do que ocorre com a Lei do Cadastro Positivo, a LGPD regula um fluxo informacional mais considerável e uma variedade de situações maior que envolvem o tratamento de dados pessoais. Por isso, apesar de existirem normas similares no ordenamento, a forma genérica como se coloca a limitação dos deveres de transparência alcança situações jurídicas que sequer podem ser previstas e por isso se torna

ser compartilhados, não é claro qual o exato escopo do que é a explicabilidade direcionada ao indivíduo, justamente porque o agente pode escolher o que é ou não segredo de negócio dentro de suas operações e assim se recusar a disponibilizar essa informação ou dado ao titular.

As limitações criadas pela LGPD à explicabilidade direcionada ao titular criam, portanto, a possibilidade de o agente ampliar a opacidade sob suas operações, escolhendo em qual extensão ele quer assegurar direitos dos titulares ou cumprir com suas obrigações de transparência. No lugar de criar mecanismos efetivos de transparência, a redação da LGPD pode possibilitar o aumento da assimetria informacional e o distanciamento (ainda maior) do titular em relação ao conhecimento de como são tomadas as decisões automatizadas[413]. Ou seja, o titular deixa de ter acesso a esclarecimentos importantes, que compõem a sua autodeterminação informativa[414].

A hipervulnerabilidade do titular é agravada a ponto de criar distorções que dão ao agente o conhecimento amplo e irrestrito sobre o titular, ao passo que o titular sequer tem o direito de saber quais os dados sobre si foram coletados[415].

São imensuráveis as consequências dessa opacidade criada pelos agentes de tratamento a partir da redação genérica dos dispositivos legais. Elas vão desde a ampliação das possibilidades de coleta de dados pessoais[416] até o aumento da capacidade de interferência nos comportamentos sociais[417]. Surgem impactos também na capacidade

---

mais gravosa. Sem prejuízo, limitação de acesso às informações que são utilizadas no risco de crédito comportam as mesmas críticas que foram feitas ao precedente julgado pelo STJ, como foi discutido anteriormente neste trabalho.

[413] BERTONCELLO, Káren Rick Danilevicz. Fluência algorítmica: concretização do dever de informação e de explicabilidade na concessão do crédito ao consumidor. *In*: MARQUES, Claudia Lima *et al*. (coord). *5 anos de LGPD*: estudos em homenagem a Danilo Doneda. São Paulo: Thomson Reuters Brasil, 2023 [livro eletrônico]. p. RB-17.2.

[414] BAYAMLIOĞLU, Emre. Contesting Automated Decisions. *European Data Protection Law Review*, v. 4, 2018. Disponível em: https://ssrn.com/abstract=3305272. Acesso em: 16 abr. 2024.

[415] TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology & Intellectual Property*, v. 11. p. 239, 2013. p. 255. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 19 maio 2024.

[416] Em esforço que foi divulgado internacionalmente, um titular de dados na Irlanda conseguiu acesso integral a seus dados pessoais por meio de anos de requisições feitas a uma famosa plataforma de rede social. Quando conseguiu acesso aos dados, o documento tinha mais de mil páginas de dados coletados, muitos dos quais, segundo alegou o titular, não haviam sido coletados de forma autorizada. Ainda assim, o titular alega que não teve acesso a todos os dados e que diversas informações comportamentais, de rastreio de comportamentos ainda deveriam ser fornecidas. Ver: O'BRIEN, Kevin J. Austrian Law Student Faces Down Facebook. *The New York Times*. 2012. Disponível em: https://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html. Acesso em: 02 maio 2024.

[417] MAGIOLINO, Mariateresa. EU Trade Secret Law and Algorithmic Transparency. *Bocconi Legal Studies Research Paper, n. 3363178,* 2019. p. 2. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363178. Acesso em: 04 abr. 2024; LA DIEGA,

de o titular influenciar no tratamento dos dados[418]; no devido processo legal[419]; e na possibilidade concreta de rever e contestar decisões automatizadas[420].

Também se torna mais difícil acreditar na segurança dos dados e criar elementos de confiabilidade sobre os sistemas[421]. Com a limitação da explicabilidade em razão dos segredos de negócio, o titular é expropriado da possibilidade de conhecer toda a extensão dos riscos envolvidos no tratamento de seus dados. O titular diminui sua preocupação com as condutas dos agentes porque perde completamente a dimensão dos impactos envolvidos na atividade[422].

Ainda, a nova opacidade faz aumentar a ubiquidade com que as tecnologias se inserem no cotidiano, aumentando a distância entre o agente e o titular e tornando o titular

---

Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 1-2. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

[418] BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 134.

[419] Apesar de já ter sido mencionado antes, é importante detalhar o que pode ser considerado devido processo legal no âmbito do tratamento automatizado de dados. Ele envolve o direito assegurado ao titular de dados para que conheça as premissas fundamentais que ensejaram o resultado, ainda que isso se dê por meio de auditorias e explicações mais amplas sobre o processo decisório como um todo (CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, v. 55, n. 93, 2014. p. 122 Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784. Acesso em: 12 mar. 2024). Envolve também a possibilidade de ser ouvido (p. 123-124) e poder questionar aquela decisão com a revisão dela por um novo método, que pode envolver uma análise por um diferente sistema ou a supervisão humana de um terceiro (p. 124-125). Também sobre o tema, o devido processo pode envolver aspectos amplos como o direito de ser ouvido e a notificação prévia sobre quais decisões são tomadas sobre si (CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, 85, 1249, 2008. Disponível em: https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2. Acesso em: 02 mar. 2024).

[420] A contestação das decisões automatizadas, por outro lado, é mais controversa e pode ser objeto de disputa. Existe significativa disparidade de poder entre o agente que toma a decisão automatizada e o titular que é impactado por ela, e não existem parâmetros tão unânimes na doutrina sobre como seria possível assegurar uma contestação efetiva. Revisões humanas, por exemplo, podem acabar sendo inefetivas, na medida em que humanos tendem a ser influenciados a seguirem a decisão algorítmica (KAMINSKI, Margot E. Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability. South *California Law Review*, v. 92. 2019. p. 1.594. Disponível em: https://scholar.law.colorado.edu/faculty-articles/1265/. Acesso em: 17 mar. 2024; LYONS, Henrietta; VELLOSO, Eduardo; MILLER, Tim. Conceptualising Contestability: Perspectives on Contesting Algorithmic Decisions. *Proceedings of the ACM Human-Computer Interaction*, Volume 5, CSCW1, Article 106, 2021. p. 1-25. Disponível em: https://dl.acm.org/doi/10.1145/3449180. Acesso em: 12 maio 2024). Existem também diferentes tipos de contestação das decisões e métodos por meio dos quais elas podem ser feitas (LYONS; VELLOSO; MILLER, *op. cit.*). O objetivo do presente trabalho não é detalhar tais questões, mas sim defender que os segredos de negócio não podem constituir um óbice para que elas sejam possíveis.

[421] MARANHÃO, Juliano. COZMAN, Fábio Gagliardi; ALMADA, Marco. Concepções de explicação e do direito à explicação de decisões automatizadas. *In*: VAINZOF, Rony; GUTIERREZ, Andrei Guerrero (coord.). *Inteligência* artificial [livro eletrônico]: sociedade, economia e Estado. São Paulo: Thomson Reuters, 2021. p. RB 6.2.

[422] CITRON, Danielle Keats. Open Code Governance. *University of Chicago Legal Forum*, vol. 2008, n. 1, 2008, Artigo 9. p. 369-370. Disponível em: http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/9. Acesso em: 27 abr. 2024.

ainda mais alheio aos sistemas algorítmicos que passam a controlar a sua vida[423]. Em uma perspectiva mais ampla, a autodeterminação informativa acaba sendo esvaziada e dá lugar ao determinismo algorítmico, por meio do qual os sistemas administrados pelos agentes retiram do consumidor o seu livre-arbítrio, sua individualidade e suas possibilidades de escolha[424].

Tais preocupações não são exclusivas da legislação brasileira[425], mas certamente são agravadas pela quantidade excessiva de vezes que a LGPD possibilita excepcionar o cumprimento da obrigação legal em prol da proteção aos segredos de negócio. A própria discricionariedade com a qual os agentes podem decidir a extensão do cumprimento de obrigações legais é criada pela forma ampla com que a LGPD tratou os segredos de negócio, fazendo surgir dúvidas concretas se a proteção de dados é mesmo o objetivo final da norma[426].

Individualmente, portanto, as possibilidades de escolha do titular se mostram cada vez mais restritas: além das limitações de racionalidade e da opacidade inerente às operações, ele ainda é limitado pelo que o agente escolhe ou não disponibilizar. O Direito acaba fornecendo aos titulares um argumento adicional para revestirem suas operações de níveis de opacidade ainda maiores.

---

[423] OELDORF-HIRSCH, Anne; NEUBAUM, German. What Do We Know About Algorithmic Literacy? the Status Quo and a Research Agenda for a Growing Field. *SocArXiv*. November 18, 2021. Disponível em: https://doi.org/10.31235/osf.io/2fd4j. Acesso em: 20 dez. 2023; BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. p. 4. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023.

[424] VERBICARO, Dennis. Determinismo algorítmico: uma ameaça real à individualidade do consumidor. *In*: MARQUES, Claudia Lima *et al*. (coord). *5 anos de LGPD*: estudos em homenagem a Danilo Doneda. São Paulo: Thomson Reuters Brasil, 2023 [livro eletrônico]. p. RB-7.2.

[425] Problema similar é mapeado no âmbito do RGPD, já que a extensão dos direitos relacionados à explicabilidade também é limitado e não se sabe o que deve ou não ser obrigatoriamente fornecido pelo agente de tratamento, quais são as informações que devem compor a explicação necessária sobre as operações, e qual o nível de transparência que pode ser esperado, até mesmo diante da proteção que se dá aos segredos de negócio. Sobre a questão, ver: EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, v. 16. p. 18, maio 2017. Disponível em: https://ssrn.com/abstract=2972855. Acesso em:10 abr. 2024.

[426] Aproveitando as palavras de Bruno Bioni, tamanho poder decisório nas mãos dos agentes sobre qual a extensão de cumprimento das obrigações de transparência significa colocar "a raposa para cuidar do galinheiro" (BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 81). Em considerações similares, disse "This raises the question of whether a company whose interests do not Always align with its users' will be capable of providing adequate process and fair results" [Isso levanta a questão de se uma empresa cujos interesses nem sempre se alinham com os de seus usuários será capaz de fornecer um processo adequado e resultados justos] (KAMINSKI, Margot E. Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability. South *California Law Review*, v. 92, 2019. p. 1.593-1.594, tradução livre. Disponível em: https://scholar.law.colorado.edu/faculty-articles/1265/. Acesso em: 17 mar. 2024).

III.2.3 Acesso aos dados pessoais e explicações sobre as operações direcionadas à autoridade regulatória

O acesso aos dados também pode ocorrer por meio de obrigações que são direcionadas às autoridades, a fim de que elas possam cumprir os objetivos de *accountability*, de regulação e de controle de poder.

A ideia é que a *accountability* aumente a responsabilidade dos agentes e crie caminhos efetivos para a compreensão sobre como ocorrem as operações[427][428]. Pela competência regulatória, a ANPD cria políticas e regulações que estejam lastradas na realidade de como os dados são tratados[429]. E para o controle de poder, a autoridade consegue avaliar os impactos discriminatórios na tomada de decisão automatizada[430], bem como os excessos e usos abusivos dos dados pessoais (especialmente em relação a grupos mais vulneráveis, como menores de idade[431]).

---

[427] HERT, Paulo de. Accountability and system responsibility: new concepts in data protection law and human rights. *In*: GUAGNIN, Daniel *et al.* (org). *Managing Privacy through Accountability*. London: Palgrave Macmillan UK, 2012. p. 219.

[428] Nesse ponto, Bioni destaca que existem outros atores sociais que são igualmente importantes na *accountability* e que deveriam também participar do processo de controle de poder (BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022). A perspectiva adotada no presente trabalho não ignora a importância desses atores, mas entende que a competência maior é da autoridade, justamente por possuir ela poder de polícia e poder sancionador, além de outras competências exclusivamente estatais, que permitem algum tipo de equilíbrio em relação aos agentes de tratamento.

[429] BUSUIOC, Madalina. Accountable artificial intelligence: holding algorithms to account. *Public Administration Review*, v. 81, n. 5. p. 825-836, Sept./Oct. 2021. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293. Acesso em:18 abr. 2024.

[430] Anita Allen é uma importante autora que denunciou as preocupações com os vieses discriminatórios e a opacidade que cerca esses algoritmos no que diz respeito à população afro-americana. Também desenhou considerações importantes sobre a necessidade de se criarem sistemas que incorporem consciência racial para evitar discriminações e incorporar uma ideia de privacidade que considere também as desigualdades sociais. Ver: ALLEN, Anita L. Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform. *The Yale Law Journal Forum*, February 2022. Disponível em: https://www.yalelawjournal.org/forum/dismantling-the-black-opticon. Acesso em: 11 jan. 2023.

[431] A importância da atividade da ANPD para proteção dos interesses de crianças e adolescentes é muito expressiva, quando se toma por dimensão a situação de vulnerabilidade dos menores de idade e o ambiente ao qual eles estão expostos nas redes sociais, que coletam dados pessoais e produzem resultados (ainda que de menor impacto) automatizados em relação a eles. Pensando em menores, "a autoestima e a própria concepção individual necessárias para a formação da personalidade e da identidade de crianças e adolescentes são construídas de maneira digital. É nesse cenário que afloram discussões sobre a tomada de decisões com base no tratamento automatizado de dados que interfiram, de maneira sensível, em crianças e adolescentes. Para além da própria admissibilidade das decisões automatizadas, o exercício de remédios jurídicos diante dessas decisões, em atenção à condição peculiar de desenvolvimento desses agentes, também deve ser analisado" (DE ÁVILA, Sergio marcos Carvalho; KORKMAZ, Maria Regina Rigolon. Decisões automatizadas e a proteção de crianças e adolescentes. *In*: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (coord.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de

Mais que deveres, existem obrigações de os agentes fornecerem informações, Relatório de Impacto e auditorias, assumindo-se que, quanto maior a concentração de poder e a possibilidade de escolher como tratar os dados, mais transparentes deveriam ser as operações e maiores as obrigações de prestação de contas[432].

Em contrapartida, a ANPD deve fornecer segurança, não permitindo a divulgação de documentos e conteúdos sigilosos dos agentes e utilizando as informações somente para instrução de suas investigações internas.

As possibilidades que criam essas obrigações envolvem circunstâncias diversas: fiscalização de tratamento de dados de segurança pública, defesa nacional ou relacionadas às infrações penais (arts. 4º, III, parágrafo 3º); apuração de conformidade da base legal do legítimo interesse (arts. 10, parágrafo 3º e 38, da LGPD); investigação de riscos discriminatórios (art. 20, parágrafo 2º), dentre outros.

Contudo, e independentemente da circunstância, as três possibilidades de comunicação entre o agente e a autoridade – por meio de esclarecimentos, Relatório de Impacto e auditorias – têm suas extensões limitadas pelos segredos de negócio. Surgem, então, preocupações importantes sobre como a autoridade passa a ter seus objetivos e suas competências significativamente restringidos.

Para o cumprimento de seus objetivos, espera-se que a ANPD tenha acesso aos dados e aos elementos que compõem as operações. São explicações que podem vir de diferentes formas, como já mencionado, mas que precisam reunir o conjunto de conteúdos necessários à compreensão técnica exata sobre como os dados são coletados, qual a extensão e finalidade das operações e quais os riscos envolvidos ao titular e à sociedade[433].

Esse amplo acesso não é assegurado pela LGPD. A redação das normas limita o que o agente é obrigado a compartilhar com a autoridade e acaba por conferir aos segredos de negócio níveis de sigilo absolutos, que obstam as possibilidades de disponibilização de informações. Inexiste paralelo detalhamento de quais dados ou quais conteúdos devem ser excluídos dos esclarecimentos, dos Relatórios de Impacto, ou das auditorias. Mais uma vez, a escolha sobre o que vai ser ou não fornecido fica a critério do agente, que pode

---

Janeiro: Obliq, 2021. E-book. p. 111). E esse controle, de certa forma, só pode ser feito por parte da autoridade.

[432] BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 128-129.

[433] MACCARTHY, Mark. New Directions In Privacy: Disclosure, Unfairness and Externalities. *I/S*: A Journal of Law and Policy for the Information Society. 425. 2011. p. 69-72. Disponível em: https://ssrn.com/abstract=3093301. Acesso em: 27 nov. 2023.

decidir como ele quer cumprir suas obrigações em relação à autoridade e qual será a extensão da fiscalização que ele irá permitir sobre suas operações.

Se toda a ideia de controle de poder tem lastro na colaboração entre o agente e a autoridade, na prática, não há *accountability*, porque os segredos de negócio fornecem aos agentes a justificativa necessária para interromperem o fluxo de esclarecimentos que precisaria existir. Os agentes escolhem o que compartilhar com a autoridade, e certamente escolhem não divulgar elementos do processo que possam indicar vieses, violações legais ou desrespeito aos compromissos éticos[434].

A capacidade regulatória e de criar políticas públicas de proteção de dados também diminui, pois a autoridade não consegue ter acesso à realidade do tratamento de dados para poder editar normas que sejam efetivas para assegurar direitos[435]. Sem conhecimento e sem regulação, também não há debate público e atuação política para popularizar os riscos e os impactos do mercado de dados na vida individual[436].

Lembre-se que a autoridade adota uma perspectiva de regulação colaborativa e responsiva, que depende fortemente da contribuição dos agentes de tratamento para que ela possa ser efetiva. Limitando as possibilidades de fornecimento de informações, essa colaboração deixa de ser confiável e todo o propósito regulatório se esvai.

O controle de poder por parte da autoridade também é impactado, e em diferentes níveis. Há maior dificuldade de compreender como se dá o tratamento abusivo de dados e quem são os responsáveis pelos resultados produzidos. Desenvolvedores e programadores têm um papel relevante para a apuração de responsabilidades[437], mas com

---

[434] MARANHÃO, Juliano Souza de Albuquerque; JUNQUILHO, Tainá Aguiar; TASSO, Fernando Antônio. Transparência sobre o emprego de Inteligência Artificial no Judiciário: um modelo de governança. *Suprema - Revista de Estudos Constitucionais*, Distrito Federal, Brasil, v. 3, n. 2. p. 145–187, 2023. p. 150. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/231. Acesso em: 17 maio 2024.

[435] BUSUIOC, Madalina. Accountable artificial intelligence: holding algorithms to account. *Public Administration Review*, v. 81, n. 5. p. 825-836, Sept./Oct. 2021. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293 Acesso em: 18 abr. 2024.

[436] YU, Howard. GDPR Isn't Enough To Protect Us In An Age Of Smart Algorithms: Facebook and Google already face a legal complaint in the wake of the new data protection law, but the most precious data still isn't covered. *IMD - International Institute for Management Development*. 2018. Disponível em: https://www.imd.org/research-knowledge/data-analytics/articles/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms/. Acesso em: 03 abr. 2024.

[437] MITTELSTADT, Brent. Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, v. 1, 2019. p. 9-10. Disponível em: https://www.nature.com/articles/s42256-019-0114-4. Acesso em: 03 abr. 2024; LYONS, Henrietta; VELLOSO, Eduardo; MILLER, Tim. Conceptualising Contestability: Perspectives on Contesting Algorithmic Decisions. *Proceedings of the ACM Human-Computer Interaction*, Volume 5, CSCW1, Article 106, 2021. p. 1-25. Disponível em: https://dl.acm.org/doi/10.1145/3449180. Acesso em: 12 maio 2024.

a opacidade criada através dos segredos de negócio, torna-se impossível compreender em qual extensão esses atores concorreram para potenciais atos ilícitos[438].

Há também uma possibilidade de amplificação da datificação do comportamento humano, da transformação da vivência em commodities, e da exploração ostensiva dos dados pessoais[439]. Sem mecanismos suficientes para controlar como o poder é exercido, os agentes conseguem coletar e tratar cada vez mais dados pessoais, inexistindo mecanismos suficientes para avaliar (e reverter) a maneira como isso ocorre[440].

Surgem também maiores riscos de os agentes conseguirem impactar processos democráticos[441] e de interesse público[442]. Questões que envolvem a polarização e a desinformação são um exemplo relevante nesse sentido e, no mundo todo, vêm sendo objeto de debates sobre como aprimorar uma regulação que evite o espalhamento de notícias falsas[443]. A regulação desse debate não poderia passar ao largo da compreensão

---

[438] Impede, também, a possibilidade de os programadores se empoderarem em esforços maiores para desenvolverem sistemas mais transparentes, com menores extensões de opacidade incontrolável. É o que se chama de princípio da auditabilidade (*auditability*): "The principle of auditability states that algorithms should be developed to enable third parties to probe and review the behavior of an algorithm. Enabling algorithms to be monitored, checked, and criticized would lead to more conscious design and course correction in the event of failure" [O princípio da auditabilidade afirma que os algoritmos devem ser desenvolvidos para permitir que terceiros investiguem e revisem o seus resultados. Permitir que os algoritmos sejam monitorados, verificados e criticados levaria a um design mais consciente e a correções de curso em caso de falha] (DIAKOPOULOS, Nicholas; FRIEDLER, Sorelle. How To Hold Algorithms Accountable. *MIT Technology Review*, 17 nov. 2016, tradução livre. Disponível em: https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/. Acesso em: 2 maio 2024).

[439] TIMCKE, Scott. *Algorithms and the end of politics*: how technology shapes 21st-century American life. Bristol: Bristol University Press, 2021. p. 25-26.

[440] ZUBOFF, Shoshana. *The age of surveillance capitalism.* The fight for a human future at the new frontier of power. New York: Public Affairs, 2019. p. 193.

[441] Ver: DA EMPOLI, Giuliano. *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. São Paulo: Vestígio, 2020; IETA, Vânia Siciliano. O Impacto Eleitoral Resultante da Manipulação das Fake News no Universo das Redes Sociais: a Construção da Desinformação. *Revista Interdisciplinar do Direito* - Faculdade de Direito de Valença, [S. l.], v. 18, n. 1. p. 213–233, 2020. Disponível em: https://revistas.faa.edu.br/FDV/article/view/848. Acesso em: 01 maio 2024; MULHOLLAND, Caitlin; OLIVEIRA, Samuel Rodrigues. Uma Nova Cara Para a Política? Considerações sobre Deepfakes e Democracia. *Revista Direito Público*, v. 18. p. 368-396, 2021.

[442] Os casos de desinformação na crise da COVID-19 elucidam fortemente como a repercussão da desinformação transcende aspectos políticos e democráticos e impacta diretamente em crises coletivas, questões de saúde pública e interesses sociais. São conclusões trazidas por: HARTMANN, Ivar; MONTEIRO, Julia. Fake News no Contexto de Pandemia e Emergência Social: os Deveres e Responsabilidades das Plataformas de Redes Sociais na Moderação de Conteúdo Online: entre a Teoria e as Proposições Legislativas. *Revista de Direito Público*. v. 17, n. 94, p. 388-414, jul./ago. 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4607. Acesso em: 03 abr. 2024.

[443] ACEMOGLU, Daron. Harms of AI. *National Bureau of Economic Research*. 2021. p. 31-32. Disponível em: https://www.nber.org/papers/w29247. Acesso em: 18 nov. 2023; SUNSTEIN, Cass. *Republic.com*. Princeton, NJ: Princeton University Press, 2001; VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. The Spread of True and False News Online. *Science*, 359: 1146-1151. 2018. Disponível em: https://www.science.org/doi/10.1126/science.aap9559. Acesso em: 01 ago. 2023; ACEMOGLU, Daron; OZDAGLAR, Asu; SIDERIUS, James. Misinformation: Strategic Sharing, Homophily and Endogenous Echo Chambers. *NBER Working Paper* No. 28884. 2021.

sobre como funciona a distribuição do conteúdo, quais os impactos dos filtros-bolha e qual o nível de participação que os agentes têm nos resultados produzidos por algoritmos[444].

Contudo, além das dificuldades para apuração de responsabilidades e deveres de moderação[445], a questão profunda sobre como circula a desinformação é negligenciada, porque avaliações desse tipo demandariam acesso aos segredos de negócio, e eles são tratados, nos termos da lei e de precedentes judiciais, como sigilosos em níveis excessivamente amplos.

Existe então um conflito importante e que já foi mencionado anteriormente, que diz respeito às obrigações de segurança que a autoridade deve fornecer se pretende obter informações e conteúdos dos agentes de tratamento. Afinal, a autoridade também está sujeita a incidentes de segurança, e ela precisa assegurar que, se for requerer segredos de negócio dos agentes de tratamento, irá conseguirá manter essas informações fora do domínio público. Essa questão, contudo, não pode obstar a discussão sobre como a LGPD cria uma limitação das obrigações em relação à ANPD e quais as gravidades disso.

A questão, portanto, mostra que não só os segredos de negócio podem ser uma categoria jurídica inadequada para a realidade do mercado de dados pessoais, como também são tratados, pela LGPD, de forma a mitigar as possibilidades de controle, de autodeterminação informativa e de *accountability*.

---

[444] O tema também é desenvolvido por FELIPE, Bruno Farage da Costa; MULHOLLAND, Caitlin Sampaio. Filtro bolha e *big nudging*: a decomocracia participativa na era dos algorítimos. *Rev. direitos fundam. democ*., v. 27, n. 3. p. 06-18, set./dez. 2022. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/download/2275/753/6074. Acesso em: 14 mar. 2024. Os autores tratam como processos políticos são pautados por questões sutis que podem influenciar a opinião pública e determinar resultados de votações. Daí porque a forma como as redes sociais distribuem conteúdo se mostra tão relevante de ser compreendida, porque é a forma como a opinião pública, em grande medida, é construída nos dias de hoje.

[445] Discussões sobre a questão estão ocorrendo em diversas frentes, especialmente em âmbito legislativo (cita-se, como exemplo, o PL 592/2023, que pretende diminuir as possibilidades de moderação de conteúdo; e o PL 2.630/2020, que discute responsabilidade das plataformas pela circulação de conteúdo desinformativo e tenta estabelecer perspectivas de transparência), administrativo (o TSE, por exemplo, vem exercendo sua competência normativa para estabelecer diretrizes eleitorais sobre uso de inteligências artificiais e apurar veiculação de conteúdo desinformativo nas redes sociais) e judicial (por meio do Tema 987, o STF julga a constitucionalidade de dispositivo do Marco Civil da Internet que dispõe sobre responsabilidade do provedor e da plataforma), a fim de tentar apurar regimes de moderação de conteúdo e responsabilização das plataformas pelo espalhamento de *fake news*.

III.2.4 Acesso às explicações sobre o tratamento dos dados na comunicação de incidentes de segurança

As menções aos segredos de negócio da LGPD se estendem também aos dispositivos que tratam sobre a comunicação dos incidentes de segurança, notadamente no artigo 48, parágrafo 1º, inciso III, da Lei.

A segurança com os dados pessoais e suas repercussões na privacidade não foram inauguradas pela LGPD. Antes dela, o Marco Civil da Internet, em seus arts. 13 e 15, já estabelecia parâmetros mínimos de segurança da informação e precauções a serem adotadas pelos provedores[446]. Outras regulações setoriais também se manifestavam sobre o tema, a exemplo da Resolução 4.658/2018 do Banco Central do Brasil (BACEN), dispondo sobre política de segurança cibernética[447]; ou da Lei do Cadastro Positivo (Lei n. 12.414/2012), sobre a segurança das bases de dados utilizadas para risco de crédito[448].

Na LGPD, a segurança da informação é um dos eixos principiológicos centrais. Em diversos momentos (como nos arts. 6º, VIII, e 46), a norma detalha a relevância das obrigações de segurança e o comprometimento necessário por parte do agente para que ele empenhe esforços para evitar incidentes envolvendo dados pessoais. Se eles ocorrerem, a lei impõe o dever de mitigação máxima dos prejuízos e reforço nos padrões de segurança. Trata-se de uma preocupação não só com os dados na forma de ativos importantes para diversos setores econômicos, mas também com a grande variedade de prejuízos aos titulares que podem surgir caso sejam comprometidas as operações[449].

---

[446] SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023. p. RB-15.2.

[447] SOUZA, *op. cit*., p. RB-15.2.

[448] As considerações reforçam, inclusive, que a LGPD não inaugurou um sistema de proteção de dados dentro do ordenamento jurídico brasileiro. Isso fica evidente não só pelas leis anteriores sobre o tema, mas também sobre a postura de Tribunais brasileiros em tentar viabilizar, desde meados dos anos 90, a proteção a direitos de privacidade, de autodeterminação informativa, e de proteção de dados. Nesse sentido: CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023.

[449] FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 377; PRATA DE CARVALHO, Angelo. O papel da estratégia de segurança da informação nos mecanismos de compliance de dados: em busca de uma abordagem integrada. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021. p. 229.

Mais que uma preocupação genérica com a privacidade, os agentes de tratamento devem dedicar esforços para preservar diversos aspectos da vida individual e coletiva que podem ser impactados pelo uso dos dados pessoais[450]. Não sem motivo, a estrutura da LGPD valoriza e incentiva a criação de programas de adequação normativa (*compliance*), como forma de tentar dirimir potenciais riscos e incentivar os agentes a adotarem medidas de segurança que se alinhem aos propósitos da lei[451].

Dentre as preocupações com a segurança da informação, a LGPD estabelece providências imediatas a serem tomadas para contenção de riscos. Essas providências envolvem várias etapas que demandam organização interna dos agentes, elaboração de planos de resposta, adoção de medidas técnicas para isolamento de estruturas comprometidas, documentação de todas as operações realizadas e avaliação dos riscos[452].

Em seguida, inicia-se o processo de notificação do incidente. As disposições sobre essa etapa estão contidas no art. 48 da LGPD nas orientações gerais da ANPD[453], e estabelecem que algumas informações mínimas sobre o ocorrido devem ser fornecidas em até 2 (dois) dias úteis, a contar da data de ciência. A obrigação de prestar informações sobre o incidente é direcionada a destinatários diferentes: ao titular dos dados e à autoridade. A finalidade de cada notificação é distinta, e até mesmo considerando as capacidades técnicas de cada um, não se pode esperar que o nível de detalhamento da comunicação seja o mesmo em ambos os cenários.

Ao titular, a notificação tem o propósito de informá-lo sobre o ocorrido, dando ciência dos dados vazados e dos riscos envolvidos no incidente, além das providências tomadas para contenção da crise. Trata-se de uma maneira de garantir acesso aos dados em uma circunstância relevante, reforçando a transparência e a preocupação com as diferentes dimensões da autodeterminação informativa: o titular poderá reavaliar o fornecedor do serviço; adotar providências para se proteger de eventuais consequências

---

[450] FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de compliance e das políticas de proteção de dados. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021. p. 34.

[451] FRAZÃO, *op. cit*., p. 35.

[452] SOMBRA, Thiago Luís. Planos de Resposta a incidentes de segurança com dados pessoais e a construção de uma governança responsiva. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021. p. 611-614.

[453] BRASIL. Comunicação de incidente de segurança. *gov.br*. 2022. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 14 mar. 2024.

causadas pelo incidente; rever a necessidade de fornecer alguns de seus dados, dentre outras medidas[454].

Também se pode dizer que a obrigação de notificação do titular contribui para promover a conscientização sobre a importância dos dados pessoais e seu impacto no cotidiano. O objetivo é instituir e consolidar uma cultura de proteção de dados, além de criar um interesse político dentro do debate público sobre o tema[455].

No inciso III do parágrafo 1º do art. 48, contudo, as informações sobre medidas técnicas e de segurança utilizadas para a proteção de dados são limitadas, em relação ao titular, pelos segredos de negócio. Novamente sem considerar que os segredos deveriam envolver riscos concorrenciais e uma gestão da informação, a LGPD diminui expressamente as possibilidades da transparência sobre o que foi adotado pelo agente em uma situação grave, na qual os dados dos titulares foram expostos e seus direitos estão em risco. Longe de ser trivial, o cumprimento da obrigação de comunicar o titular é limitado por um juízo subjetivo do agente sobre quais são as informações que ele quer ou não enquadrar como segredos de negócio.

Rompe-se um fluxo de comunicação com o titular que deveria ser honesto e transparente, na medida em que ele deixa de ter acesso às informações que indicam os riscos aos quais ele está exposto. Além disso, os titulares são excluídos do processo de construção e desenvolvimento tecnológico, ignorando-se que seus feedbacks poderiam auxiliar na melhoria do sistema[456].

À autoridade, por sua vez, a comunicação tem o propósito de efetivamente avaliar os riscos, a gravidade e as consequências do incidente, além de verificar a pertinência e a

---

[454] De acordo com Sombra: "essa notificação deve conter informações específicas, tais como a descrição da natureza do incidente; o nome e os detalhes de contato do responsável pela proteção de dados ou outro ponto de contato; a descrição das prováveis consequências; a descrição das medidas tomadas ou propostas pelo responsável pelo tratamento para lidar com o incidente, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos; e o responsável pelo tratamento também deve fornecer orientação específica para os titulares se protegerem de possíveis consequências adversas do incidente, como a redefinição de senhas, atualização de sistemas, criptografia de dados, etc." (SOMBRA, Thiago Luís. Planos de Resposta a incidentes de segurança com dados pessoais e a construção de uma governança responsiva. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021. p. 617).

[455] SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023. p. RB-15.1.

[456] Existem dados mostrando como experiências dos titulares são importantes para reduzir vieses e fazer com que os padrões de segurança dos sistemas sejam aprimorados, prestigiando não só a qualidade das decisões automatizadas, como também a segurança dos dados envolvidos. Nesse sentido, ver: DIAKOPOULOS, Nicholas. Algorithmic Accountability Reporting: On the Investigation of Black Boxes. *Columbia Journalism School*. 2014. p. 30. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/D8TT536K/download. Acesso em: 03 nov. 2023.

efetividade das medidas adotadas pelos agentes para segurança da informação. Diante de sua capacidade técnica, a autoridade pode, se julgar pertinente, exigir que sejam adotadas medidas complementares, não só para dar maior ciência aos titulares sobre o ocorrido, mas também para que o agente utilize meios adicionais para contenção dos danos[457].

Quando destinada à autoridade, até mesmo diante da sua possibilidade em avaliar a gravidade do incidente e a compatibilidade das medidas adotadas, a expectativa é bem diferente daquela em relação ao titular. Espera-se que sejam compartilhadas informações técnicas detalhadas ao máximo, que elucidem amplamente a extensão do ocorrido e a fragilidade das medidas de segurança de dados que, porventura, tenham facilitado ou possibilitado a ocorrência do incidente. Indicar medidas técnicas de segurança é fundamental para que a ANPD possa compreender quais os esforços o agente efetivamente estava empenhando na proteção dos dados, e qual a sua extensão de responsabilidade.

Também é um conhecimento importante para avaliar a eficácia das soluções de contenção de danos, quais os riscos futuros e quais ajustes sistêmicos ou mudanças estruturais nas operações evitariam novos incidentes. Idealmente, a autoridade ainda poderia utilizar as informações sobre a eficácia das medidas de segurança para aprimorar sua regulação e fiscalização, além de orientar outros fornecedores do mesmo setor para evitar novos incidentes.

Essas atuações, contudo, tornam-se igualmente limitadas pelos segredos de negócio. De forma injustificada, e mesmo diante de um momento de crise e risco de violações de direitos, o agente continua podendo escolher quais informações compartilhar com a ANPD.

É interessante que, pensando no uso dos segredos de negócio no mercado, uma das vantagens que se defende é justamente o prestígio à segurança da informação e a possibilidade que o sigilo tem de auxiliar na proteção da privacidade sobre quais dados estão armazenados[458]. Todavia, esse argumento se enfraquece quando o agente utiliza o mesmo instituto para não dar completa ciência aos titulares e aos agentes sobre qual a extensão dos riscos de suas operações e quais medidas foram adotadas para preservá-las.

---

[457] SOMBRA, Thiago Luís. Planos de Resposta a incidentes de segurança com dados pessoais e a construção de uma governança responsiva. *In*: CUEVA Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021. p. 617.

[458] PASQUALE, Frank A. Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries. *Northwestern University Law Review*. 1 out. 2010. p. 165. Disponível em: https://ssrn.com/abstract=1686043. Acesso em: 22 abr. 2024.

Na prática, portanto, os titulares e as autoridades passam a depender dos agentes para acessarem esclarecimentos sobre incidentes de segurança e problemas com as operações. Para além de dificultar a concretização da transparência, os segredos de negócio limitam mais uma vez a autodeterminação informativa dos titulares e a atuação da autoridade regulatória no exercício de importantes competências para efetivação de um sistema de proteção de dados pessoais[459].

III.3 UMA LGPD PROCEDIMENTAL E AS PREOCUPAÇÕES COM O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

As reflexões trazidas até aqui constituem críticas expressivas à LGPD e que podem ser adicionadas às reflexões sobre a natureza procedimental das leis de proteção de dados.

Ainda que seu propósito seja a proteção de dados pessoais, estudos vêm mostrando que as leis de proteção de dados possuem "enunciação de um conjunto de requisitos que está mais inclinado a apoiar quem deseja explorar os dados do que em relação a quem os titulariza"[460]. Para corroborar essa hipótese, são mapeadas dificuldades na concretização da regulação da proteção de dados que decorrem tanto da influência exercida pelos agentes econômicos, como das dificuldades que a regulação da matéria pressupõe.

---

[459] "While model transparency is in and of itself unlikely to resolve all informational problems pertaining to AI algorithm use, a reliance on proprietary models in the public sector engenders and exacerbates a heavy dependence on private providers truthfully reporting on their models' functioning (and malfunctioning), highly problematic given the considerable financial and reputational costs at stake shaping disclosure incentives. Without model transparency, independent third parties will not be able to independently audit algorithm functioning (for instance, by testing algorithm operation and predictions on different data) and/or will be left guessing key features when attempting to reverse-engineer algorithm functioning, while public sector bodies will be left unable to comply with their administrative disclosure duties towards affected citizens" [Embora a transparência do modelo, por si só, seja improvável de resolver todos os problemas informativos relacionados ao uso de algoritmos de IA, a dependência de modelos proprietários no setor público gera e exacerba uma forte dependência de provedores privados relatarem de forma verídica sobre o funcionamento (e mau funcionamento) de seus modelos, o que é altamente problemático, dada a considerável quantidade de custos financeiros e de reputação em jogo que moldam os incentivos para a divulgação. Sem transparência do modelo, terceiros independentes não serão capazes de auditar independentemente o funcionamento do algoritmo (por exemplo, testando a operação e as previsões do algoritmo em diferentes dados) e/ou ficarão apenas especulando sobre as principais características ao tentar reverter a engenharia do funcionamento do algoritmo, ao passo que os órgãos do setor público ficarão impossibilitados de cumprir seus deveres de divulgação administrativa para com os cidadãos afetados] (BUSUIOC, Madalina. Accountable artificial intelligence: holding algorithms to account. Public Administration Review, v. 81, n. 5. Sept./Oct. 2021. p. 829, tradução livre. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293. Acesso em: 18 abr. 2024.

[460] BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 79.

Análises históricas mostram que as leis evoluíram para diminuir cada vez mais o espaço decisório dos titulares sem diminuir, em paralelo, as possibilidades de exploração das suas informações pessoais[461] e a expressividade do fluxo informacional[462]. Os agentes hoje conseguem garantir o *compliance* necessário para legitimar suas atividades sem precisarem envolver o titular dos dados, ou até sem precisar dar a ele ciência das operações realizadas[463]. As autoridades podem até opinar na forma como se dá o tratamento, mas fazem isso por meio de informações limitadas e análises de risco que são enviesadas, uma vez que fornecidas pelos próprios agentes[464].

Outra perspectiva avalia a inexequibilidade de diversas pretensões que estão inseridas nas leis de proteção de dados à revelia de estudos profundos que já existiam sobre o tema. É o caso da base legal do consentimento e da execução de contrato, que colocam o titular em excessiva posição negocial frente ao agente[465], mesmo diante da grande assimetria, das limitações de racionalidade, da posição de vulnerabilidade do titular e dos impactos coletivos do tratamento dos dados.

O uso de conceitos excessivamente abertos dentro das leis de proteção de dados também pode trazer conflitos. Se por um lado serve para atender à dinamicidade com que as tecnologias evoluem, criando uma estrutura principiológica transponível para diversas

---

[461] QUELLE, Claudia. *Privacy, proceduralism and Self-Regulation in Data Protection Law*. Teoria e Critica della Regolazione Sociale. 2018. p. 98. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3139901. Acesso em: 16 set. 2023.

[462] Daniel J. Solove foi um dos primeiros autores a trazer essa reflexão, ao falar sobre os custos do discurso do "eu não tenho nada a esconder"(*I've got nothing to hide*). Como destaca em sua tradicional publicação, violações a direitos de privacidade não afetam somente os indivíduos, mas sim aspectos variados da vida humana, incluindo a percepção coletiva sobre o direito e os esforços que devem ser empregados pelos agentes públicos para preservá-lo, ainda que em casos difíceis e a *contrario sensu* (SOLOVE, Daniel J. I've got Nothing to Hide and other misunderstandings of privacy. *San Diego Law Review*, vol. 44, 2007. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565. Acesso em: 25 ago. 2022). Depois dele, diversos outros autores destacaram que além dos impactos sociais que a percepção do direito de privacidade em si tem, há também que se falar que os dados não dizem respeito somente a uma pessoa: provavelmente, um titular que autoriza divulgação de suas informações está também divulgando dados sobre seus amigos, familiares ou outros, causando impactos que transcendem significativamente a sua esfera individual. É o que diz Carissa Véliz (VÉLIZ, Carissa. *Privacidade é poder*. Por que e como você deveria retomar o controle de seus dados. São Paulo: Editora Contracorrente, 2021), mas também Daron Acemoglu (ACEMOGLU, Daron. Harms of AI. *National Bureau Of Economic Research*, Cambridge, 2021. p. 6. Disponível em: https://www.nber.org/papers/w29247. Acesso em: 09 set. 2023), Anita Allen (ALLEN, Anita. L. An Ethical Duty to Protec One's Own Information Privacy. *All Faculty Scholarship*. 451, 2013. Disponível em: https://scholarship.law.upenn.edu/faculty_scholarship/451. Acesso em: 04 jan. 2024) e outros.

[463] QUELLE, Claudia. Privacy, proceduralism and Self-Regulation in Data Protection Law. Teoria e Critica della Regolazione Sociale. 2018. p. 101-102. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3139901. Acesso em: 16 set. 2023.

[464] QUELLE, *op. cit*., p. 103.

[465] LINDOSO, Maria Cristine. Comentários sobre o consentimento: Principais aspectos e preocupações. *In*: PINHO, Anna Carolina (org.). *Manual de Direito na Era Digital*. Indaiatuba, SP: Editora Foco, 2023. p. 158-167.

circunstâncias, por outro se mostra insuficiente para criar obrigações que impõem aos agentes a garantia do acesso do titular ao que ele precisa para exercer sua autodeterminação informativa[466].

O princípio da transparência se enquadra nessa crítica: desenhada em termos genéricos, o princípio por vezes cria uma expectativa de racionalidade que não existe no campo da proteção de dados[467]. Pode-se defender que o conceito é, por si só, inadequado ao dinâmico mercado das informações pessoais[468], e que a forma como ele é proposto pelas regulações é insuficiente para delimitar a extensão obrigacional dos agentes de tratamento para que se considerem transparentes as operações.

Esses são elementos que subsidiam a crítica de que a LGPD e as normas de proteção de dados em geral são essencialmente procedimentais, que mais servem para legitimar a existência do mercado de tratamento de dados do que efetivamente proteger a privacidade e outras garantias dos titulares[469]. Sabe-se que as leis costumam ter como propósito a combinação dessas duas funções, mas a crítica é que pensando na perspectiva do titular de dados, ele tem seus direitos fragilizados e acaba sendo desprestigiado pela norma.

As reflexões que foram feitas sobre os segredos de negócio na LGPD podem corroborar com essa visão. Ao que parece, não houve muita reflexão sobre todas as preocupações que podem surgir ao tratar os elementos do mercado de dados pessoais como segredos de negócio. Além da possível impropriedade da categoria jurídica, dados pessoais possuem dimensão existencial, e o seu uso pode trazer repercussões que somente podem ser administradas e controladas com níveis amplos de transparência – o que não é compatível com o sigilo atribuído aos segredos.

---

[466] ALBERS, Marion. A complexidade da proteção de dados. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 10, n. 35. 2016. p. 29-32. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/93. Acesso em: 4 maio 2024.

[467] DONEDA, Danilo; ALMEIDA, Virgílio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20. p. 60-63, 2016. p. 60. Disponível em: https://www.researchgate.net/publication/305801954_What_Is_Algorithm_Governance. Acesso em: 12 nov. 2023.

[468] ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Midia & Society*, 20(3), 2018. p. 11. Disponível em: https://doi.org/10.1177/1461444816676645. Acesso em: 12 out. 2023.

[469] "Além de permitir o desenvolvimento de novos bens juridicamente tutelados, os direitos fundamentais permitem uma compreensão multidimensional das reservas e das regulamentações. As normas jurídicas não só limitam liberdades. Elas também podem, antes de tudo, criar liberdades, torná-las concretas e influenciar suas condições e pré-requisitos sociais. O direito referente à proteção de dados deve estar fundamentado nas diversas funções e diversas formas do direito" (ALBERS, Marion. A complexidade da proteção de dados. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 10, n. 35. 2016. p. 39. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/93. Acesso em: 4 maio 2024).

Para além disso, a lei fez uma série de ressalvas a garantias e direitos dos titulares, limitando suas extensões a uma proteção primária dos segredos de negócio. O mesmo ocorre para as autoridades: a extensão de suas competências parece estar vinculada a uma disposição anterior dos agentes em decidirem o que querem ou não fornecer em termos de explicações, diante da possibilidade de se recusarem em fazê-lo em razão das ressalvas dos segredos de negócio.

A leitura dos dispositivos legais acaba sugerindo que os segredos de negócio têm proteção talvez até prioritária dentro da lei, e que no lugar de prestigiar a proteção de dados pessoais e as garantias individuais, prestigiam-se os interesses dos agentes de tratamento por meio dos segredos de negócio. Essa percepção se reforça com a inclusão, no rol de competências da ANPD, da proteção aos segredos de negócio (art. 55-J, II, LGPD).

Pensar como a LGPD cria uma estrutura normativa que prestigia os interesses do mercado resgata reflexões feitas no início deste trabalho sobre o papel do Direito na proteção dos interesses dos agentes econômicos. Não é possível afirmar que a LGPD é resultado exclusivo de interferências dos agentes de tratamento, que tentaram torná-la uma estrutura excessivamente protetiva dos segredos de negócio. Mas sabe-se que essas interferências ocorrem e no mercado em questão as possibilidades de exercê-las explorando dados pessoais e tecnologias podem ser poderosas e por vezes efetivas.

Independentemente de como foi o processo, o resultado é uma norma que acaba reproduzindo uma distorção do Direito, qual seja, a de fornecer a estrutura normativa necessária para que os agentes econômicos persigam seus interesses. A possibilidade de os agentes escolherem entre tutela jurídicas mais transparentes (como da propriedade intelectual ou dos direitos autorais) e segredos de negócio já constitui um uso do Direito em benefício dos interesses privados[470]. A estrutura da LGPD cria mais uma distorção, pois reforça a possibilidade de os segredos de negócio comporem o mercado de dados pessoais e excepcionarem uma série de garantias individuais.

Percebe-se que o Direito acaba corroborando com um modelo de dominação capitalística[471] que pode ser muito agressivo no contexto dos dados pessoais, criando uma

[470] Pistor também falou desse processo, mostrando como a possibilidade de escolha das leis e os conflitos que surgem nesse processo acabam favorecendo os interesses dos agentes privados (PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019. p. 135).

[471] Pachukanis já dizia como o Direito pode reproduzir estruturas de dominação capitalística, transcrevendo para a forma jurídica as relações sociais objetivas (PACHUKANIS, Evguiéni B. *Teoria Geral do Direito e Marxismo.* São Paulo: Editora Acadêmica, 1988. p. 41). Essa crítica é explorada recentemente por

série de impactos já descritos e intensificando processos de comodificação do ser humano[472].

Para importantes autores, sempre serão frustradas as tentativas de fortalecer a proteção de dados[473] e de modificar a lógica do acúmulo informacional cada vez maior[474]. Questões como a origem essencialmente discriminatória do desenvolvimento tecnológico[475], da extensão dos processos de datificação[476], e da crescente dependência dos titulares em relação às plataformas sociais[477], fortalecem essa descrença.

Repensar a estrutura da proteção de dados no mundo, para que ela se torne efetiva, impõe enormes desafios. Até mesmo os desafios específicos da LGPD, a fim de torná-la uma norma menos procedimental, já se mostram significativos e transcendem o propósito do presente trabalho. Contudo, especificamente em relação aos conflitos de transparência e segredos de negócio, é possível criar algumas premissas para que as interpretações dos dispositivos legais possam se tornar compatíveis com a garantia fundamental de proteção de dados. São essas reflexões que se pretende fazer a seguir.

ALAPANIAN, Silvia. A crítica marxista do Direito: um olhar sobre as posições de Evgeni Pachukanis. *Semina*: *Ciências Sociais e Humanas*, Londrina, v. 26. p. 15- 26, set. 2005. p. 17. Disponível em: https://ojs.uel.br/revistas/uel/index.php/seminasoc/article/view/3794/3050. Acesso em: 04 maio 2024. Também: NAVES, Márcio Bilharinho. *Marx*: Ciência e Revolução. São Paulo: Moderna, Campinas, SP, Editora da Universidade de Campinas, 2000. p. 40-42.

[472] ZUBOFF, Shoshana. Caveat Usor: Surveillance Capitalism as Epistemic Inequality. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020. p. 193.

[473] ZUBOFF, Shoshana. Big Other: Capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda *et al*. (org.). *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 18; ZUBOFF, Shoshana. *The age of surveillance capitalism.* The fight for a human future at the new frontier of power. New York: Public Affairs, 2019. p. 193; GIL, Gabriel de Siqueira; HIRSCHFELD, María Noel C. Extrativismo hi-tech e expansão capitalista no século XXI: uma breve contribuição para a crítica latino-americana na era do colonialismo de dados. *In*: PARANÁ, Edemilson; KAMINSKI, Ricardo S. (org.). *Tecnologia e Desenvolvimento nas Américas*: novas fronteiras e dilemas do capitalismo contemporâneo. Curitiba, 2021.

[474] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 16.

[475] Essa questão foi bem exposta por Klaus Swab: o desenvolvimento tecnológico que marca a Quarta Revolução Industrial é profundamente desigual no mundo, já que uma parte significativa da população mundial sequer tem acesso à energia elétrica e mais de 4 bilhões de pessoas no mundo nunca teriam tido tal acesso (em 2016, quando o livro foi publicado). Assim, apesar de ser um movimento inevitável de profundas transformações, ele não ocorre de forma igualitária e homogênea, e também não prestigia o desenvolvimento de regiões de maior necessidade (SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016. p. 36).

[476] MEJIAS, Ulises A.; COULDRY, Nick. Datafication. *Internet Policy Review*, 8, 2019. p. 3. Disponível em: https://policyreview.info/concepts/datafication. Acesso em: 11 nov. 2023.

[477] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 38; CAMPOS, Ricardo. *Metamorfoses do direito global*: Sobre a interação entre direito, tempo e tecnologia. São Paulo: Editora Contracorrente, 2022. p. 280.

CAPÍTULO IV – REFLEXÕES SOBRE AS POSSIBILIDADES DE CONCILIAR A PROTEÇÃO AOS SEGREDOS DE NEGÓCIO COM A PROTEÇÃO DE DADOS PESSOAIS

IV.1 DIFICULDADES COM A CATEGORIA DOS SEGREDOS DE NEGÓCIO NO MERCADO DE DADOS PESSOAIS

Os segredos de negócio podem ser considerados um instrumento jurídico importante para preservação da inovação. Contudo, para a realidade e as complexidades do mercado de dados pessoais, seu uso envolve questões complexas que precisam ser levadas em consideração.

A principal dificuldade envolve a tensão entre transparência e sigilo que, no mercado de dados, possui impactos muito significativos. Existem dúvidas de se o mercado de dados pessoais sequer deveria existir e se é legítimo tratar a experiência humana como um produto. Mesmo se superado esse conflito, renunciar à transparência pode ser sinônimo de renunciar à autodeterminação informativa, ao controle de poder, à *accountability*, à regulação, sucumbindo, em última análise, a um ambiente onde garantias fundamentais como a da proteção de dados pessoais são irrelevantes.

A tensão entre transparência e sigilo pode trazer à tona discussões muito mais complexas sobre o mercado de dados pessoais, que vão desde a sua legitimidade até as suas possibilidades de controle. Essa tensão não tem, portanto, soluções simples. Mas isso não impede um exercício propositivo.

Uma primeira consideração seria no sentido de que o mercado de dados pessoais, ainda que traga inúmeros benefícios à vida humana, hoje se desenvolve em níveis abusivos de exploração dos dados pessoais. A intensidade crescente com que se dá a vigilância deveria suscitar preocupações muito maiores. Como isso não ocorre, o debate público sobre o tema é fortemente asfixiado e a falta de protagonismo das autoridades de proteção de dados passa despercebida.

Outra consideração é que a voracidade com que os dados são coletados e tratados certamente contribuiu para que as operações automatizadas se tornassem ainda mais opacas. Isso se dá em razão dos processos inerentes ao desenvolvimento tecnológico, das dificuldades técnicas em criar parâmetros razoáveis de compreensão e das escolhas dos agentes econômicos. Independentemente de como se cria a opacidade, ela é crescente e afasta as possibilidades de aproximação dos titulares e das autoridades à tomada de decisão autônoma.

Também se deve considerar que muitas categorias jurídicas são impróprias para serem transportadas para o mercado de dados pessoais. Discussões sobre a forma de tributação dos serviços prestados por plataformas[478]; a forma de moderação do conteúdo[479]; direitos autorais e proteção das criações[480] são apenas alguns exemplos nesse sentido. Ao longo do trabalho, buscou-se focar nos segredos de negócio e na possibilidade que os agentes de tratamento têm de escolher enquadrar alguns elementos de suas operações como segredos de negócio, o que implica em uma série de outras dificuldades, porque acaba trazendo como consequência a possibilidade de se criar uma opacidade adicional.

Isso para dizer que, especificamente quanto ao problema que foi exposto aqui, não existe um esforço único que deva ser empenhado e que irá solucionar o problema. Mas ignorar a forma como a datificação da experiência humana está crescendo; não buscar meios de reverter a crescente opacidade; e transportar cegamente categorias jurídicas já existentes para o mercado de dados, certamente não são os melhores caminhos a serem perseguidos.

Na questão específica que foi explorada ao longo do trabalho, deve-se refletir sobre o interesse coletivo em manter a possibilidade de escolha dos agentes de tratamento em definir como segredos de negócio o que eles desejem. Leis específicas que delimitem os níveis de proteção ou novas tutelas jurídicas pensadas exclusivamente para o mercado de dados pessoais podem ser soluções que melhor conciliam os interesses dos agentes de tratamento com perspectivas concretas de proteção de dados pessoais.

---

[478] Sobre o tema, ver: RUSSO, Raffaele. Reflections about the Implications of Platforms and Technology for Taxation and Taxpayers' Rights. *In*: WEBER, Dennis (ed.). *The Implications of Online Platforms and Technology on Taxation*. The Netherlands: IBFD, 2023.

[479] Questões nesse sentido são trazidas por: HARTMANN, Ivar; MONTEIRO, Julia. Fake News no Contexto de Pandemia e Emergência Social: os Deveres e Responsabilidades das Plataformas de Redes Sociais na Moderação de Conteúdo Online: entre a Teoria e as Proposições Legislativas. *Revista de Direito Público*. v. 17, n. 94, p. 388-414, jul./ago. 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4607. Acesso em: 03 abr. 2024; CUEVA, Ricardo Villas Bôas. Alternativas para a remoção de fake news das redes sociais. *In*: MENDES, Gilmar Ferreira; MORAIS, Carlos Blanco. *Reforma do Estado Social no contexto da globalização*. Rio de Janeiro: FGV Projetos, 2018. p. 79-91; GRIMMELMANN, James. The virtues of moderation. *Yale Journal of Law & Technology*, 2015, v. 17. p. 48. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1110&context=yjolt. Acesso em: 08 set. 2021.

[480] Ver: GAON, Aviv H. *The Future of Copyright in the Age of Artificial Intelligence*. Elgar Law, Technology and Society series, 2021; LESSIG, Lawrence. *Free culture*: the nature and future of creativity. Penguin Books, 2004.

Contudo, enquanto essas novas formas não são pensadas, deve-se pensar na melhor forma de interpretar a LGPD para que se possa prestigiar a proteção aos segredos de negócio e também o direito fundamental à proteção de dados pessoais.

IV.1.1 Preservando os segredos de negócio e tentando conciliá-los com a transparência

Priorizar o respeito aos direitos fundamentais[481] impõe que a interpretação das normas infraconstitucionais deva respeitar uma vontade social maior[482], de modo que a força normativa necessária à condução do Direito infraconstitucional esteja em um sentido que interesse à sociedade[483]. Isso implica reconhecer que toda a realidade política e social está direcionada a um mesmo fluxo[484], qual seja, o de respeito aos direitos subjetivos e às garantias institucionais de pluralidade e diversidade.

No mercado de dados pessoais, quer dizer que os dispositivos da LGPD devem ser lidos no sentido de concretizar a vontade constitucional, especialmente a partir da Emenda Constitucional n. 115, de 10 de fevereiro de 2022 e de decisões do STF no julgamento das ADIs n. 6.387 389, 6.390, 6.393 e 6.388[485].

---

[481] Segundo Pistor: "Not only capital is coded in law, but so too are other entitlements; it is a matter of social choice to whom to leave the final say about which assets deserve special status in law. On balance, privately coded capital has won the day, time and again, although not with periodic convulsions that have forced the hand of legislatures to rebalance the playing field or at least to mitigate the losses that less well protected individuals face" [Não apenas o capital é codificado na lei, mas também outros direitos; é uma questão de escolha social a quem deixar a palavra final sobre quais ativos merecem status especial na lei. No geral, o capital codificado de forma privada tem prevalecido, repetidas vezes, embora não sem convulsões periódicas que tenham forçado as mãos dos legisladores a reequilibrar o jogo ou, pelo menos, a mitigar as perdas enfrentadas por indivíduos menos protegidos] (PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019, p. 217, tradução livre). Adiante, também prossegue Pistor: "The fact that capital cannot rule without law does not imply the reverse, namely that law could not be used to protect other interests on par with capital. One could, for example, harness the code and its modules to empower others who have experienced the empire of law mostly from below: as losers in the battles over enclosure of land, knowledge, or nature, as mostly involuntary risk bearers of a financial system that primarily benefits the one percent at the top, or as workers in firms whose expectations to future income are denied the same protection that shareholders' expectations to future profit have readily received" [O fato de que o capital não pode governar sem a lei não implica o inverso, ou seja, que a lei não poderia ser usada para proteger outros interesses em pé de igualdade com o capital. Poder-se-ia, por exemplo, utilizar o código e seus módulos para capacitar outros que experimentaram predominantemente o império da lei de baixo para cima: como perdedores nas batalhas sobre a apropriação de terras, conhecimento ou natureza, como portadores de risco predominantemente involuntários de um sistema financeiro que beneficia principalmente o um por cento no topo, ou como trabalhadores em empresas cujas expectativas de renda futura são negadas a mesma proteção que as expectativas de lucro futuro dos acionistas prontamente receberam] (PISTOR, *op. cit*., p. 229, tradução livre).

[482] HESSE, Konrad. *A força normativa da constituição*. Tradução: Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris Editor, 1991. p. 19.

[483] TEUBNER, Gunther. Societal constitutionalism: alternatives to state-centered constitutional theory. *In*: JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther (eds.). *Constitutionalism and transnational governance*. Oxford: Hart Publishing, 2004. p. 3-28.

[484] HESSE, *op. cit*., p. 34.

[485] Cf. STF, Rel. Min. Rosa Weber, j. 07 maio de 2020.

O direito fundamental à proteção de dados pessoais se insere em um contexto que se relaciona com a privacidade, mas que não se limita a ela, uma vez que o atual mercado se desenvolveu com a exploração ostensiva das informações privadas. O direito fundamental à proteção de dados engloba também reflexões sobre a situação de vulnerabilidade dos indivíduos frente ao poder acumulado pelos agentes; reflexões sobre a preservação da personalidade e sobre a dimensão coletiva dos direitos de privacidade[486]. Engloba preocupações sobre uma nova forma de expressão da dignidade da pessoa humana[487] e que deve se manifestar nas normas infraconstitucionais e interpretações jurisprudenciais, a fim de que todas as atividades envolvendo dados passem a considerar um parâmetro mais amplo de preocupação com a dimensão existencial das operações[488].

E apesar de o direito de proteção de dados como um direito fundamental marcar a sua tutela constitucional de forma autônoma, não se abandona a necessidade de medidas ativas para a preservação e o exercício dessa garantia[489], dentre as quais se deve incluir "um conjunto de prerrogativas traduzidas por um regime jurídico reforçado e uma

---

[486] SARLET, Ingo Wolfgang; SARLET, Gabrielle Bezerra Sales. Proteção de dados pessoais como direito fundamental autônomo na Constituição Brasileira de 1988 – a contribuição de Danilo Doneda. In: CUEVA, Ricardo Villas Bôas ... [et al.]. *Direitos fundamentais e novas tecnologias*: homenagem ao professor Danilo Doneda. 1ª ed. Rio de janeiro: GZ, 2024.

[487] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. *Direitos Fundamentais & Justiça*, ano 13, n. 41. p. 183-212, jul./dez. 2019. p. 206. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/811. Acesso em: 14 mar. 2024.

[488] Trata-se do julgamento da ADI 6.387 MC-Ref/DF, julgamento em 6 e 7 de maio de 2020, de relatoria da Ministra Rosa Weber, julgada em conjunto com as ADIs 389, 6.390, 6.393, 6.388 e 6.387. Cabe destacar o seguinte trecho das conclusões do Supremo: "A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5o, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data como instrumento de tutela material do direito à autodeterminação informativa. [...] Considerando que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e de privacidade. Todas essas transformações tecnológicas ensejam aquilo que, nas palavras de Bruno Bioni, é identificado como verdadeiro cenário de hipervulnerabilidade no regime de proteção de dados pessoais, que se desdobra em traços vulnerantes peculiares sob as perspectivas informacional, técnica e econômica (BIONI, *op. cit*., p. 164). Desse modo, a afirmação da força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade indissociável de proteção à dignidade da pessoa humana ante a contínua exposição dos indivíduos aos riscos de comprometimento da autodeterminação informacional nas sociedades contemporâneas. É importante ainda assentar que essa afirmação de um novo direito fundamental não resulta de um criacionismo jurisprudencial dissociado da própria tradição jurídica brasileira, naquilo que transformada pelos recentes influxos legislativos".

[489] MENDES, Laura Schertel. Decisão Histórica do STF reconhece direito fundamental à proteção de dados pessoais: Novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. *JOTA*. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 10 mar. 2024.

dogmática sofisticada"[490]. Também implica interpretar normas abertas e resolver eventuais antinomias, prestigiando a concretização do direito fundamental à proteção de dados[491].

Para prestigiar o direito fundamental à proteção de dados, deve-se prestigiar a transparência. É por meio desse princípio que se consolidam as posições jurídicas subjetivas do titular de dados, delimitando-se a extensão do que é a proteção de dados[492]. Também é por meio da transparência que se torna possível exercer o controle de poder dos agentes de tratamento[493] e dimensionar as repercussões coletivas que podem ser causadas pelas operações[494].

Mais do que um valor ético a ser perseguido, a transparência é uma norma finalística[495] que cria deveres exequíveis[496] e condiciona todo o comportamento dos

---

[490] SARLET, Ingo Wolfgang. Proteção de Dados Pessoais como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo para a Construção de uma Dogmática Constitucionalmente Adequada. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 14, n. 42. 2020. p. 214. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 26 maio 2024.

[491] LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 23. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024; ALBERS, Marion. A complexidade da proteção de dados. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 10, n. 35. 2016. p. 33-35. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/93. Acesso em: 4 maio 2024. Também se destaca o trabalho de SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com*. Rio de Janeiro, ano 8, n. 1, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 7 abr. 2024, que demonstra a necessidade de prestígio às garantias dos titulares de dados como decorrência da proteção integral e da dignidade da pessoa humana.

[492] SARLET, Ingo Wolfgang. Proteção de Dados Pessoais como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo para a Construção de uma Dogmática Constitucionalmente Adequada. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 14, n. 42. 2020. p. 195-196. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 26 maio 2024. O autor menciona os arts. 17, 18, 20 e 21 da LGPD como expressões dessa dimensões subjetivas do direito fundamental à proteção de dados. E ambos os dispositivos trazem expressões da transparência e do acesso aos dados pessoais.

[493] COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019. p. 270-271.

[494] Nesse aspecto, além da considerações que já foram trazidas, é importante reforçar que muitos algoritmos são utilizados em substituição a agentes públicos e em processos de tomada de decisão que impactam fortemente escolhas individuais. Por isso, a dimensão coletiva da proteção de dados mostra-se cada vez mais relevante (RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. 2020. p. 87. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 2024).

[495] Esse é o conceito de princípio adotado por ÁVILA, Humberto. *Teoria dos Princípios*: da definição à aplicação dos princípios jurídicos. 4. ed. São Paulo: Editora Malheiros, 2022. p. 70.

[496] Como defende Brent Mittelstadt, o desenvolvimento de tecnologias, especialmente inteligências artificiais, focado somente em princípios encontra limitações importantes porque (i) não existem deveres fiduciários para quem desenvolve IA (qualquer um pode fazê-lo em suas casas); (ii) não existem normas que regulem a profissão (novamente, sequer é necessário ser um desenvolvedor para ter acesso à tecnologia); (iii) não existem métodos comprovados que, historicamente, consigam incorporar os princípios à prática; e (iv) não existem mecanismos de *accountability* efetivos em relação à responsabilização de quem

agentes no mercado, a pondo de condicionar também toda a construção dos esforços regulatórios no setor. Quer dizer, então, que mesmo quando se dispõe sobre segredos de negócio, a avaliação da melhor interpretação deverá considerar como compatibilizar direitos, a fim de prestigiar a transparência[497], pois é ela que assegura que a proteção de dados pessoais está sendo observada.

Não se ignora que a proteção aos segredos de negócio foi inserida na LGPD como um dos deveres da autoridade, assim como são eixos centrais da lei a inovação, o desenvolvimento tecnológico e a livre iniciativa. Contudo, a concretização desses deveres e eixos centrais deve se dar à luz do direito à proteção de dados, considerando a imposição que se cria em razão da natureza fundamental do direito à proteção de dados pessoais.

Isso faz com que demais objetivos sejam secundários ou complementares ao verdadeiro propósito da LGPD, que deve ser, então, o de assegurar a proteção de dados. Especificamente sobre o tema em questão, quer dizer que conflitos envolvendo segredos de negócio deverão resultar em escolhas que prestigiem os interesses dos titulares de dados e da coletividade à luz da proteção de dados pessoais, e não somente os interesses dos agentes de tratamento.

Em outras jurisdições, o conflito sobre a proteção de dados e os segredos de negócio não é menos complexo. No entanto, os esforços para delimitar quais são os verdadeiros propósitos da lei são mais efetivos e criam condições melhores para obstar condutas dos agentes de tratamento que tornem a proteção aos segredos de negócio um método de ampliação das opacidades.

No RGPD, a proteção aos segredos de negócio é um fundamento da lei, mas há expressa menção no sentido de que seu uso não pode limitar objetivamente o exercício da explicabilidade direcionada ao titular dos dados[498]. Através do Considerando 39, os direitos dos titulares de conhecerem como se dão as operações são detalhados de forma a

---

desenvolve essas tecnologias. Por isso, cabe à regulação transformar esses princípios em obrigações exequíveis que prestigiem a proteção de dados e a tutela de interesses relacionados à privacidade, sob risco de se desenvolverem inteligências artificiais e sistemas completamente voltados aos interesses do capital (MITTELSTADT, Brent. Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, v. 1, 2019, p. 2. Disponível em: https://www.nature.com/articles/s42256-019-0114-4. Acesso em: 03 abr. 2024).

[497] A ideia foi sugerida por Pasquale já em 2008: PASQUALE, Frank A.; BRACHA, Oren. Federal Search Commission? Access, Fairness and Accountability in the Law of Search. *Cornell Law Review*, setembro 2008. U of Texas Law, Public Law Research Paper No. 123, Seton Hall Public Law Research Paper No. 1002453. Disponível em: https://ssrn.com/abstract=1002453. Acesso em: 27 abr. 2024. p. 29-31.

[498] EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, v. 16. n. 18, maio 2017. p. 53. Disponível em: https://ssrn.com/abstract=2972855. Acesso em: 10 abr. 2024.

assegurar que nenhuma dessas informações poderá deixar de ser fornecida pelo agente[499]. O Recital 63 do RGPD igualmente não permite a interpretação de que a proteção dos segredos de negócio poderá prevalecer em relação à proteção de dados[500].

Além da previsão legal, os tribunais interpretam a legislação para que, mesmo diante da ausência de obrigação expressa em compartilhar segredos de negócio, os agentes sejam obrigados a fornecer um conjunto detalhado de conteúdos e explicações, especialmente em casos mais sensíveis (como de análise de crédito)[501]. Essa descrição mais minuciosa retira o espaço do agente de escolher quais conteúdos ele quer ou não compartilhar e o que ele enquadra ou não como segredo de negócio[502].

No *Artificial Intelligence Act* europeu foi incorporado o princípio geral da transparência para regulação de inteligências artificiais, o que implica conferir níveis de explicabilidade que igualmente não são limitados pelos segredos de negócio[503]. A União Europeia também tem uma diretiva específica de tutela dos segredos de negócio, que não foi elaborada pensando na transparência algorítmica, mas que contém normas que

---

[499] Cf. Considerando 39, RGPD: "O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa.
Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados.
O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados.
As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento".
Em especial, as finalidades específicas do tratamento dos dados pessoais deverão ser explícitas e legítimas e ser determinadas aquando da recolha dos dados pessoais. [...] RGPD, Considerando 39.

[500] LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 25. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

[501] VALE; Sebastião Barros; ZANFIR-FORTUNA, Gabriela. *Automated Decision-Making Under the GDPR*: Practical Cases from Courts and Data Protection Authorities. *Future of Privacy Forum*. May 2022. p. 25. Disponível em: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf. Acesso em: 2 maio 2024.

[502] WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, n. 2, 2019. p. 117-119. Disponível em: https://ssrn.com/abstract=3248829. Acesso em: 6 abr. 2024.

[503] KAUFMAN, Dora; JUNQUILHO, Tainá; REIS, Priscila. Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e direitos humanos. *Revista de Direitos e Garantias Fundamentais*, [S. l.], v. 24, n. 3. 2023. p. 51-52. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/2198. Acesso em: 17 abr. 2024.

possibilitam a divulgação dos segredos às autoridades quando houver casos de amplo interesse público ou necessidade de compatibilizar direitos fundamentais[504].

Mas ainda assim subsistem dificuldades. No caso europeu, por exemplo, elas envolvem ausência de parâmetros claros sobre quais são os meios para contornar eventual recusa no fornecimento de conteúdo em razão dos segredos de negócio. Também não existe clareza sobre o que é considerado interesse público, a ponto de autorizar um acesso mais amplo aos segredos de negócio[505].

Ao fim, o exemplo europeu mostra que não existem soluções simples, mas que a compatibilização dos segredos de negócio com a proteção de dados impõe reconhecer que os segredos de negócio não podem ser utilizados de forma a sobrepor os interesses dos agentes em relação aos direitos dos titulares.

IV.1.2 As dimensões de sigilo no mercado de dados pessoais

A fim de prestigiar a transparência na interpretação da LGPD, deve-se também avaliar o alcance do sigilo que é conferido aos segredos de negócio.

Nesse sentido, é importante resgatar que o propósito do enquadramento de conteúdos como segredos de negócio deve ser o de administrar o fluxo informacional, a fim de evitar comportamentos que ensejem concorrência desleal.

Há uma falsa convicção de que o enquadramento jurídico de um conteúdo como segredo de negócio impõe uma condição secreta absoluta. Mas essa condição não existe. A preservação da condição sigilosa é relativa e circunstancial[506], podendo ser mitigada a critério do agente ou para cumprir obrigações legais. Na primeira circunstância, os agentes podem licenciar, vender ou compartilhar livremente os segredos, desde que eles não sejam amplamente disponibilizados em domínio público[507].

---

[504] MAGIOLINO, Mariateresa. EU Trade Secret Law and Algorithmic Transparency. *Bocconi Legal Studies Research Paper, n. 3363178,* 2019. p. 16. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363178. Acesso em: 04 abr. 2024.

[505] VAROSANEC, Ida. Silence is golden, or is it? Trade secrets versus transparency in AI systems. *The Digital Constitutionalist*, 17 de novembro de 2022. Disponível em: https://digi-con.org/silence-is-golden-or-is-it/. Acesso em: 22 abr. 2024.

[506] SANDEEN. Sharon K. The limits of trade secret law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on which it is based. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 555.

[507] Avalia-se, inclusive, quais são os investimentos feitos pelos agentes para que isso ocorra, e esses investimentos podem incluir não apenas tecnologias, como também instrumentos contratuais, reforçando a natureza secreta do conteúdo comercializado. Até esse critério, contudo, hoje vem sendo revisto diante do fluxo informacional intenso e de outros paradigmas de proteção das inovações. Nesse sentido, ver: BONE,

Na segunda, os agentes podem ser compelidos por autoridades públicas para disponibilizarem segredos no âmbito de fiscalizações, processos administrativos ou judiciais. Foram mencionadas investigações pelo CADE, disposições legais como a do art. 206 da LPI e até leis específicas que regulamentam a obrigatoriedade de compartilhar dados e informações como requisito à obtenção da licença comercial.

Nesse ponto, compreender que inexiste sigilo absoluto envolvendo segredos de negócio torna possível concluir que o propósito verdadeiro do instituto está mais voltado para a estruturação do trânsito de ideias e conteúdos de uma forma controlada[508], mitigando-se riscos concorrenciais[509]. A preservação da condição sigilosa é um requisito para controle desse fluxo de conteúdo e um mecanismo de se atribuir valor à informação. Ela não impõe, contudo, uma observância de padrões abstratos que obstem completamente a divulgação da informação.

Somente a interpretação do segredo de negócio como um instrumento de controle do acesso ao conteúdo torna possível efetivar as obrigações de transparência que existem na LGPD. É esse mecanismo que autoriza aos agentes manterem seus conteúdos longe do acesso de concorrentes diretos, ao mesmo tempo em que viabiliza o acesso de titulares e de autoridades aos elementos necessários para explicabilidade e *accountability*[510].

A conclusão, inclusive, alinha-se à ideia de que o propósito dos segredos de negócio é evitar a concorrência desleal, e que a condição subjetiva da tutela jurídica é evitar os impactos negativos que ela possa causar no mercado, regulando um comportamento individual – o do compartilhamento da informação – e não o sigilo de um conteúdo específico.

Robert G. Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions. *In*: DREYFUSS, Rochelle C.; STRANDBERG, Katherine J. (eds.). The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research. Edward Elgar Press, 2010. *Boston Univ. School of Law Working* Paper No. 09-40. Disponível em: https://ssrn.com/abstract=1467723. Acesso em:10 mar. 2024.

[508] VOGT, Sander. Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence—Part II. *In*: *The Journal of Robotics, Artificial Intelligence & Law* (Fastcase), Volume 5, No. 5, September–October 2022, Full Court Press, an imprint of Fastcase, Inc. p. 312-312. Disponível em: https://www.crowell.com/en/insights/publications/show-me-your-secrets-how-the-use-of-trade-secrets-relates-to-the-demand-for-transparent-artificial-intelligence-part-ii. Acesso em: 24 mar. 2024.

[509] SAPPA, Cristiana. How data protection fits with the algorithmic society via two intellectual property rights – a comparative analysis. *Journal of Intellectual Property Law & Practice*, Volume 14, Issue 5, May 2019. p. 11. Disponível em: https://academic.oup.com/jiplp/article-abstract/14/5/407/5369198. Acesso em: 19 fev. 2024.

[510] LEMLEY, Mark A. The Surprising Virtues of Treating Trade Secrets as IP Rights. *Stanford Law Review*, v. 61. p. 311, junho 2008. Stanford Law and Economics Olin Working Paper No. 358. Disponível em: https://law.stanford.edu/sites/default/files/publication/258632/doc/slspublic/Lemley%20Surprising.pdf. Acesso em: 03 mar. 2024.

IV.2 PREOCUPAÇÕES SOBRE O USO DE SISTEMAS PROTEGIDOS POR SEGREDOS DE NEGÓCIO POR PARTE DA ADMINISTRAÇÃO PÚBLICA

Nos debates sobre transparência e criação de opacidade por meio dos segredos de negócio, surge igualmente uma importante discussão sobre o papel da administração pública quando adota sistemas (mais ou menos complexos) de tratamento de dados para o desempenho de suas funções.

Como vem sendo desenhado no presente estudo, há de haver um esforço para compatibilizar a transparência e a proteção aos segredos de negócio, a fim de que a atividade econômica não seja prejudicada e, simultaneamente, não existam óbices à concretização da proteção de dados pessoais.

No âmbito da administração pública, essas discussões ganham camadas adicionais de sofisticação. Isso porque os tribunais brasileiros vêm dando indicativos de que esse padrão de incorporação da inteligência artificial no processo judicial será por meio de contratação de entes privados para desenvolvimento desses programas[511]. Em termos de vigilância, essa também é a regra, através do licenciamento de *softwares* de monitoramento e identificação facial desenvolvidos por entes privados.

Pelos exemplos que já foram trazidos, percebe-se que a incorporação desse tipo de tecnologia a nível da administração pública pode trazer significativos prejuízos à coletividade, seja diante do risco de decisões discriminatórias, seja em razão de possíveis resultados incorretos, ou seja, ainda, em razão da ausência de devido processo legal para questionamento desses modelos decisórios.

Resolver essas questões implica reconhecer que, para a administração pública, não se trata apenas de comprar um produto ou adquirir um serviço que é protegido por segredos de negócio. Trata-se de uma atuação que tem por base o exercício de uma função pública, cujo desempenho depende de níveis de transparência amplos e simplificados[512].

---

[511] STF. STF recebe propostas de uso de inteligência artificial para agilizar serviços. *STF*. 2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=522767&ori=1. Acesso em: 02 jun. 2024.

[512] LEVINE, David S. The impact of trade secrecy on public transparency. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 409.

Ainda que possam existir formas de acesso aos segredos de negócio para fiscalização, no contexto da transparência pública, essas formas podem ser ineficazes por alguns motivos: haverá sempre um interesse privado na preservação dos segredos de negócio; os agentes privados vão prestigiar a busca do lucro (e não do interesse público); e os mecanismos para acesso aos segredos de negócio, a fim de assegurar a *accountability*, podem levar tempo que acabará prejudicando o administrado (gerando ineficiência pública e maiores gastos[513]). Não se pode perder de vista que a consequência das ações adotadas pela administração impactam diretamente políticas públicas e podem criar inúmeros prejuízos aos cidadãos[514].

Isso quer dizer que a transparência exigida da administração pública quando do uso de sistemas de tratamento de dados automatizados não pode ser eventual. Ela deve ser de fácil acesso, passível de auditoria e de fácil controle[515]. Também deve pressupor a possibilidade de compartilhamento integral de informações sobre o uso, a operação, o modelo e os dados utilizados[516], impondo níveis de divulgação de conteúdo que vão desde o fornecimento de *inputs* para tratamento até divulgação de quais são os dados pessoais utilizados pelo sistema[517].

---

[513] PASQUALE, Frank. The troubling consequences of trade secret protection of search engine rankings. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 401.

[514] LEVINE, David S. The impact of trade secrecy on public transparency. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 410.

[515] LEVINE, *op. cit*., p. 410.

[516] Existem discussões sobre a compatibilização de transparência por parte da administração pública envolvendo dados pessoais em um modelo aberto, até para facilitar a implementação de políticas públicas (ZANATTA, Rafael Augusto Ferreira. O Uso da Lei Geral de Proteção de Dados Pessoais por Gestores Públicos: Origens e Funções Procedimentais em Políticas Públicas no Brasil. *Revista de Estudos em Organizações e Controladoria-REOC*, ISSN 2763-9673, UNICENTRO, Irati-PR, v. 3, n. 2, jul./dez., 2023. p. 226-232. Disponível em: https://revistas.unicentro.br/index.php/reoc/article/view/7614. Acesso em: 08 jun. 2024). Isso ajuda a elucidar os níveis amplos de transparência que são esperados na atuação da administração.

[517] De acordo com Maranhão, Junquilho e Tasso: "Transparência quanto ao uso. A transparência quanto ao uso do sistema requer daqueles que empregam o sistema de IA que informem não só que o usuário interage direta ou indiretamente com um sistema de IA ou que estão sujeitos a um processo de tomada de decisão que é influenciado por um sistema de IA, mas também que indiquem qual o grau de influência da IA no resultado final da decisão [...] Transparência quanto à operação. Como indicado acima, a transparência quanto à operação refere-se a três elementos-chave no desenvolvimento de sistemas de IA, em particular aqueles baseados em aprendizado de máquina: a) transparência quanto aos dados; b) transparência quanto ao modelo e suas inferências; c) transparência quanto ao envolvimento humano. [...] A transparência quanto aos dados refere-se, em primeiro lugar, à indicação sobre o emprego de dados pessoais e uso de profiling dos indivíduos sujeitos à decisão. [...] Em segundo lugar, a transparência também deve conter elementos para avaliar a qualidade dos dados empregados: sua completude, fidedignidade, confiança quanto à fonte, forma de coleta ou possíveis adulterações, frequência de atualização e representatividade em relação a populações de interesse (grupos menos favorecidos)" (MARANHÃO, Juliano Souza de Albuquerque; JUNQUILHO, Tainá Aguiar; TASSO, Fernando Antônio. Transparência sobre o emprego de Inteligência Artificial no Judiciário: um modelo de governança. *Suprema - Revista de Estudos Constitucionais*, Distrito

Esses requisitos podem se mostrar incompatíveis com o desempenho de atividades no âmbito da iniciativa privada, o que implica considerar que a proteção dos segredos de negócio pode ser inadequada para atingir os níveis de *accountability* que a administração pública precisa ter em relação aos seus administrados[518].

Na prática, deve-se considerar que os requisitos de transparência exigíveis do ente público devem impor a ele que desenvolva suas próprias tecnologia por meio de *softwares* abertos e auditáveis, no lugar de contratar agentes privados para fazê-lo[519]. A possibilidade de participação pública na criação e no aprimoramento dessas tecnologias reforça parâmetros que são exigidos da administração e pode viabilizar incentivos em pesquisas cujo foco não seja o lucro, mas sim a proteção do interesse e do bem público[520].

Outra possibilidade seria admitir a cooperação com entes privados, desde que o ente público firme contratos que já estabeleçam possibilidades amplas de divulgação de segredos de negócio para cumprir o propósito de transparência necessário à atividade pública[521]. Dentre as negociações possíveis, e para não pensar somente na divulgação de códigos e compartilhamento integral de sistemas, a administração pública deverá poder solicitar auditorias amplas, divulgação de elementos decisórios para facilitar a compreensão sobre a tomada de decisão e produção de Relatórios de Impacto em sofisticados níveis de complexidade[522]. Afinal, se desenvolvem função pública, os entes

---

Federal, Brasil, v. 3, n. 2, 2023. p. 156-157. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/231. Acesso em: 17 maio 2024). Os autores também falam em transparência sobre o modelo, que busca "a partir de uma grande massa de dados, obter uma regra de decisão ou função objetiva probabilística, conforme o modelo matemático escolhido (regressão linear, árvore de decisão, florestas randômicas, redes neurais, etc.) que atribua pesos relativos aos dados de entrada, de modo a obter a predição mais acurada da variável de saída" (MARANHÃO, Juliano Souza de Albuquerque; JUNQUILHO, Tainá Aguiar; TASSO, Fernando Antônio. Transparência sobre o emprego de Inteligência Artificial no Judiciário: um modelo de governança. *Suprema - Revista de Estudos Constitucionais*, Distrito Federal, Brasil, v. 3, n. 2, 2023. p. 158. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/231. Acesso em: 17 maio 2024).

[518] CITRON, Danielle Keats. Open Code Governance. *University of Chicago Legal Forum*, vol. 2008, n. 1, 2008, Artigo 9. p. 357. Disponível em: http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/9. Acesso em: 27 abr. 2024.

[519] CITRON, *op. cit*.

[520] COGLIANESE, Cary; LAMPMANN, Erik. Contracting for Algorithmic Accountability. *Administrative Law Review Accord*, v. 6. 2021. p. 194-196. Disponível em: https://administrativelawreview.org/wp-content/uploads/sites/2/2021/10/Coglianese-Lampmann_For-ACCORD-1.pdf. Acesso em: 12 abr. 2024.

[521] SANCHEZ-GRAELLS, Albert. Ensuring algorithmic transparency through public contracts? *The Digital Constitutionalist*, 24 de novembro de 2022. Disponível em: https://digi-con.org/ensuring-algorithmic-transparency-through-public-contracts/. Acesso em: 28 abr. 2024; COGLIANESE; LAMPMANN, *op. cit*., p. 185-186; LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. *International Journal of Law and Information Technology*, Vol. 27, Issue 2, 2019. p. 22. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313916. Acesso em: 10 jan. 2024.

[522] COGLIANESE; LAMPMANN, *op. cit*., p. 190-193.

privados devem se submeter às mesmas regras de transparência exigíveis da administração pública[523].

Também é possível pensar em recomendar que os entes públicos prestigiem a contratação de sistemas abertos, que são explicáveis e completamente transparentes (na medida de suas possibilidades), e não envolvam aprendizagem autônoma ou elementos técnicos de *deep learning*, os quais podem ter grande extensão de opacidade e proteção pelos segredos de negócio[524]. A ideia é que a implementação das tecnologias no âmbito da administração prestigie sistemas que sejam compreensíveis e permitam a rastreabilidade dos resultados, até mesmo para assegurar o devido processo legal[525].

O objetivo final não é privar o agente público de adotar tecnologias para otimizar suas operações e torná-las mais eficientes. Mas qualquer incorporação de sistemas automatizados de tratamento de dados, no caso da administração pública, deve levar em consideração paradigmas de transparência mais amplos, que não vão se submeter às mesmas dificuldades de explicabilidade e *accountability* que se submetem os sistemas operados por entes privados com finalidade privada.

O risco de não se observar essas questões é retirar parte da legitimidade de atuação do ente público, conforme exposto anteriormente[526]. Níveis diferenciados de transparência são preocupações fundamentais na esfera pública e constituem mais uma forma de evitar que a proteção aos segredos de negócio seja utilizada como uma camada adicional de opacidade.

---

[523] CARLSON, Alyssa M. The Need for Transparency in the Age of Predictive Sentencing Algorithms. *Iowa Law Review*, Vol. 103, 2017. p. 322-329. Disponível em: https://ilr.law.uiowa.edu/print/volume-103-issue-1/the-need-for-transparency-in-the-age-of-predictive-sentencing-algorithms. Acesso em: 12 maio 2024. Como destacam também Gilmar Mendes e Paulo Gonet, a transparência no âmbito da administração pública se associa também ao princípio da moralidade e publicidade e ao exercício democrático (MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito Constitucional*. 9. ed. rev. e atual. São Paulo: Saraiva, 2014. p. 747-749).

[524] BUSUIOC, Madalina. Accountable artificial intelligence: holding algorithms to account. *Public Administration Review*, v. 81, n. 5. p. 825-836, Sept./Oct. 2021. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293. Acesso em: 18 abr. 2024; CITRON, Danielle Keats. Open Code Governance. *University of Chicago Legal Forum*, vol. 2008, n. 1, 2008, Artigo 9. p. 371-373. Disponível em: http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/9. Acesso em: 27 abr. 2024.

[525] HILDEBRANDT, Mireille. Algorithmic regulation and the rule of law. *Philosophical Transactions Royal Society Publishing*. A 376, n. 20170355, 2018. p. 2-3. Disponível em: http://dx.doi.org/10.1098/rsta.2017.0355. Acesso em: 19 out. 2023.

[526] CALO, Ryan; CITRON, Danielle. The Automated Administrative State: A Crisis of Legitimacy. *Emory Law Journal*, v. 70. p. 797–846, 2021. p. 818-819. Disponível em: https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj. Acesso em: 19 out. 2023.

IV.3 ESFORÇOS PARA O RESGATE DA NATUREZA SUBSTANCIAL DAS LEIS DE PROTEÇÃO DE DADOS E A OPÇÃO POR NÃO USAR SEGREDOS DE NEGÓCIO NO MERCADO DE DADOS PESSOAIS

Trazida anteriormente, a crítica de procedimentalização da LGPD é corroborada pelo tratamento que a lei dá aos segredos de negócio. Foram analisadas diferentes menções feitas ao longo do texto para elucidar que os segredos de negócio acabam criando a possibilidade dos agentes de tratamento de adicionarem uma camada de opacidade sobre as operações. Em outros momentos, também foi explorada a inadequação dos segredos de negócio para tratar determinados elementos do mercado de dados pessoais.

Pretende-se agora analisar e rever as principais menções aos segredos de negócio, a fim de compreender de que forma essas questões podem ser interpretadas, sempre com vistas à garantia fundamental de proteção dos dados pessoais.

IV.3.1 Segredos de negócio na portabilidade de dados

A portabilidade se inclui como um legítimo direito do titular de acesso aos dados de poder transportar os dados para migrar de serviços. Por envolver concorrentes diretos, ela cria limitações ao compartilhamento de segredos de negócio em razão dos riscos de concorrência desleal.

Por isso, existem controvérsias importantes. De um lado, está a proteção aos dados pessoais que o agente de tratamento empenha esforços, tecnologia e criatividade para coletar. Do outro, está o direito do titular de poder dispor de todo o conteúdo existente sobre si, seja para ter mera ciência da sua existência, seja para poder disponibilizá-lo a outro fornecedor.

Diante das dificuldades de interoperabilidade e da necessidade de um sistema específico, é inquestionável que a matéria deve ser objeto de regulação própria pela ANPD, dedicando considerações específicas sobre todos os aspectos técnicos necessários para portabilizar os dados pessoais. Mas, no âmbito dos segredos de negócio, é necessário que a regulação, e até a interpretação da lei, não crie limitações e dificuldades adicionais ao acesso do titular sobre quais informações sobre si foram coletadas e exploradas comercialmente.

É fácil ver a portabilidade como uma operação de intercâmbio de ativos, nos quais concorrentes diretos trocam conteúdos entre si, a fim de satisfazer a vontade de um consumidor em mudar de fornecedor. Mas antes de ativos, os dados são extensões da personalidade. Eles se referem a um indivíduo e atraem para si todas as reflexões sobre dignidade da pessoa, sobre direitos fundamentais e sobre proteção das dimensões individuais que colocam o ser humano no vértice do ordenamento jurídico[527].

Tratar dados apenas dentro de uma dimensão comercial exclui os titulares de um processo informacional importante e que vem antes da portabilidade: mais do que assegurar a disponibilização dos dados e as trocas entre os mercados, as garantias dispostas nos arts. 18, V, e 19, parágrafo 3º, da LGPD, dão ao titular um acesso amplo sobre quais informações sobre ele são utilizadas na atividade econômica. Limitar esse acesso em razão dos segredos de negócio seria tirar do titular o direito de saber exatamente quais dados ele fornece para um agente econômico usar.

Nesse aspecto, defende-se que não pode haver a possibilidade de escolher como se enquadram os dados pessoais: eles não podem ser tratados como segredos de negócio.

Ainda que não exista uma extensão absoluta de sigilo conferida aos segredos de negócio, enquadrar os dados nessa categoria jurídica reforça sua percepção como ativo e pode criar óbices para garantir o direito de acesso amplo que deve ser assegurado aos titulares. Frise-se: o propósito da LGPD deve ser o da proteção de dados pessoais, e não há como se garantir esse direito sem que o titular possa dispor integralmente de todos os dados que são coletados e tratados sobre ele próprio.

Não se pode ignorar, por outro lado, as possíveis repercussões concorrenciais que a portabilidade pode trazer se o agente for compelido a fornecer integralmente todos os dados pessoais que armazena de um determinado titular. Não quer dizer que os dados vão ser tratados como segredos, mas pode implicar que a extensão dos dados objeto de portabilidade pode vir a ser limitada com o objetivo de não criar distorções no mercado.

E é possível ao agente de tratamento diferenciar a forma como ele assegura o acesso aos dados pessoais ao titular. Em todas as circunstâncias, o titular deverá ter amplo, integral e facilitado acesso aos dados pessoais que foram coletados sobre si. Contudo, quando houver intenção de trocar fornecedores, o agente poderá disponibilizar esses

---

[527] TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology & Intellectual Property*, v. 11. p. 239, 2013. p. 269. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 16 nov. 2023.

dados em formatos diferentes, diferenciando os dados que podem ser transferidos para o concorrente e os que não podem permitir a reutilização.

A dificuldade certamente é diferenciar esses tipos de dados, pois não se pode autorizar que a portabilidade seja excessivamente limitada com o não compartilhamento de dados importantes para o desempenho da atividade comercial. Em outra perspectiva, é legítimo reconhecer que nem todos os agentes econômicos têm acesso a determinados tipos de dados pessoais, especialmente aqueles que só podem ser coletados ou criados (no caso dos dados inferidos) por sofisticados processos tecnológicos[528]. Assim, modos parciais de visualização e reutilização dos dados permitem diferenciar esses conteúdos, competindo à regulação setorial detalhar exatamente o que se incluir em cada categoria.

Essa solução é uma proposta mais arrojada do que a prática, inclusive no âmbito de outras jurisdições. O RGPD, por exemplo, elimina um problema ao dizer quais são os dados objeto de portabilidade, mas cria outro ao limitar excessivamente os contornos da autodeterminação informativa. Diz o diploma europeu que somente são portabilizáveis os dados pessoais "fornecidos" pelos titulares, sendo expressamente excluídos do direito de requisição os dados deletados ou anonimizados[529]. Contudo, o intercâmbio informacional acaba ficando restrito[530], suprimindo informações que, em setores mais sofisticados (como o da internet das coisas) podem ser essenciais para o desempenho dos serviços sem que se prejudique o consumidor[531].

IV.3.2 Segredos de negócio no direito à explicabilidade

Uma grande preocupação sobre as limitações criadas pelos segredos de negócio é permitir que eles reconfigurem as dimensões de explicabilidade e assim esvaziem por completo a autodeterminação informativa.

---

[528] LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 27. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

[529] JANAL, Ruth. Data portability under the GDPR: A blueprint for access rights? *In*: German Federal Ministry of Justice and Consumer Protection | Max Planck Institute for Innovation and Competition (eds.). *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos. 2021. p. 321.

[530] CRAVO, Daniela. O direito à portabilidade na Lei Geral de Proteção de Dados. *In* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023. p. RB-12.4.

[531] LA DIEGA; SAPPA, *op. cit*., p. 27.

A explicabilidade não pode ser reduzida pela escolhas dos agentes que optam pela tutela jurídica dos segredos de negócio, sob risco de se aumentar a opacidade. A materialização da transparência deve ser perseguida de forma efetiva no mercado em questão[532], a fim de se buscar o cumprimento do direito fundamental à proteção de dados.

Uma primeira forma de viabilizar essa explicabilidade é por meio do direito de acesso aos dados pessoais. Em um ordenamento jurídico que tem como garantia fundamental a proteção de dados e a privacidade, é impositivo que se assegure ao titular o acesso integral aos dados sobre si que são coletados e explorados pelos agentes de tratamento[533].

O acesso aos dados constituiu uma garantia do titular, uma expectativa legítima, que precisa ser cumprida tanto pelos agentes quanto pelo ente público que coleta informações. Essa compreensão reforça que não se pode considerar dados pessoais como segredos de negócio, sob risco de impedir a garantia do titular e impedir que ele possa conhecer integralmente quais informações foram coletadas ou criadas sobre si. Frise-se: a dimensão existencial dos dados pessoais sempre será preponderante, e ainda que sejam ativos, eles são, antes de tudo, desdobramentos da personalidade, cujo controle, acesso e cuja administração devem ser integralmente assegurados aos titulares.

A interpretação da LGPD, portanto, não pode ser no sentido de que a ressalva dos segredos de negócio alcança os dados pessoais quando se discutir o direito de acesso (a exemplo do art. 19,II, e parágrafo 3º, da lei). Ela deve ser no sentido de que outros elementos podem ser até tratados como segredos, mas não as informações sobre os titulares, que precisam ser integralmente disponibilizadas de forma célere, sem custo, respeitando o formato de comunicação imposto pela lei[534].

O agente é responsável, ainda, por disponibilizar a infraestrutura por meio da qual será assegurado o direito de acesso[535], o que não deve ser visto como um fardo, mas sim

---

[532] TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. Northwestern Journal of Technology & Intellectual Property, v. 11, 2013. p. 264-265. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 16 nov. 2023.

[533] Como diz Tavares Guerreiro: "vem se firmando um direito individual, que se pode afirmar típico da época contemporânea, outorgado e garantido a cada um, de conhecer as informações que lhe dizem respeito, armazenadas em repositórios, de caráter público ou privado" (GUERREIRO, José Tavares *et al*. *Comentários ao Código do Consumidor*. (José Cretella Júnior e René Ariel Dotti - coord). Rio de Janeiro: Forense, 1992. p. 142.

[534] O art. 43 do CDC já traz regulamentação específica em relação aos consumidores e dispõe que o acesso integral ao consumidor deve ser imediato e gratuito. Sobre o tema: GRINOVER, Ada Pellegrini *et al*. *Código Brasileiro de Defesa do Consumidor*. 13. ed. Reio de Janeiro: Forense, 2022. p. 384.

[535] Os agentes deverão se responsabilizar por toda uma infraestrutura que consiga garantir que o acesso dos dados será feito somente ao titular, criando mecanismos de checagem de identidade e segurança para que

como um benefício. Ao poder escolher o meio pelo qual o acesso será feito, o agente pode tentar separar suas bases de dados e não denunciar a forma como estrutura suas operações[536] (o que pode ser mais simples ou mais complexo a depender do nível e do volume que os dados são tratados).

Também se pode destacar que há uma diferença entre assegurar o acesso aos dados e assegurar o reúso desses dados. Como foi mencionado em relação à portabilidade, existem dados pessoais que, mesmo não são considerados segredos, podem trazer distorções concorrenciais se utilizados por terceiros. Por isso, é importante pensar em um exercício regulatório setorial que possa distinguir a forma de assegurar esse direito, a fim de que o acesso do titular não esteja condicionado à necessidade de torna esses dados disponíveis para uso futuro.

O que se defende é que o acesso por si só deve ser assegurado em termos integrais, disponibilizando-se ao titular informações sobre todos os dados pessoais que são coletados sobre ele[537]. Isso pode ser feito em uma modalidade que assegure apenas um modo de visualização, sem que os dados, especialmente aqueles mais valiosos, possam ser reutilizados por terceiros[538]. A solução proposta afasta a restrição de acesso dos

---

as informações disponíveis não se relacionem com terceiros. Também surgem preocupações com a segurança dos dados e riscos de incidentes, que devem ser incluídos nas diligências, a fim de evitar que o acesso integral aos dados seja viabilizado sem que, simultaneamente, aumentem os riscos para os titulares. Nesse sentido: TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology & Intellectual Property*, v. 11. p. 239, 2013. p. 269. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 16 nov. 2023.

[536] OCAÑA, Teresa Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020. p. 77-86.

[537] É possível que empresas, caso não desejem fornecer toda extensão dos dados pessoais, tenham a possibilidade de anonimizá-los, o que tornaria menor o escopo do dever de transparência ao assegurar acesso aos dados (MALGIERI, Gianclaudio. Trade Secrets v Personal Data: A Possible Solution for Balancing Rights. *International Data Privacy Law*, Volume 6, Issue 2. p. 102-116, maio de 2016. Disponível em: https://ssrn.com/abstract=3002685. Acesso em: 02 maio 2024). Contudo, deve permanecer a preocupação de evitar que esses dados anonimizados (ou descontextualizados) não possam ser novamente identificados posteriormente, no que Solove e Schwartz nomearam de "PII Problem". Como mencionam os autores, a tecnologia cada vez mais sofisticada faz com que a anonimização seja uma operação pouco segura para retirar os elementos que associam um dado a um titular específico. Por esse motivo, não deveriam ser medidas adotadas comumente para resguardar privacidade e outros direitos dos titulares (SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, Vol. 86. p. 1814, 2011. Disponível em: https://www.nyulawreview.org/issues/volume-86-number-6/the-pii-problem-privacy-and-a-new-concept-of-personally-identifiable-information/. Acesso em: 16 nov. 2023). Considerações similares foram trazidas recentemente também por Diego Machado: MACHADO, Diego. Considerações iniciais sobre o conceito de dado pessoal no ordenamento jurídico brasileiro. *Civilistica.com*, Rio de Janeiro, v. 12, n. 1. p. 1–34, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/843. Acesso em: 4 maio. 2024.

[538] LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower

titulares e assegura que se poderá, ao menos, conhecer integralmente todos os dados pessoais que são tratados sobre si.

A interpretação proposta sobre o direito de acesso se alinha à Constituição Federal, nas disposições sobre o *habeas data* e o direito de acesso às informações relativas à pessoa (art. 5º, LXII, CF). Também se alinha ao Código de Defesa do Consumidor[539], ao criar o direito de acesso amplo e irrestrito aos dados que ensejaram anotações sobre o consumidor, incluindo a fonte da qual foram coletados (art. 43, parágrafo 1º)[540].

Além do acesso integral aos dados, elementos de explicabilidade direcionados ao titular compreendem também o acesso integral aos critérios decisórios por meio dos quais os dados e as tecnologias produziram resultados. O acesso a esses conteúdos é ressalvado pela LGPD em dispositivos como o art. 9, II, e 20, parágrafo 1º.

Não sendo os dados pessoais tratados como segredos de negócio, fica a controvérsia sobre o que são então os segredos de negócio dentro do mercado de dados pessoais. Já foi explorado que, em grande medida, essa categoria jurídica pode ser inapropriada para falar até mesmo de bases de dados, códigos e elementos que compõem a decisão automatizada.

Se, por outro lado, o propósito é pensar em formas de interpretar a LGPD à luz da proteção de dados, superando-se essa inadequação, deve-se ter em mente que a escolha do agente em tratar conteúdos como segredos de negócio não implica conferir a eles um nível de sigilo absoluto, pois a prioridade será sempre assegurar ao titular as informações necessárias para o exercício da sua autodeterminação informativa.

Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. p. 26. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

[539] Sobre o referido dispositivo e a postura do CDC em relação aos bancos de dados de consumidores para fins de anotações cadastrais, destaca-se o comentário de Grinover *et al*: "Em síntese, o CDC, ao cuidar dos arquivos de consumo, não pretendeu, nem mesmo remota ou indiretamente, legitimar sua atenção e presença no mercado. Deles, não tratou para lhes conferir extensão maior ou intocabilidade; ao revés, foi intuito seu confinar, sob o manto de uma rígida disciplina, a discricionariedade e irresponsabilidade legal que os caracterizava, impondo-lhe regras claras, sempre com os olhos postos na proteção dos consumidores e, através deles, na preservação de direitos fundamentais inalienáveis, que a todos aproveita"(GRINOVER, Ada Pellegrini *et al*. *Código Brasileiro de Defesa do Consumidor*. 13. ed. Reio de Janeiro: Forense, 2022. p. 347).

[540] Novamente cabe transcrever as conclusões de Grinover *et al*: "Em outras palavras, a *raison d'être* da lei brasileira é, pois, conferir ao consumidor acesso amplo e irrestrito às informações a seu respeito, colhidas de outra fonte que não ele próprio, estejam elas onde estiverem: em organismos privados ou públicos, em cadastros das empresas ou em banco de dados prestador de serviços a terceiros. Não pode o arquivista, sob pena de sancionamento administrativo, civil e penal, alegar sigilo, qualquer que seja a natureza assento. Se disponível em arquivo, mesmo que de acesso vedado a terceiros, o primeiro garantido no sentido de conhecer as fontes e conteúdos registrados é o próprio consumidor objeto da anotação" (GRINOVER, Ada Pellegrini *et al*. *Código Brasileiro de Defesa do Consumidor*. 13. ed. Reio de Janeiro: Forense, 2022. p. 382 e 383).

Isso impõe reconhecer que os critérios para tomada de decisão automatizada devem ser fornecidos aos titulares, independentemente de como eles vão ser enquadrados juridicamente pelo agente de tratamento.

A dificuldade é definir exatamente o que são os critérios decisórios. Como visto, as decisões automatizadas são compostas por inúmeros elementos além dos códigos que impactam no resultado produzido[541]. Idealmente, e diante dos esforços da ANPD em estabelecer um modelo colaborativo[542], a regulação poderia detalhar, para cada atividade setorial específica, o que são os critérios a serem divulgados e de que forma deve ser assegurado esse acesso aos titulares[543].

Por meio de uma regulação específica voltada para diferentes setores que produzem decisões automatizadas, a proposta ainda elimina a preocupação de não deixar a critério exclusivo dos agentes quais são os requisitos para cumprir a explicabilidade. Cria-se uma situação de maior segurança jurídica, na qual o conteúdo que vai ser disponibilizado não fica sujeito a escolhas discricionárias; e na qual os titulares podem criar legítimas expectativas sobre o que podem saber sobre cada agente que trata seus dados pessoais.

Na ausência da regulação, a interpretação da norma deve considerar se a recusa, por meio dos segredos de negócio, envolve uma informação essencial para que o titular compreenda como se dá o tratamento de seus dados. E sendo esse o caso, deverá superar o sigilo e viabilizar o acesso do titular dos dados.

Não é repetitivo lembrar que as discussões sobre os critérios decisórios envolvem questões amplas que não estão somente associadas à autodeterminação informativa, e que atendem a uma política coletiva de proteção de dados. Trata-se de uma forma de auxiliar no controle ético das operações; facilitar a compreensão sobre possíveis discriminações

---

[541] MENDONÇA, Ricardo F.; FILGEURIAS, Fernando; ALMEIDA, Virgílio. *Algorithmic Institutionalism*. The Change Rules of Social and Political Life. United Kingdom: Oxford University Press, 2023. p. 29; PEREL, Maayan; ELKIN-KOREN, Niva. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, n. 181, 2017, p. 188-189. Disponível em: https://scholarship.law.ufl.edu/flr/vol69/iss1/5/. Acesso em: 18 fev. 2024.

[542] WIMMER, Miriam; PIERANTI, Octavio Penna. Programas de compliance e a LGPD: a interação entre autorregulação e a regulação estatal. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021. p. 212.

[543] A proposta também é feita em âmbito do RGPD, para que o diploma também seja pensado em termos de governança colaborativa e possibilite criação de pontes para diálogo na construção do que é um direito de explicabilidade possível quando se pensa em decisões algorítmicas. Sobre a questão, ver: KAMINSKI, Margot E. Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability. *South California Law Review*, v. 92. p. 1529, 2019. p. 1.596. Disponível em: https://scholar.law.colorado.edu/faculty-articles/1265/. Acesso em: 17 mar. 2024.

e resultados enviesados[544]; entender o poder dos dados pessoais e dos algoritmos; diminuir a assimetria informacional; auxiliar no devido processo legal das decisões automatizadas[545]; e possibilitar a contestação de decisões, especialmente quando envolverem aspectos de segurança, confiabilidade e violação a garantias fundamentais[546].

Diante dessa gama de benefícios, as contrapartidas para obstar o acesso do titular aos critérios decisórios se mostram diminutas. Comparadas com a dimensão existencial que esse acesso promove, as preocupações com o sigilo e as repercussões patrimoniais dos agentes de tratamento também se mostram superáveis, e garantem a coerência sistêmica necessária a um ordenamento jurídico que prestigia a proteção da garantia fundamental à proteção de dados.

Elementos de explicabilidade podem, por fim, envolver o acesso aos códigos e aos elementos técnicos que compõem o tratamento dos dados. Para esses casos, o enquadramento como segredos de negócio pode ser mais justificável (ainda que, em uma primeira análise, mostre-se impróprio, conforme visto anteriormente), de modo que é legítimo esperar uma limitação maior do acesso assegurado ao titular.

Em alguma medida, pode-se dizer que a autodeterminação informativa não depende do acesso integral da sintaxe matemática que estrutura os sistemas de tratamento de dados. Primeiro, porque o titular possui inúmeras dificuldades cognitivas que impedem a compreensão exata de qual a funcionalidade desses algoritmos e seus elementos[547]. Segundo, porque o direito de acesso não pode se confundir com o escrutínio das operações[548]. E terceiro, porque o controle estrutural sobre os códigos para avaliação de seus impactos está majoritariamente inserido dentro da competência da autoridade, e não

---

[544] TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology & Intellectual Property*, v. 11. p. 239, 2013. p. 270. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 16 nov. 2023.

[545] COGLIANESE, Cary; LAMPMANN, Erik. Contracting for Algorithmic Accountability. *Administrative Law Review Accord*, v. 6. p. 175, 2021. p. 186. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 12 abr. 2024.

[546] HILDEBRANDT, Mireille. Preregistration of Machine Learning Research Design. Against P-hacking. *In*: BAYAMLIOLGU, Emre; BARALIUC, Irina; JANSSENS, Lisa; HILDEBRANDT, Mireille (eds.). *Being Profiled*: Cogitas Ergo Sum. Amsterdam University Press, 2018. p. 104-105.

[547] MENDES, Laura Schertel; FONSECA, Gabriel Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista de Estudos Institucionais*, v. 6, n. 2, p-507-533, maio/ago 2020. p. 515. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 11 mar. 2023.

[548] DÖHMANN, Indra Spiecker genannt. The legal framework for access to data from a data protection viewpoint – especially under the RGPD. *In*: Bundesministerium Der Justiz Und Für Verbraucherschutz; Max-Planck-Institut Für Innovation Und Wettbewerb. *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos, 2021. p. 189-191.

do titular. O acesso aos códigos diz respeito a dimensões de controle que não podem ser feitas na esfera individual.

Somente em circunstâncias excepcionais o acesso poderia ser assegurado ao titular, mas ainda assim de forma limitada, em processos tramitando com segredo de justiça, e diante de uma legítima justificativa por parte do titular. São casos, por exemplo, em que há fundado receio de discriminação algorítmica e vieses nas fórmulas matemáticas. Nesses cenários, o titular não consegue produzir prova de suas alegações, e deve caber ao agente de tratamento demonstrar a idoneidade de seus códigos.

Note-se que existem várias formas de o agente de tratamento produzir essa prova e que não envolvem, necessariamente, a disponibilização de seus códigos. Como exemplo, tem-se a possibilidade de utilizar *sandboxes* e espaços virtuais controlados para avaliação de resultados; ou de produzir auditorias feitas por especialistas externos, sem que os elementos matemáticos sejam integralmente fornecidos em juízo. Essas alternativas devem ser exploradas e prestigiadas, na tentativa de equilibrar os interesses dos agentes econômicos.

Mas não se pode perder de vista que, em última análise, o art. 206 da LPI autoriza o fornecimento dos segredos de negócio em processos judiciais sigilosos. Ainda que seja medida excepcional, trata-se de uma possibilidade que está prevista no ordenamento jurídico e que pode ser explorada em casos extremos.

IV.3.2.1 Uma necessária revisão da jurisprudência sobre formulação de risco de crédito

Em linha com a necessidade de refletir como as metodologias e critérios de tomada de decisão automatizada são protegidos pelos segredos de negócio, surge a necessidade de revisar importante precedente judicial sobre o risco de crédito e sobre quais informações devem ser disponibilizadas aos consumidores.

Trata-se de precedente julgado pelo STJ, no qual se discute o direito do consumidor de ter acesso às informações que compõem o seu risco de crédito. Referido processo foi julgado em 2014 e estabeleceu, em suma, que o consumidor somente tem direito de acessar os dados pessoais utilizados pelos agentes de tratamento, estando

vedado o acesso aos critérios e às metodologias decisórias, uma vez que estes estão protegidos por segredos de negócio[549].

Há uma fundada preocupação de que as premissas desse precedente sejam utilizadas por outros agentes que utilizem ferramentas de decisões automatizadas no âmbito de outras relações de consumo. Existem vários exemplos nesse sentido: seguros, financiamentos, créditos bancários, dentre tantos outros.

Através das premissas que são propostas neste trabalho, a melhor interpretação da LGPD impõe que o precedente seja revisto, a fim de que ele possa refletir a preocupação com perspectivas mais amplas de proteção de dados e se oriente à luz do direito fundamental à proteção de dados. Já naquela época, ele estabelecia parâmetros que poderiam ser considerados obsoletos a partir dos estudos da doutrina, por ampliarem extensões de opacidade e riscos discriminatórios, em contraposição às perspectivas de justiça (*fairness*) que se almejavam aos consumidores[550]. Hoje, a revisão do julgado é ainda mais urgente e existem vários estudos comprovando que a limitação pelos segredos de negócio em casos como esse prejudica fortemente direitos individuais importantes, como o da própria autodeterminação informativa.

Deve-se entender que atribuir às metodologias e aos critérios da formação do risco de crédito a condição de segredos de negócio não pode ser uma forma de criar opacidade sobre como o *score* foi formulado[551]. Sendo um mercado que é tão relevante na atualidade, o titular deve poder conhecer os desenhos metodológicos e os critérios que concorrem para a produção do resultado[552] sem que fique sujeito aos gestores dos bancos de dados e às explicações genéricas que eles hoje fornecem sobre as operações[553]. Se for

---

[549]Cf. REsp 1.419.697, j. 12.11.2014, rel. Min. Paulo de Tarso Sanseverino. Trecho do voto. p. 35. Acesso em: 15 fev. 2024.

[550] CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, Vol. 89, 2014, p. 1-, U of Maryland Legal Studies Research Paper No. 2014-8. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 12 maio 2024.

[551] Decisão similar foi trazida no TJUE no Processo C-634/21 pelo Advogado Geral, ao discutir a recusa da empresa SCHUFA em fornecer informações sobre a metodologia de cálculo na formulação de risco de crédito dos cidadãos. O caso foi comentado por MACHADO, Diego. *Algoritmos e Proteção de Dados Pessoais*. Tutela de direitos na era dos perfis. São Paulo: Almedina, 2023. p. 338.

[552] HILDEBRANDT, Mireille. Preregistration of Machine Learning Research Design. Against P-hacking. *In*: BAYAMLIOLGU, Emre; BARALIUC, Irina; JANSSENS, Liisa; HILDEBRANDT, Mireille (eds.). *Being Profiled*: Cogitas Ergo Sum. Amsterdam University Press, 2018. p. 104-105. A autora defende, inclusive, que esses elementos devem ser previamente registrados, incluindo atualizações, para que estejam amplamente disponibilizados.

[553] STINGHEN, João Rodrigo de Morais; ANDRADE, Aline Rodrigues de. *Os riscos à privacidade do novo cadastro positivo e o papel da ANDP*. Revista dos Tribunais. vol. 1025. ano 110. p. 203-223. São Paulo: Ed. RT, março 2021. p. 217-218.

requerido judicialmente, a contrapartida ao acesso do titular deve ser, apenas, a observância do segredo de justiça no processo[554].

Ainda que o acesso integral resulte em informações incompreensíveis ao titular, especialistas técnicos indicados pelo juízo ou autoridades que venham a ser chamadas a avaliarem as informações prestadas terão a capacidade técnica para dizer sobre a idoneidade dos critérios e fornecer níveis maiores de explicabilidade que satisfaçam o consumidor[555].

Esse é o entendimento que vem sendo adotado por cortes europeias, que avaliam esses pedidos à luz do RGPD. Em caso julgado pela autoridade da Áustria, o consumidor individual requereu acesso aos elementos de explicabilidade da formulação de seu risco de crédito e a empresa se recusou a fornecê-los ao argumento de que seriam segredos de negócio. A justificativa não foi aceita pelo tribunal, na medida em que é um dever do agente fornecer informações significativas sobre como é formulado o *score* individual, incluindo considerações sobre a lógica e a metodologia envolvida[556].

IV.3.3 Segredos de negócio em relação às autoridades

Pensar nas ressalvas que são criadas pela LGPD dentro das obrigações direcionadas às autoridades também traz reflexões complexas. Afinal, o amplo escopo de atuação da ANPD, como mencionado, impõe que ela tenha acesso ao maior nível possível de explicações, seja para poder fiscalizar a atuação dos agentes de tratamento, seja para conseguir promover regulações e políticas públicas compatíveis com a realidade do mercado.

Deve-se ter em mente que a autoridade possui (ou deve possuir) corpo técnico suficientemente robusto para fazer análises mais sofisticadas, o que faz com que a comunicação e a complexidade da informação não sejam necessariamente óbices na comunicação com o agente.

Existem preocupações importantes sobre o nível de segurança que a ANPD tem para preservar o sigilo de informações que venham a ser eventualmente compartilhadas

---

[554] MACHADO, Diego. *Algoritmos e Proteção de Dados Pessoais*. Tutela de direitos na era dos perfis. São Paulo: Almedina, 2023. p. 339.
[555] MACHADO, *op. cit*., p. 338.
[556] VALE; Sebastião Barros; ZANFIR-FORTUNA, Gabriela. *Automated Decision-Making Under the GDPR*: Practical Cases from Courts and Data Protection Authorities. *Future of Privacy Forum*. May 2022. p. 19. Disponível em: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf Acesso em: 2 maio 2024.

com ela. Afinal, autoridades e órgãos do governo também estão sujeitos a incidentes de segurança e, em casos recentes, foram vítimas de ataques *hackers* que até hoje não foram devidamente explicados ou tiveram seus riscos completamente elucidados para a população.

Assim, a ANPD deve assumir, antes de tudo, um forte compromisso com a segurança que, talvez no momento presente, ainda não exista. Deve assegurar que tem a interface necessária para receber informações, armazená-las pelo tempo que for necessário e depois excluí-las de suas bases, para que a atividade comercial do agente também fique protegida[557].

Havendo esse compromisso, defende-se que os esforços interpretativos da LGPD precisam ser de sempre prestigiar o compartilhamento de informações e esclarecimentos em níveis amplos, a fim de munir a autoridade com o conhecimento necessário para que ela exerça suas funções. Pensando não só no papel desempenhado pela autoridade, mas também nas possibilidades dos agentes de tratamento de dados, as obrigações de transparência devem ser interpretadas com objetivo de dar a maior concretude possível à proteção dos dados pessoais[558].

Também para a autoridade, aplica-se o racional de que dados pessoais não são segredos de negócio e, portanto, quanto a esse conteúdo, o acesso amplo deve ser assegurado. Outros elementos, ainda que tratados como segredos de negócio, eventualmente poderão ser compartilhados com a autoridade, sem que isso implique em violação ao instituto. Afinal, como foi amplamente detalhado, a extensão do sigilo alcança situações nas quais há risco de concorrência desleal, e não pode ser oponível ao exercício das competências das autoridades.

Pensando na forma de atuação da autoridade e no seu propósito responsivo e colaborativo, bem como na relação dinâmica que existe na *accountability*[559]*,*tem-se que a ANPD não poderá, de pronto, requerer dos agentes de tratamento informações que sejam segredos de negócio.

---

[557] RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest*. Nevada Law Journal*, v. 21, n. 1. p. 61-116, 2020. p. 107. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 2024.

[558] Disse Danilo Doneda em seminário proferido em 2017: "a transparência deve ser diretamente proporcional ao poder". Ver: DONEDA, Danilo. Palestra no Seminário Interamericano de Transparência e Acesso à Informação promovido em 2017 pela Organização dos Estados Americanos (OEA) e pelo Governo Federal do Brasil. Disponível em: https://www.gov.br/cgu/pt-br/acesso-a-informacao/institucional/eventos/anos-anteriores/2017/5-anos-da-lei-de-acesso/arquivos/mesa-3-danilo-doneda.pdf. Acesso em: 26 agosto 2024.

[559] BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 78.

Em diversas circunstâncias, os esclarecimentos e os Relatórios de Impacto, ainda que elaborados em observância às ressalvas dos segredos de negócio, podem ser suficientes para que se compreenda como os dados são tratados e quais os riscos envolvidos[560]. São meios previstos em lei que já impõem a observância de rigores metodológicos para trazer confiabilidade às informações e que podem atender à pretensão da autoridade naquele momento, em relação àquele agente[561].

O mesmo pode ser dito sobre as auditorias. É fato que sua regulamentação ainda está pendente, especialmente para detalhar quais são os tipos a serem implementados e qual o escopo das análises que vão ser conduzidas[562]. Mas, para apurar impactos discriminatórios, elas também podem fazer avaliações suficientes, que não necessariamente demandem acesso imediato ao que o agente considerar segredo de negócio.

Em termos mais amplos, ainda é possível reconhecer que apenas os controles de resultados e esclarecimentos detalhados sobre metodologias e critérios decisórios possam ser suficientes para o exercício da competência fiscalizatória da autoridade[563]. Por isso, a requisição de segredos de negócio não é medida necessária em todos os casos.

Pode haver situações específicas nas quais as limitações que existem em relação a essas três medidas principais sejam mais evidentes, e assim acabem prejudicando o exercício da atividade da ANPD. Nesses cenários, ela poderia depender de maiores esclarecimentos que podem então ser requeridos dos agentes de tratamento em uma segunda rodada.

Nesse segundo momento, a autoridade deverá indicar quais as limitações que encontrou e quais esclarecimentos estão pendentes, fazendo isso da forma clara e precisa, a fim de indicar exatamente o que é necessário do agente. Ao agente, deverá ser

---

[560] MOORE, Taylor R. Trade Secrets and Algorithms as Barriers to Social Justice. *CDT Free Expression Fellow*. 2017. p. 12. Disponível em: https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf. Acesso em: 2 maio 2024.

[561] FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022. p. 264.

[562] Mesmo com as dificuldades mapeadas em relação às auditorias, existem esforços para tornar os algoritmos mais auditáveis e explicáveis. E esses são esforços que dependem de empenhos técnicos da autoridade em parceria com os agentes privados, desenvolvedores e programadores para tanto. Sobre o princípio da auditabilidade, ver: DIAKOPOULOS, Nicholas; FRIEDLER, Sorelle. How To Hold Algorithms Accountable. *MIT Technology Review*, 17 nov. 2016. Disponível em: https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/. Acesso em: 2 maio 2024.

[563]Sobre o tema, ver: PEREL, Maayan; ELKIN-KOREN, Niva. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, 69, 181, 2017. Disponível em: https://scholarship.law.ufl.edu/flr/vol69/iss1/5/. Acesso em: 18 fev. 2024.

viabilizada a possibilidade de complementar informações (aditando Relatórios de Impacto, prestando novos esclarecimentos ou fornecendo mais subsídios às auditorias), bem como de fornecerem explicabilidade por outros meios. Isto é, o agente deve poder oferecer à autoridade soluções técnicas diferentes e que não estejam expressamente descritas em lei, mas que também possam viabilizar o conhecimento detalhado sobre as operações sem que isso implique, necessariamente, em acesso aos segredos de negócio.

O tema vem sendo trabalhado na doutrina e desenvolvido no âmbito técnico como propósito de preservar as atividades econômicas do agente e compatibilizar possibilidades de transparência, para que as autoridades possam exercer fiscalizações mais amplas e minuciosas[564]. Como exemplo, tem-se a possibilidade já mencionada de o agente criar cenários diferentes e controlados (algo análogo aos *sandboxes*) para que a autoridade possa avaliar a estrutura de desempenho do sistema[565]. A criatividade fica, em uma segunda rodada de esclarecimentos, a critério do agente de tratamento, que deve se empenhar para atender às expectativas da autoridade.

Munida dessas possibilidades, ainda assim é possível reconhecer que circunstâncias excepcionais vão existir e os esclarecimentos fornecidos pelos agentes poderão ser insuficientes. Nesse cenário, excluir a possibilidade de acesso pelo Estado aos segredos de negócio[566] não é compatível com um ordenamento jurídico que tenha como garantias fundamentais a não discriminação, a proteção da privacidade e a proteção de dados pessoais.

Portanto, em caráter excepcional, uma terceira etapa deve considerar que o acesso aos segredos de negócio é uma medida de transparência. Não quer dizer que isso implicará em violação aos segredos de negócio, porque não há sigilo absoluto assegurado a esses conteúdos, como já mencionado anteriormente. Trata-se, por outro lado, de uma medida que permite diferenciar o *black box* jurídico da opacidade inerente ao funcionamento dos sistemas, assegurando que importantes avaliações sobre a decisão automatizada vão ser revisadas pela autoridade[567].

---

[564] MOORE, Taylor R. Trade Secrets and Algorithms as Barriers to Social Justice. *CDT Free Expression Fellow*. 2017. p. 12. Disponível em: https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf. Acesso em: 2 maio 2024.

[565] WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, v. 31, n. 2, 2018. Disponível em: https://ssrn.com/abstract=3063289. Acesso em: 4 maio 2024.

[566] SPECHT-RIEMENSCHNEIDER, Louisa. Data access rights – A comparative perspective. *In*: German Federal Ministry of Justice and Consumer Protection | Max Planck Institute for Innovation and Competition (eds.). *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos. 2021. p. 402.

[567] LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. *International Journal of Law and Information*

Deve-se esclarecer que a maior preocupação não é viabilizar o acesso da ANPD aos algoritmos desenvolvidos. A questão mais complexa é em relação a outros elementos que compõem o tratamento que podem ser enquadrados como segredos de negócio a critério dos agentes de tratamento. A possibilidade de escolha não pode trazer como consequência uma opacidade adicional. Assim, mesmo sendo segredos de negócio, esses são elementos fundamentais para alcançar determinados níveis de explicabilidade sobre as decisões automatizadas. E havendo justificativa plausível para requisitar seu acesso, os agentes deverão fornecê-los à autoridade.

Em todas as etapas de interação com o agente, a autoridade também deve ter em mente que, mesmo dentro dos conteúdos enquadrados como segredos de negócio, existem aqueles que são mais valiosos e por isso são protegidos em condições maiores de sigilo. Assim, o escalonamento proposto demanda que tal aspecto também seja considerado pela ANPD: ela deverá solicitar primeiro informações complementares aos Relatórios de Impacto, e/ou acesso aos segredos de negócio menos sensíveis às atividades dos agentes. Somente em um segundo momento, justificando a insuficiência das informações para seu propósito fiscalizatório, ela poderá requisitar elementos mais sofisticados ou realizar auditorias mais amplas em códigos e sistemas.

A ANPD igualmente precisará avaliar qual a extensão do conteúdo que quer ter acesso. Não necessariamente serão fornecidos códigos integrais ou elementos amplos que assegurem uma devassa nas operações dos agentes. A autoridade deve fazer requisições dentro de um juízo de razoabilidade e proporcionalidade, atendo-se aos limites do necessário para os propósitos de fiscalização. Deverá justificar, ainda, a essencialidade daqueles segredos para cumprir seus objetivos.

A proposta feita no presente estudo depende de uma última ressalva importante: a requisição de segredos de negócio deve ser medida excepcional, avaliada caso a caso e circunscrita somente às operações mais complexas[568]. São exemplos as que envolvam aprendizagem autônoma de algoritmos ou internet das coisas; coletem e tratem um extenso volume de dados; tenham riscos discriminatórios mais evidentes; sejam de setores específicos ou de forte interesse público[569]. Tratam-se de circunstâncias que

---

Technology, Vol. 27, Issue 2, 2019. p. 122-141. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313916. Acesso em: 10 jan. 2024.

[568] RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. p. 61-116, 2020. p. 107. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 2024.

[569] Alguns autores podem defender que essa prerrogativa pode ser mais ampla, para alcançar situações em que se estuda abuso de posição dominante no mercado, violações aos regimes de proteção do consumidor e outras (PASQUALE, Frank. The troubling consequences of trade secret protection of search engine

precisam ser previamente reguladas pela ANPD, inclusive para que o agente avalie se tem interesse em exercer sua atividade econômica nesses setores, a partir dos riscos em fazê-lo.

Dessas ressalvas, pretende-se afastar a possibilidade de que os segredos de negócio sejam utilizados como um escudo, que autoriza o agente a excepcionar o cumprimento de suas obrigações de transparência[570]. A *accountability* é uma obrigação dinâmica, que permite, através de uma relação de cooperação entre as partes, a criação de medidas de contingenciamento das atividades em prol do interesse público[571]. Essa cooperação pode exigir que segredos de negócio venham a ser fornecidos às autoridades, pois, em níveis mais extremos, somente o acesso a eles vai fornecer algum nível de controle sobre como a decisão automatizada foi tomada.

Garantir, em caráter excepcional, o acesso da autoridade a elementos que sejam segredos de negócio é uma opção compatível com o ordenamento jurídico brasileiro e até com tratados internacionais que dispõem sobre a matéria[572]. Essa possibilidade de acesso mais amplo resgata o uso dos segredos de negócio que melhor possibilita o cumprimento das funções da ANPD.

Como acesso aos segredos de negócio deve ser pensado caso a caso, até mesmo o modelo de acesso aos segredos de negócio pode ser discutido[573]. Havendo fundado receio sobre a capacidade de preservação do sigilo por parte da autoridade, ou até em casos de processos judiciais, nos quais a ANPD não esteja envolvida, é possível elaborar saídas

---

rankings. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 397). Análises sobre a extensão de como esse fornecimento de segredos de negócio devem ocorrer são objeto de pesquisas futuras, pois o propósito do presente estudo é defender a possibilidade de acesso maior aos elementos de explicabilidade, seja pelo titular, seja pelas autoridades, a fim de obstar a opacidade criada pelos agentes.

[570] Em seminário realizado pelo Comitê Gestor da Internet no Brasil (CGI.br), a diretora da ANPD chegou a tecer considerações sobre o tema, falando da importância de se reconhecer que o nível de compartilhamento de informações com a autoridade deve ser maior, e potencialmente até envolver segredos comerciais e industriais, para que a autoridade tenha acesso às informações e possa exercer sua competência fiscalizatória. Sobre o tema, ver: CRUZ, Carolina. Diretora da ANPD aponta limites do segredo comercial. *TeleSíntese*. 2022. Disponível em: https://www.nic.br/noticia/na-midia/diretora-da-anpd-aponta-limites-do-segredo-comercial/\. Acesso em: 24 fev. 2024.

[571] BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022. p. 78.

[572] Como foi mencionado anteriormente, o TRIPS prevê a possibilidade de divulgação de determinados segredos de negócio a autoridades em seu art. 39.3. Ainda que o referido dispositivo trate de dados específicos, ele mostra que o racional por trás da proteção aos segredos de negócio não é de conferir a esses conteúdos um tipo de sigilo absoluto, e cria bases para que outras normas locais (como o art. 206 da LPI) assegurem formas de acesso em circunstâncias excepcionais.

[573] RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. p. 61-116, 2020. p. 106. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 2024.

alternativas para que segredos de negócio eventualmente compartilhados sejam preservados.

A título de exemplo, pode-se pensar em especialistas técnicos de confiança, que fiquem permanentemente à disposição das cortes, e que tenham como função exclusiva a análise dos segredos de negócio[574]. Diferentemente de peritos apontados pelos juízes em casos específicos, seriam instituições ou profissionais contratados pelos tribunais com o propósito exclusivo de prestar serviços de auditoria e fiscalização, e que assumiriam o compromisso de informar aos juízes o necessário para solução do caso concreto[575]. Esses profissionais, eventualmente, podem até ser apontados e treinados pela própria ANPD.

Com a proposta feita no presente estudo, destacam-se importantes benefícios, para além do controle de poder propriamente dito. Estima-se que o acesso amplo da autoridade também poderá facilitar a promoção de políticas públicas mais robustas na área de proteção de dados, que consigam diminuir a assimetria existente entre o titular e o agente[576]. Também poderá ser possível administrar qual é a extensão da opacidade inerente aos algoritmos, fornecendo uma compreensão completa, na medida do que é possível, sobre as operações[577].

Munida de mais informações, a ANPD pode editar regulações mais efetivas para os setores, com obrigações de transparência que sejam compatíveis com as atividades e que tenham perspectivas de segurança mais adequadas. Pode-se também pensar em orientações para promoção de uma cultura de proteção de dados a partir de educação e conscientização sobre como, de fato, se dão as operações.

IV.3.3.1 Abrir ou não abrir o black box?

---

[574] LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. *International Journal of Law and Information Technology*, Vol. 27, Issue 2, 2019. p. 122-141. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313916. Acesso em: 10 jan. 2024.

[575] PASQUALE, Frank. The troubling consequences of trade secret protection of search engine rankings. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011. p. 383; RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. p. 61-116, 2020. p. 108. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 2024.

[576] TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology & Intellectual Property*, v. 11. p. 239, 2013. p. 262. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 16 nov. 2023.

[577] PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 14-15.

Grande parte da retórica utilizada pelos agentes para não fornecer os códigos que compõem o tratamento de dados envolve a defesa de que esses são elementos insuficientes para a compreensão sobre as operações. Até por esse motivo, as discussões sobre transparência muitas vezes voltam à pergunta sobre o *black box* de Frank Pasquale e a necessidade de se fornecer os algoritmos e as estruturas matemáticas dos sistemas para assegurar a transparência efetiva.

Ocorre que o que se chama de "abrir o *black box*" pode ter significados diferentes para determinados autores e autoras. Para alguns, pode envolver a divulgação dos códigos e o fornecimento dos algoritmos[578]. Para outros, pode compreender apenas o acesso às informações mais amplas e o controle de resultados para compreensão, dentro da extensão do que é possível, sobre como foi tomada a decisão algorítmica[579].

A fim de atender os propósitos do presente estudo, abrir o *black box* deve ter em mente que não existe um nível de explicabilidade absoluto que irá permitir a compreensão completa sobre como se dá o tratamento de dados[580]. Como visto, existe uma dimensão das operações que é intangível aos critérios de racionalidade e que, por isso, nunca poderá ser completamente desnudada. E quanto mais complexo o sistema e mais sofisticada a automação, maior é a intangibilidade[581].

Essa compreensão não tem relação nenhuma com a opacidade que é criada pelos agentes de tratamento. Como se pretendeu detalhar até aqui, o uso dos segredos de negócio consiste em uma dificuldade adicional que foi estruturada pelos agentes a partir de uma categoria jurídica que tem lastro na proteção da informação valiosa e sigilosa para a atividade comercial. Trata-se de um tipo de opacidade adicional, que existe para além da opacidade inerente aos sistemas, mas que se inclui em uma mesma categoria de óbices

---

[578] PASQUALE, *op. cit*., p. 141.

[579] BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. p. 12. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023; PEREL, Maayan; ELKIN-KOREN, Niva. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, n. 181, 2017. p. 181. Disponível em: https://scholarship.law.ufl.edu/flr/vol69/iss1/5/. Acesso em: 18 fev. 2024; RUDZITE, L. Algorithmic Explainability and the Sufficient-Disclosure Requirement under the European Patent Convention. *Juridica International*, [S. l.], v. 31. p. 125–135, 2022. p. 128. Disponível em: https://ojs.utlib.ee/index.php/juridica/article/view/19323. Acesso em: 15 abr. 2024.

[580] BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023.

[581] BUSUIOC, Madalina. Accountable artificial intelligence: holding algorithms to account. *Public Administration Review*, v. 81, n. 5. p. 825-836, Sept./Oct. 2021. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293. Acesso em: 18 abr. 2024.

que dificultam a compreensão dos titulares e das autoridades sobre como os dados são explorados e os resultados são produzidos.

Por isso, ainda que tenha acesso a segredos de negócio, sintaxes matemáticas que compõem o sistema e outros elementos, a ANPD deve ter em mente que não existe compreensão racional completa sobre as operações[582]. Discussões que partem da ideia de que "abrir o *black box*" demanda a busca por esse tipo de transparência são, portanto, ineficazes.

A questão é compreender que, por vezes, o resultado de suas investigações conduzidas pelas autoridades pode definir exatamente qual é a extensão da racionalidade alcançada pelos sistemas e qual parte envolve a produção de resultados não rastreável. São circunstâncias que criam uma dimensão de transparência que está atenta às limitações da explicabilidade e à impossibilidade de nem sempre ser possível estabelecer uma relação causal direta entre o resultado produzido e o processo[583]. Nesses casos, o controle de resultados será a única medida possível, e podem ser criadas obrigações maiores de revisão de decisões automatizadas ou até controle humano de parte das operações.

Quer dizer então que a pretensão de enfrentar a opacidade criada pelo agente de tratamento através do uso dos segredos de negócio não tem por objetivo compreender integralmente o funcionamento dos sistemas (pois, frise-se, isso é impossível)[584].

Tem, por outro lado, o objetivo de ampliar as possibilidades de controle das operações; de permitir ao titular o exercício da autodeterminação informativa; de viabilizar o devido processo legal; de assegurar a possibilidade de controle de poder por parte da autoridade[585]. O objetivo é resgatar o Direito para que ele sirva ao propósito de proteger a privacidade e os dados pessoais, utilizando seus mecanismos não como

---

[582] PEREL, Maayan; ELKIN-KOREN, Niva. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, n. 181, 2017. p. 181. Acesso em: 18 fev. 2024.
[583] KLUTTZ, Daniel N.; KOHLI, Nitin; MULLIGAN, Deirdre K. Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020. p. 144.
[584] Nesse ponto, a diferença é justamente entre abrir o chamado *black box* jurídico, sem a pretensão de abrir o chamado *black box* técnico (ou seja, aquele que é inerente ao funcionamento dos sistemas). LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability (December 20, 2018). *International Journal of Law and Information Technology*, Vol. 27, Issue 2, p. 122-141 (2019). p. 16-18. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313916. Acesso em: 10 jan. 2024.
[585] LIU; LIN; CHEN, *op. cit*.

escudos que dificultam a *accountability*, mas sim como lanternas que iluminam as dúvidas possíveis sobre o obscuro funcionamento autônomo de tratamento de dados[586].

Chamar essa possibilidade de controle poderia ser visto como um processo de "abrir o *black box*", pois criaria disponibilidade de os agentes de tratamento de dados materializarem a transparência dentro do possível. Retiraria, ainda, as barreiras que são criadas conscientemente, por meio do Direito, para evitar esse processo.

Nesse sentido, de acordo com Pasquale, autorizar possibilidades de acesso mais amplo às informações dos agentes de tratamento de dados é uma medida de coibir a opacidade criada pelos segredos de negócio, porque diversos problemas do tratamento de dados estão contidos em parâmetros que podem ser altamente controláveis, desde que haja disponibilidade dos agentes de tratamento para tanto[587].

Excepcionalmente, essa pretensão de abrir o *black box* pode ensejar o fornecimento de segredos de negócio para avaliação das autoridades. Mas como defendido anteriormente, essa é uma situação extremamente excepcional e que precisa ser justificada, antes de tudo, pela exclusão de todas as outras medidas possíveis e menos gravosas para viabilizar os propósitos da transparência. Ainda, é uma situação que não vai eliminar completamente a opacidade da operação, mas apenas assegurar outros níveis de explicação dentro do que é possível[588].

---

[586] KLUTTZ, Daniel N.; KOHLI, Nitin; MULLIGAN, Deirdre K. Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020. p. 146.

[587] BUCHER, Taina. *If...Then*: Algorithmic power and politics. Oxford University Press, 2018. p. 45.

[588] ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Midia & Society*, 20(3), 2018. p. 9. Disponível em: https://doi.org/10.1177/1461444816676645. Acesso em: 12 out. 2023.

CONCLUSÃO

O presente estudo teve por objetivo analisar quais são as diferentes dimensões de opacidade que criam óbices à transparência no âmbito da proteção de dados pessoais. Esses óbices foram tratados dentro de uma categoria ampla de opacidades, que diz respeito a uma falta de clareza geral sobre como se dão as operações de dados.

Foram sistematizados quatro principais tipos de opacidades: (i) os óbices relacionados ao titular dos dados; (ii) as opacidades (*stricto sensu*) inerentes ao funcionamento do sistema; (iii) as dificuldades de concretizar a fiscalização por parte da autoridade; e (iv) os óbices legais e institucionais explorados pelos agentes para dificultar a compreensão das operações.

Os óbices relacionados aos titulares envolvem limitações que os impedem de compreender exatamente como se dão as operações de dados. Podem ser limitações de racionalidade ou de técnica, que se associam a vieses, subjetividades ou ao simples desconhecimento. São questões que, mesmo endereçadas pela LGPD para tentar criar uma estrutura de comunicação mais simplificada e objetiva, representam significativas dificuldades para que o titular possa se apropriar do conhecimento necessário sobre como se dá o uso de seus dados pessoais.

As opacidades inerentes ao funcionamento do sistema dizem respeito à incompreensão que é consequência do volume, da velocidade e da técnica que hoje se emprega no tratamento de dados pessoais. Em razão do *big data*, da datificação da experiência humana, e de algoritmos e estruturas cada vez mais sofisticadas, o processo de tomada de decisão por vezes escapa à racionalidade e envolve aspectos intangíveis que são uma consequência natural das operações.

Opacidades que dificultam as fiscalizações pela autoridade decorrem de limitações das medidas previstas em lei e que são direcionadas à ANPD. Foram trazidas três principais medidas: os esclarecimentos em geral, que podem ser excessivamente genéricos; os Relatórios de Impacto, que podem ser enviesados e metodologicamente frágeis; e as auditorias, que além de carecerem de regulação específica sobre como vão ser realizadas e com qual escopo, têm ainda limitações quanto aos resultados que podem ser produzidos.

O último tipo de opacidade trazido pela pesquisa diz respeito a uma opacidade que é criada pelos agentes de tratamento de dados pessoais através do Direito. Dentre as possibilidades, foi explorada a possibilidade de os agentes escolherem categorias

jurídicas que mais os favorecerem e que trazem, como consequência, um óbice adicional à compreensão sobre como se dão as operações. Ao optar pelo uso dos segredos de negócio, os agentes de tratamento renunciam formas mais transparentes de proteção da inovação e conseguem explorar excessivamente a natureza sigilosa dos conteúdos, podendo adotar uma retórica de recusa no fornecimento de informações que seriam necessárias à efetivação da transparência no mercado de dados pessoais.

Como foi desenvolvido ao longo do trabalho, essa possibilidade de obstar a transparência pode denunciar uma impropriedade no uso dos segredos de negócio como categoria jurídica compatível com a busca pela proteção de dados. Isso porque a exploração dos dados pessoais envolve dinâmicas de poder importantes e seus impactos são sentidos não só na esfera individual, como também em nível coletivo. Por tal motivo, as obrigações de transparência que estão inseridas dentro do mercado de dados pessoais devem ser mais amplas, a fim de assegurar a autodeterminação informativa, a *accountability* e as possibilidades de controle do poder exercido pelos agentes de tratamento.

Nesse sentido, elucidou-se também que, para além da complexa discussão sobre segredos de negócio no mercado de dados, a LGPD acaba criando caminhos que reforçam a possibilidade de os agentes de tratamento utilizarem essa categoria jurídica como um escudo sob suas operações, dificultando ainda mais a transparência. Há, então, uma extensão de opacidade que pode ser criada pelos agentes de tratamento e que é consequência do uso dos segredos de negócio dentro do mercado.

O objetivo do presente estudo foi, portanto, (i) denunciar as dificuldades que existem ao tratar elementos do mercado de dados como segredos de negócio e (ii) indicar como a LGPD ignora essas dificuldades e acaba criando caminhos adicionais para que os agentes de tratamento explorem a categoria jurídica dos segredos de modo a aumentar ainda mais a opacidade sobre suas operações.

O trabalho também buscou apresentar reflexões propositivas, que colocam a garantia fundamental à proteção de dados pessoais como vetor normativo central da LGPD. A pretensão foi buscar contribuir para o debate que procura soluções para a tensão entre transparência e segredos de negócio, a fim de que seja possível fazer uma leitura da LGPD compatível com a proteção dos direitos fundamentais da privacidade e da proteção de dados pessoais.

Nesse sentido, defendeu-se que os conteúdos do mercado de dados, ainda que enquadrados como segredos de negócio, não estão resguardados em nível de sigilo

absoluto e, por isso, não podem obstar o acesso integral dos titulares e das autoridades sobre as explicações necessárias à compreensão das operações de tratamento de dados pessoais.

Também foram feitas reflexões sobre a importância de se diferenciar os destinatários das obrigações de transparência, a fim de compreender qual a extensão das explicações exigidas aos agentes de tratamento. Quando os destinatários forem os titulares de dados, devem-se avaliar suas limitações de racionalidade e as posições de assimetria informacional, a fim de avaliar qual tipo de conteúdo deve ser fornecido e em qual extensão os segredos de negócio não precisam ser disponibilizados.

Dificuldades do titular de dados, contudo, não podem impedir o acesso amplo aos dados pessoais que são coletados e tratados pelo agente. Ainda que em uma modalidade de visualização, o titular tem o direito de ter um acesso célere e sem custo sobre quais de seus dados pessoais foram coletados e são explorados, respeitando-se um formato de comunicação objetivo e simplificado.

Os titulares também devem ter o direito de acessar amplamente as informações sobre as metodologias e os critérios de tomada de decisões automatizadas. Novamente, deve-se observar que o nível de detalhamento dessas informações não precisa ser tão amplo, em razão das limitações de racionalidade do titular de dados. Mas não se pode autorizar que os segredos de negócio viabilizem uma recusa absoluta no fornecimento desse tipo de explicação ao titular, especialmente se considerado que as decisões automatizadas podem impactar tão fortemente no desenvolvimento da personalidade.

Defendeu-se, nesse aspecto, a necessidade de haver uma detalhada regulação setorial para cada atividade, a fim de que autoridades competentes possam avaliar as metodologias e os critérios de tomada de decisão, decidindo como essas informações devem ser fornecidas ao titular. No âmbito do risco de crédito, demonstrou-se que essas informações, ainda que protegidas por segredos de negócio, podem ser disponibilizadas, uma vez que os segredos de negócio não impõem um sigilo absoluto sobre os conteúdos. Por esse motivo, faz-se necessároa uma atualização da jurisprudência sobre a matéria, a fim de que se possa assegurar as dimensões de explicabilidade necessárias à autodeterminação informativa.

Outros elementos – como bases de dados, códigos e sintaxes matemáticas que compõem as operações – não necessariamente precisam ser fornecidos ao titular de dados para assegurar a autodeterminação informativa. Considerando todas as limitações que cercam o titular, bem como a sua posição de assimetria, elementos mais complexos e

sofisticados das operações podem acabar sendo prestigiados com maiores níveis de sigilo. Isso não impede, contudo, que existam circunstâncias específicas que possam impor a mitigação dos segredos de negócio.

À autoridade, por sua vez, pode ser imprescindível que se assegure um acesso mais amplo de todos os elementos que compõem o tratamento dos dados pessoais. Foi demonstrado que a autoridade é o único ente capaz de exercer um controle do poder dos agentes de tratamento. Também é a autoridade que consegue avaliar impactos coletivos das operações e riscos discriminatórios, além de ser ela a responsável pela promoção de uma cultura de proteção de dados que ainda é incipiente no Brasil.

O exercício de todas essas competências pode depender de diferentes níveis de acesso, os quais precisam ser avaliados caso a caso. Nesse sentido, o presente estudo propôs que as medidas possíveis de serem adotadas pela ANPD devem observar um escalonamento, conferindo níveis de sigilo proporcionais à explicabilidade necessária para o exercício de suas funções.

Em um primeiro momento, o acesso da autoridade deve se dar por meio dos esclarecimentos, dos Relatórios de Impacto e das auditorias, nos termos em que se encontram previstos em lei. Apesar de serem instrumentos que podem ter limitações, são meios suficientemente efetivos para instruir relevante parte das investigações conduzidas pela autoridade.

Em uma segunda etapa, se esses instrumentos iniciais se mostrarem insuficientes para os propósitos da atuação da autoridade, deve ser autorizada ao agente a possibilidade de criar medidas alternativas e soluções técnicas não especificadas em lei que consigam fornecer níveis maiores de explicabilidade. São iniciativas abertas que podem ser desenvolvidas pelos agentes no exercício de sua criatividade, a fim de que as explicações sejam fornecidas de forma menos invasiva, mas com o objetivo de atender aos interesses da autoridade.

Somente em um terceiro momento, se o agente não conseguir fornecer as explicações necessárias através de métodos alternativos, a autoridade poderá então requisitar acesso a elementos que são segredos de negócio. Para fazê-lo, deverá considerar que existem níveis de relevância entre os segredos de negócio e que, por isso, também existem níveis de sigilos e proteção do conteúdo que são diferentes. A autoridade deverá prestigiar a solicitação aos segredos de negócio menos sensíveis aos agentes, que possam se mostrar suficientes para complementar os esclarecimentos, os Relatórios de Impacto e as auditorias já realizadas.

Não só, a requisição dos segredos de negócio deverá demandar uma regulação específica por parte da autoridade, para que ela indique casos específicos e atividades de maior interesse público que poderão estar sujeitas a um escrutínio maior das operações. Essa é uma medida de segurança jurídica que precisa contemplar, ainda, a delimitação quanto aos níveis de acesso dos segredos de negócio.

O objetivo não é assegurar o acesso da autoridade aos códigos do agente de tratamento, mas apenas coibir que os segredos de negócio sejam utilizados como um óbice imediato à compreensão das operações. Por isso, a atuação da autoridade nessa última etapa deve se orientar pelos juízos de razoabilidade e proporcionalidade, para que o acesso aos segredos de negócio realmente esteja inserido dentro de um escopo de necessidade. Os agentes de tratamento, por sua vez, empenharão esforços maiores para cumprir as exigências da autoridade antes de se chegar nessas medidas mais gravosas.

Em contrapartida, a autoridade deverá assegurar aos agentes de tratamento a existência de uma estrutura suficientemente segura para a preservação dos segredos de negócio eventualmente fornecidos. Isso envolve obrigações de segurança da informação, sistemas que comportem o acesso desses conteúdos, compromisso de sigilo de seus funcionários e mecanismos para que, findas as investigações, esses conteúdos sejam deletados e nenhum prejuízo à atividade empresarial seja causado.

As soluções propostas são apenas reflexões iniciais sobre um necessário aprimoramento do sistema de proteção de dados pessoais. Ainda que o mercado em estudo não seja propriamente democrático e, em grande medida, perpetue discriminações e concentração de poder nas mãos de poucos agentes, deve-se pensar em consolidar um ordenamento jurídico focado na promoção de garantias fundamentais. Refletir sobre como os segredos de negócio se inserem dentro da proteção de dados é um primeiro passo para isso, tentando-se eliminar barreiras que impeçam a transparência possível no contexto atual.

REFERÊNCIAS

A POUSADA do Bom Barão. Intérprete: Os Saltimbancos. Compositores: Chico Buarque, Luis Bacalov, Sergio Bardotti. *In*: Os Saltimbancos. Intérprete: Os Saltimbancos. [*S. l*] Universal Music Ltd., 1977. 1 CD: faixa 8.

ACEMOGLU, Daron *et al*. Too Much Data: Prices and Inefficiencies in Data Markets. *American Economic Journal*: Microeconomics. v. 14, n. 4, 2022. Disponível em: https://www.aeaweb.org/articles?id=10.1257/mic.20200200. Acesso em: 27 nov. 2023.

ACEMOGLU, Daron; OZDAGLAR, Asu; SIDERIUS, James. Misinformation: Strategic Sharing, Homophily and Endogenous Echo Chambers. *NBER Working Paper* No. 28884. 2021.

ACEMOGLU, Daron; RESTREPO, Pascual. The Race between Man and Machine: Implications of Technology for Growth, Factor Shares, and Employment. *American Economic Review*, v. 108, n. 6. p. 1488-1542, 2018. Disponível em: https://www.aeaweb.org/articles?id=10.1257/aer.20160696. Acesso em: 10 fev. 2024.

ACEMOGLU, Daron. Harms of AI. *National Bureau of Economic Research*. 2021. Disponível em: https://www.nber.org/papers/w29247. Acesso em: 18 nov. 2023.

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Primeira Secção), 7 de dezembro de 2023. InfoCuria. 2023. Disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=24E21076CD67811091 2F514CAF865B96?text=&docid=280426&pageIndex=0&doclang=pt&mode=lst&dir= &occ=first&part=1&cid=1302015. Acesso em: 25 maio 2024.

AFFELT, Amy. Big Data, Big Opportunity. *Australia Law Librarian*, vol. 21, n. 2, 2013. p. 1. Disponível em: https://www.researchgate.net/publication/269697881_Big_Data_Big_Opportunity. Acesso em: 11 abr. 2023.

ALAPANIAN, Silvia. A crítica marxista do Direito: um olhar sobre as posições de Evgeni Pachukanis. *Semina*: *Ciências Sociais e Humanas*, Londrina, v. 26. p. 15- 26, set. 2005. Disponível em: https://ojs.uel.br/revistas/uel/index.php/seminasoc/article/view/3794/3050. Acesso em: 04 maio 2024.

ALBERS, Marion. A complexidade da proteção de dados. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 10, n. 35. 2016. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/93. Acesso em: 4 maio 2024.

ALLEN, Anita L. Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform. *The Yale Law Journal Forum*, February 2022. Disponível em: https://www.yalelawjournal.org/forum/dismantling-the-black-opticon. Acesso em: 11 jan. 2023.

AMORIM, Ana Clara Azevedo de. O regime jurídico dos segredos comerciais no novo Código de Propriedade Industrial. *Revista Electrónica de Direito*, n. 2, v. 19, jun., 2019. Disponível em: https://cij.up.pt/client/files/0000000001/2-ana-clara-amorim_927.pdf. Acesso em: 22 maio 2024; LEE, N. Open yet secret - trading of tangible goods and trade

secrets. *In*: BRUUN, Niklas; DINWOODIE, Graeme B.; LEVIN, Marianne; OHLY, Ansgar (eds.). *Transition and Coherence In Intellectual Property Law*: Essays in Honour of Annette Kur. Cambridge: Cambridge University Press, 2021.

ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Midia & Society*, 20(3), 2018. Disponível em: https://doi.org/10.1177/1461444816676645. Acesso em: 12 out. 2023.

APLIN, Tanya; RADAUER, Alfred; BADER, Martin A.; SEARLE, Nicola. The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis. *National Library of Medicine*. 2023, tradução nossa. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10170042/#Fn53. Acesso em:10 fev. 2024.

APPADURAI, Arjun. Disjuncture and Difference in the Global Cultural Economy. *Theory, Culture & Society*, v. 7, n. 2-3, 1990. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/026327690007002017. Acesso em: 04 maio 2024.

ASCARELLI, Tullio. *Teoria della Concorrenza e dei Beni Immateriali.* Istituzioni di diritto industriale. 3. ed., Milão: Griuffrè.1960.

AUSTIN, Lisa M. *Enough About Me*: Why Privacy is About Power. A World Without Privacy? What Can / Should Law Do. Cambridge, 2014.

AUTORIDADE Europeia para a Proteção de Dados. *Jornal Oficial da União Europeia*. 2014. Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_ex_sum_pt_0.pdf. Acesso em: 18 fev. 2024.

ÁVILA, Humberto. *Teoria dos Princípios*: da definição à aplicação dos princípios jurídicos. 4. ed. São Paulo: Editora Malheiros, 2022.

AYRES, Ian; BRAITHWAITE, John. *Responsive Regulation*: Transcending the Deregulation Debate. New York: Oxford University Press, 1992.

Banco Central do Brasil. Open Finance. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/openfinance. Acesso em: 10 fev. 2024.

BANTERLE, Francesco. 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. *In*: BAKHOUM, Mor; CONDE GALLEGO, Beatriz; MACKENRODT, Mark-Oliver M.; SURBLYTĖ-NAMAVIČIENĖ, Gintaré (eds.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law*: Towards a Holistic Approach? Springer: Berlin, 2018.

BANTERLE, Francesco. 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. *In*: BAKHOUM, Mor; CONDE GALLEGO, Beatriz; MACKENRODT, Mark-Oliver M.; SURBLYTĖ-NAMAVIČIENĖ, Gintaré (eds.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law*: Towards a Holistic Approach? Springer: Berlin, 2018.

BARBOSA, Denis Borges. Exclusividade de dados sigilosos: agroquímicos. *In*: BARBOSA, Denis Borges. *Da Tecnologia à Cultura*: ensaios e estudos de Propriedade Intelectual. Rio de Janeiro: Lumen Juris, 2011. Disponível em: https://www.dbba.com.br/wp-content/uploads/tecnologia_a_cultura.pdf Acesso em: 23 mar. 2024.

BARBOSA, Denis Borges. Tratado da Propriedade Intelectual: Tomo III. 2. ed. Rio de Janeiro: Lumen Juris, 2017.

BARBOSA, Denis Borges. *Uma introdução à propriedade intelectual*. 2. ed. Lumen Juris, 2010. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 21 mar. 2024.

BARBOSA, Pedro Marcos Nunes. *Curso de Concorrência desleal*. Rio de Janeiro: Lumen Juris, 2022.

BARNES, Susan B. A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 1-10, 2006. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/1394. Acesso em: 11 nov. 2023.

BARNES, Susan B. A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 1-10, 2006. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/1394. Acesso em: 11 nov. 2023.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. *In*: LANE, Julia; STODDEN, Victoria; BENDER, Stefan;

BAROCAS, Solon; SELBST, Andrew D. Big Data's disparate impact. California Law Review, 2016.

BASSO, Maristela. A proteção da propriedade intelectual e o direito internacional atual. *Revista de Informação Legislativa*, Brasília, v. 41, n. 162. p. 287-309, abr./jun. 2004. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/965. Acesso em: 22 maio 2024.

BASSO, Maristela. *O direito internacional da propriedade intelectual*. Porto Alegre: Livraria do Advogado, 2000.

BASSO, Maristela. Os fundamentos atuais do direito internacional da propriedade intelectual. *Revista CEJ*. Brasília, v. 7, n. 21, jun. 2003. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/541. Acesso em: 22 maio 2024).

BAYAMLIOĞLU, Emre. Contesting Automated Decisions. *European Data Protection Law Review*, v. 4, 2018. Disponível em: https://ssrn.com/abstract=3305272. Acesso em: 16 abr. 2024.

BEER, David. Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society*, 11(6), 2009. Disponível em: https://journals.sagepub.com/doi/10.1177/1461444809336551. Acesso em: 12 ago. 2023.

BEER, David. The social power of algorithms. *Information, communication & society*, 20:1, 1-13, 2016. p. 8-9. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2016.1216147?needAccess=true. Acesso em: 08 abr. 2022.

BENKLER, Yochai. *The Wealth of Networks*: How Social Production Transforms Markets and Freedom. Yale University Press, 2006.

BENTLY, Lionel. Trade secrets. 'intellectual property' but not 'property'? *In*: HOWE, Helena R.; GRIFFITHS, Jonathan (eds.). *Concepts of Property in Intellectual Property Law*. Nova York: Cambridge University Press, 2013

BERGEMANN, Dirk; BONATTI, Alessandro; GAN, Tan. The Economics of Social Data. *Cowles Foundation Discussion Paper No. 2203R4*. New Haven, Connecticut. 2019. Disponível em: https://www.mit.edu/~bonatti/social.pdf. Acesso em: 27 nov. 2023.

BERMAN, Paul Schiff. *Global Legal Pluralism*. A Jurisprudence of law Beyond Borders. Cambridge University Press, 2012.

BERTONCELLO, Káren Rick Danilevicz. Fluência algorítmica: concretização do dever de informação e de explicabilidade na concessão do crédito ao consumidor. *In*: MARQUES, Claudia Lima *et al*. (coord). *5 anos de LGPD*: estudos em homenagem a Danilo Doneda. São Paulo: Thomson Reuters Brasil, 2023 [livro eletrônico].

BESSA, Leonardo Roscoe. *Nova Lei de Cadastro Positivo*: comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2019.

BIONI, Bruno Ricardo. Legítimo Interesse: Aspectos gerais a partir de uma visão obrigacional. *In*: DONEDA, Danilo *et. al.* (coord). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2017.

BIONI, Bruno. *Proteção de Dados Pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense. 2019.

BIONI, Bruno. *Regulação e proteção de dados pessoais*: o princípio da *accountability*. Rio de Janeiro: Forense, 2022.

BLACK, Julia. Constitutionalizing Regulatory Governance Systems. *LSE Legal Studies Working Papers*, n. 02/2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3813812. Acesso em: 15 nov. 23.

BLACK, Julia. Decentering regulation: Understanding the Role of Regulation and Self-Regulation in a "Post Regulatory" World. *Current Legal Problems*, Volume 54, Issue 1, 2001, Pages 103–146, 01 December 2001. Disponível em: https://doi.org/10.1093/clp/54.1.103. Acesso em: 08 maio 2023.

BOBBIO, Norberto. *Contribución a la teoría del derecho*. Madrid: Editorial Debate, 1990.

BODIN DE MORAES, Maria Celina; QUINELATO, João. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *CADERNOS ADENAUER*, São Paulo, v. 3. p. 1-17, 2019.

BONE, Robert G. Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions. *In*: DREYFUSS, Rochelle C.; STRANDBERG, Katherine J. (eds.). The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research. Edward Elgar Press, 2010. *Boston Univ. School of Law Working Paper* No. 09-40. Disponível em: https://ssrn.com/abstract=1467723. Acesso em:10 mar. 2024.

BOSCO, Natália. Ataque de hackers ao STJ é o mais grave da história no país. *Correio Braziliense*. 2020. Disponível em: https://www.correiobraziliense.com.br/brasil/2020/11/4886936-ataque-de-hackers-ao-stf-e-o-mais-grave-da-historia-no-pais.html. Acesso em: 13 jul. 2024.

BOURDIEU, Pierre; WACQUANT, Loic. *An invitation to reflexive sociology*. Cambridge: Polity Press, 1992 e LUNDAHL, O. Algorithmic meta-capital: Bourdieusian analysis of social power through algorithms in media consumption. *Information, Communication & Society*, v. 25 (10), 2022. Disponível em: https://research.rug.nl/files/232459855/1369118X.2020.pdf. Acesso em: 10 mar. 2024.

BRASIL. Comunicação de incidente de segurança. *gov.br*. 2022. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 14 mar. 2024.

BUCHER, Taina. *If...Then*: Algorithmic power and politics. Oxford University Press, 2018.

BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 19 dez. 2023.

BUSUIOC, Madalina. Accountable artificial intelligence: holding algorithms to account. Public Administration Review, v. 81, n. 5. Sept./Oct. 2021. p. 829, tradução nossa. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/puar.13293. Acesso em: 18 abr. 2024.

CALO, Ryan; CITRON, Danielle. The Automated Administrative State: A Crisis of Legitimacy. *Emory Law Journal*, v. 70. p. 797–846, 2021. Disponível em: https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj. Acesso em: 19 out. 2023.

CAMPOS, Ricardo. *Metamorfoses do direito global*: Sobre a interação entre direito, tempo e tecnologia. São Paulo: Editora Contracorrente, 2022.

CARLSON, Alyssa M. The Need for Transparency in the Age of Predictive Sentencing Algorithms. *Iowa Law Review*, Vol. 103, 2017. p. 322-329. Disponível em: https://ilr.law.uiowa.edu/print/volume-103-issue-1/the-need-for-transparency-in-the-age-of-predictive-sentencing-algorithms. Acesso em: 12 maio 2024.

CARLSON, Alyssa M. The Need for Transparency in the Age of Predictive Sentencing Algorithms. *Iowa Law Review*, Vol. 103, 2017. Disponível em:

https://ilr.law.uiowa.edu/print/volume-103-issue-1/the-need-for-transparency-in-the-age-of-predictive-sentencing-algorithms. Acesso em: 12 maio 2024.

CARR, Nicholas G. *What the Internet is Doing to Our Brains*. Nova York: Norton, 2010.

CASTELLS, Manuel. *The network Society*. A Cross-cultural Perspective. Northampton, MA: Edward Elgar, 2004.

CAVOUKIAN, Ann. Privacy by Design The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. *Information & Privacy Commissioner*, Ontario, Canada, v. 5, 2009. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Acesso em: 17 dez. 2020.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers and Technology*, v. 33, n. 1, p. 76–99, 2019.

CERQUEIRA, João da Gama. Tratado da Propriedade Industrial. Vol. 1, parte 1. Editora Lumen Juris: Rio de Janeiro, 2010.

CESARINO, Letícia. O mundo do avesso: verdade política na era digital. São Paulo: Ubu Editora, 2022.

CHESBROUGH, Henry. The Future of Open Innovation. The future of open innovation is more extensive, more collaborative, and more engaged with a wider variety of participants. *Research-Technology Management*. 60 (1), 2017. Disponível em: https://doi.org/10.1080/08956308.2017.1255054. Acesso em: 12 jan. 2024).

CHNEYE-LIPPOLD, John. A new algorithmic Identidy. Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*. SAGE, Los Angeles, London, New Delhi and Singapore, vol. 28 (6), 2011.

CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, Vol. 89, 2014, U of Maryland Legal Studies Research Paper No. 2014-8. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 12 maio 2024.

CITRON, Danielle Keats. Open Code Governance. *University of Chicago Legal Forum*, vol. 2008, n. 1, 2008, Artigo 9. Disponível em: http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/9. Acesso em: 27 abr. 2024.

CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, 85, 1249, 2008. Disponível em: https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2. Acesso em: 02 mar. 2024.

COECKELBERGH, Mark. Artificial intelligence, responsibility attribution, and a relational justification of explainability. *Science and Engineering Ethics*, v. 26, 2020. Disponível em: https://link.springer.com/article/10.1007/s11948-019-00146-8. Acesso em: 12 mar. 2024.

COELHO, Fábio Ulhoa. Curso de direito civil: direito das coisas, direito autoral, vol. 4 [livro eletrônico]. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

COGLIANESE, Cary; LAMPMANN, Erik. Contracting for Algorithmic Accountability. *Administrative Law Review Accord*, v. 6. p. 175, 2021. p. 186. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 12 abr. 2024.

COGLIANESE, Cary; LAMPMANN, Erik. Contracting for Algorithmic Accountability. *Administrative Law Review Accord*, v. 6. 2021. Disponível em: https://administrativelawreview.org/wp-content/uploads/sites/2/2021/10/Coglianese-Lampmann_For-ACCORD-1.pdf. Acesso em: 12 abr. 2024.

COHEN, Julie E. *Between Truth and Power*: The Legal Constructions of Informational Capitalism. Oxford University Press, 2019.

COHEN, Julie E. Turning Privacy Inside Out. *Theoretical Inquiries in Law 20.1 (2019 Forthcoming)*, 2018. Disponível em: https://ssrn.com/abstract=3162178. Acesso em: 10 out. 2023.

COHEN, Wesley; NELSON, Richard R.; WALSH, John P. Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not). 2000. *National Bureau of Economic Research Working Paper* 7552. Disponível em: http://www.nber.org/papers/w7552. Acesso em: 09 abr. 2024.

COMMISSION européenne/Europese Commissie. ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion on the notion of legitimate interests of the data controller. *Opinion 06/2014*. p. 24. Disponível em: https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf. Acesso em: 17 abr. 2024.

CONVERGÊNCIA Digital. Operadora de telecom sofre mega ataque hacker e governo da Colômbia é obrigado a parar atividades. *Convergência Digital*. 2023. Disponível em: https://encurtador.com.br/C4UWA. Acesso em: 13 jul. 2024.

COULDRY, Nick; MEJIAS, Ulisses A. A Data Colonialism: rethinking big data's relation to contemporary subject. *Television & New Media*, v. 20, n. 4. 2019.

COULDRY, Nick; MEJIAS, Ulisses Ali. *The costs of connection*: how data is colonizing human life and appropriating it for capitalism. Stanford, California: Stanford University Press, 2019.

CRAVO, Daniela. O direito à portabilidade na Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023.

CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, v. 55, n. 93, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784. Acesso em: 12 mar. 2024

CRUZ, Carolina. Diretora da ANPD aponta limites do segredo comercial. *TeleSíntese*. 2022. Disponível em: https://www.nic.br/noticia/na-midia/diretora-da-anpd-aponta-limites-do-segredo-comercial/\. Acesso em: 24 fev. 2024.

CUEVA, Ricardo Villas Bôas. A importância de proteger o segredo de negócio. *In* CALCINI, Ricardo; ANDRADE, Dino (org.). *Reflexões Jurídicas Contemporâneas*. Leme-SP: Mizuno, 2022.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023.

CUEVA, Ricardo Villas Bôas. Alternativas para a remoção de fake news das redes sociais. *In*: MENDES, Gilmar Ferreira; MORAIS, Carlos Blanco. *Reforma do Estado Social no contexto da globalização*. Rio de Janeiro: FGV Projetos, 2018.

DA EMPOLI, Giuliano. *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. São Paulo: Vestígio, 2020.

DE ÁVILA, Sergio marcos Carvalho; KORKMAZ, Maria Regina Rigolon. Decisões automatizadas e a proteção de crianças e adolescentes. *In*: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (coord.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro: Obliq, 2021. E-book.

DENEEN, Patrick J. *Por que o liberalismo fracassou?* Editora Âyiné, 2020. p. 127. Tradução de Rogério W. Galindo.

DERCLAYE, Estelle; HUSOVEC, Martin. Sui Generis Database Protection 2.0: Judicial and Legislative Reforms. *European Intellectual Property Review (EIPR)* – Forthcoming, november 16, 2021. p. 7. Disponível em: http://dx.doi.org/10.2139/ssrn.3964943. Acesso em: 10 fev. 2024.

DESAI, Deven R.; KROLL, Joshua A. Trust But Verify: A Guide To Algorithms And The Law. *Harvard Journal Of Law & Technology*, v. 31, 2017. Disponível em: https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech1.pdf. Acesso em: 13 fev. 2024.

DEVITO, Michael Ann. Adaptive folk theorization as a path to algorithmic literacy on changing platforms. *Proceedings of the ACM Conference on Human-Computer Interaction*, *5* (CSCW2). 2021. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3476080. Acesso em: 20 dez. 2023.

DIAKOPOULOS, Nicholas; FRIEDLER, Sorelle. How To Hold Algorithms Accountable. *MIT Technology Review*, 17 nov. 2016. Disponível em: https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/. Acesso em: 2 maio 2024.

DIAKOPOULOS, Nicholas. Algorithmic Accountability Reporting: On the Investigation of Black Boxes. *Columbia Journalism School*. 2014. Disponível em:

https://academiccommons.columbia.edu/doi/10.7916/D8TT536K/download. Acesso em: 03 nov. 2023.

Directiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996 relativa à protecção jurídica das bases de dados. *Jornal Oficial das Comunidades Europeias*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31996L0009. Acesso em: 10 fev. 2024.

Directiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996 relativa à protecção jurídica das bases de dados. *Jornal Oficial das Comunidades Europeias*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31996L0009. Acesso em: 10 fev. 2024.

DÖHMANN, Indra Spiecker genannt. The legal framework for access to data from a data protection viewpoint – especially under the RGPD. *In*: Bundesministerium Der Justiz Und Für Verbraucherschutz; Max-Planck-Institut Für Innovation Und Wettbewerb. *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos, 2021.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. What Is Algorithm Governance? *IEEE Internet Computing*, v. 20., 2016. Disponível em: https://www.researchgate.net/publication/305801954_What_Is_Algorithm_Governance. Acesso em: 12 nov. 2023.

DONEDA, Danilo; ALMEIDA, Virgílio. O que é governança de algoritmos. *In*: BRUNO, Fernanda *et al*. *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

DONEDA, Danilo. A Autoridade Nacional de Proteção de Dados. *In*: DONEDA, Danilo *et. al.* (coord). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2017.

DONEDA, Danilo. Os Direitos da Personalidade no Código Civil. *Revista da Faculdade de Direito de Campos*, Ano VI, No 6 - Junho de 2005. Disponível em: https://egov.ufsc.br/portal/sites/default/files/os_direitos_de_personalidade_no_codigo_civil.pdf. Acesso em: 11 abr. 2022).

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo *et al*. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. Palestra no Seminário Interamericano de Transparência e Acesso à Informação promovido em 2017 pela Organização dos Estados Americanos (OEA) e pelo Governo Federal do Brasil. Disponível em: https://www.gov.br/cgu/pt-br/acesso-a-informacao/institucional/eventos/anos-anteriores/2017/5-anos-da-lei-de-acesso/arquivos/mesa-3-danilo-doneda.pdf. Acesso em: 26 agosto 2024.

DREXL, Josef; HILTY, Reto M. *et al.* Data Ownership and Access to Data. Position Statement on the Current European Debate. *Max Planck Institute for Innovation and Competition*, 16 August 2016.

EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, v. 16, maio 2017. Disponível em: https://ssrn.com/abstract=2972855. Acesso em: 10 abr. 2024.

EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, v. 16. maio 2017. Disponível em: https://ssrn.com/abstract=2972855. Acesso em:10 abr. 2024.

EDWARDS, Michael. *Future Positive*: International Co-operation in the 21st Century. London: Earthscan, 1999.

EUROPEAN COMMISSION. Study On The Legal Protection Of Trade Secrets In The Context Of The Data Economy (GRO/SME/20/F/206). *European Commission.* 2022. Disponível em: https://research.gold.ac.uk/id/eprint/32803/2/study%20on%20the%20legal%20protection%20of%20trade%20secrets%20in-EA0922449ENN.pdf. Acesso em: 08 fev. 2024.

EUROPEAN Parliament. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html. Acesso em: 15 abr. 2024.

EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE (EUIPO). PROTECTING INNOVATION THROUGH TRADE SECRETS AND PATENTS: DETERMINANTS FOR EUROPEAN UNION FIRMS. p. 23-57. Disponível em: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf. Acesso em: 23 abr. 2024.

FAUSTINO, Deivison; LIPPOLD, Walter. *Colonialismo Digital*: por uma crítica hacker-fanoniana. São Paulo: Boitempo, 2023.

FEENBERG, Andrew. *Between Reason And Experience*. Essays in Technology and Modernity. Cambridge: The MIT Press, 2010.

FEENBERG, Andrew. Critical Theory of Technology: An Overview. *Tailoring Biotechnologies*, vol. 1, Issue 1, Winter 2005. Disponível em: https://www.sfu.ca/~andrewf/books/critbio.pdf. Acesso em: 09 out. 2023.

FEKETE, Elisabeth Kasznar. *O regime jurídico do segredo de indústria e comércio no direito brasileiro.* Rio de Janeiro: Forense, 2003.

FEKETE, Elisabeth Kasznar. Segredo de Empresa. *In*: COELHO, Fábio Ulhoa; ALMEIDA, Marcus Elidius Michelli de (coord.). *Enciclopédia Jurídica da PUCSP.* tomo IV (recurso eletrônico): direito comercial. São Paulo: Pontifícia Universidade Católica de São Paulo, 2018. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso em: 13 maio 2024.

FEKETE, Elizabeth Kasznar. Segredo de Justiça. In: ABBOUD, Georges; BARBOSA, Pedro Marcos Nunes (coord.). *Direito processual da propriedade intelectual* [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2023.

FELIPE, Bruno Farage da Costa; MULHOLLAND, Caitlin Sampaio. Filtro bolha e *big nudging*: a decomocracia participativa na era dos algorítimos. *Rev. direitos fundam. democ*., v. 27, n. 3. set./dez. 2022. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/download/2275/753/6074. Acesso em: 14 mar. 2024.

FERRANTE, Elena. *A filha perdida*. Intrínseca: São Paulo, 2016.

FERRARESE, Maria Rosaria. An entrepreneurial conception of Law? The American model through Italian eyes. In: NELKEN, David. Comparing Legal Cultures. Nova York: Routledge, 2016.

FERRARESE, Maria Rosaria. Europe and institutional change. Law: from science to "fit for purpose"? *Économie et institutions.* v. 23, 2015. Disponível em: https://doi.org/10.4000/ei.5718. Acesso em: 02 jun. 2024.

FERRARESE, Maria Rosaria. Governance: a soft revolution with hard political and legal effects. *Soft Power*, [S. l.], v. 1, n. 1. 2014. Disponível em: https://editorial.ucatolica.edu.co/index.php/SoftP/article/view/1765. Acesso em: 2 jun. 2024.

FERRARI, Isabela; BECKER, Daniel. O direito à explicação sobre decisões automatizadas: uma análise comparativa entre a União Europeia e o Brasil. Revista de Direito e as Novas Tecnologias, vol. 01, out-dez, 2018.

FERRARI, Isabela. O emprego de algoritmos para a Tomada de Decisões I – Como funcionam os algoritmos não programados? *In*: FERRARI, Isabela. *Justiça Digital*. São Paulo: Thomson Reuters Brasil, 2020.

FERREIRA FILHO, Alberto Esteves. *Licenciamento de Know-How*: considerações sobre sua legalidade e os atos do INPI. São Paulo: Editora Dialética, 2022.

FERREIRA, Waldemar. *Tratado de Direito Comercial*. O estatuto do estabelecimento e a empresa mercantil. vol. 7. Editora Saraiva: São Paulo, 1962.

FISHER, Max. *The Caos Machine*. The inside story of how social media rewired our minds and our world. New York: Little, Brown and Company, 2022.

FLIGSTEIN, Neil; CALDERS, Ryan. *Architecture of Markets. Emerging Trends in the Social and Behavioral Sciences*. John Wiley & Sons, Inc, 2015.

FONTES, André R. C. Patente, invenção e inovação. *Revista da Escola da Magistratura Regional Federal* / Escola da Magistratura Regional Federal, Tribunal Regional Federal da 2ª Região. Edição Especial de Propriedade Intelectual. Rio de Janeiro, 2011.. Disponível em: https://emarf.trf2.jus.br/site/documentos/revistapinternet2011.pdf. Acesso em: 12 jan. 2024.

FOURWEEKBMBA. Receitas do Facebook. Disponível em: https://fourweekmba.com/pt/receitas-do-facebook/. Acesso em: 04 jul. 2024.

FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de Proteção de Dados Pessoais*: fundamentos da LGPD. Rio de Janeiro: Forense, 2022.

FRAZÃO, Ana. Obstáculos para a consideração de questões éticas nos julgamentos algorítmicos. *In*: FEFERBAUM, Marina *et al*. (coord.). *Ética, Governança e Inteligência Artificial*. São Paulo: Almedina, 2023.

FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de compliance e das políticas de proteção de dados. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021.

FRIEDMAN, Batya; NISSENBAUM, Helen. *Bias in Computer Systems*. ACM Transactions on Information Systems, v. 14, n. 3, 1996.

FRIEDMAN, David D.; LANDES, William M.; POSNER, Richard A. Some Economics of Trade Secret Law. *Journal of Economic Perspectives*, 5 (1), 1991. Disponível em: https://www.aeaweb.org/articles?id=10.1257/jep.5.1.61. Acesso em: 29 jan. 2024.

FURTADO, Lucas Rocha. *Curso de Direito Administrativo*. 4. ed. Belo Horizonte: Fórum, 2013.

GALVÃO, Luiz Antonio. *Troca indireta de informações entre concorrentes*: os limites do ilícito concorrencial. Dissertação de Mestrado. Universidade de São Paulo. Programa de Pós-Graduação em Direito. São Paulo, 2018. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2132/tde-17092020-170014/publico/6487512_Dissertacao_Parcial.pdf. Acesso em: 18 fev. 2024

GAON, Aviv H. *The Future of Copyright in the Age of Artificial Intelligence*. Elgar Law, Technology and Society series, 2021; LESSIG, Lawrence. *Free culture*: the nature and future of creativity. Penguin Books, 2004.

GERALDES, João de Oliveira. Sobre a proteção jurídica dos segredos comerciais no espaço digital. *Revista da Faculdade da Universidade de Lisboa*, vol. LXIII, 1 e 2, Lisboa, 2022. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Joa%CC%83o-de-Oliveira-Geraldes_compressed.pdf. Acesso em: 06 out. 2023.

GIL, Gabriel de Siqueira; HIRSCHFELD, María Noel C. Extrativismo hi-tech e expansão capitalista no século XXI: uma breve contribuição para a crítica latino-americana na era do colonialismo de dados. *In*: PARANÁ, Edemilson; KAMINSKI, Ricardo S. (org.). *Tecnologia e Desenvolvimento nas Américas*: novas fronteiras e dilemas do capitalismo contemporâneo. Curitiba, 2021.

GILLESPIE, Tarleton. The Politics of "Platforms". *New Media & Society*, vol 12, n. 3, 2010, tradução nossa. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1601487. Acesso em: 11 nov. 23.

GILLESPIE, Tarleton. The relevance of algorithms. *In*: GILLESPIE, T.; GILLESPIE, Tarleton; BOCZKOWSKI, Pablo J.; FOOT, Kirsten A. *Media Technologies*: Essays on Communication, Materiality, and Society. MIT Press, 2014. Traduzido por Amanda Jurno mediante autorização do autor e da editora. Revisão: Carlos d'Andréa. *§ Parágrafo*, São Paulo, Brasil, v. 6, n. 1. p. 95-121, jan./abr. 2018 Disponível em: https://edisciplinas.usp.br/pluginfile.php/5971548/mod_resource/content/1/722-2195-1-PB.pdf. Acesso em: 25 dez. 2023.

GÓMEZ-GONZÁLEZ, Emilio; GÓMEZ, Emilia. *Artificial intelligence in medicine and healthcare*: Applications, availability and societal impact. Luxembourg: Publications Office of the European Union, 2020.

GRAU, Eros Roberto. *A Ordem econômica da Constituição de 1988* [interpretação crítica]. 14. ed. São Paulo: Editora Malheiros, 2010.

GREEN, Ben. Data Science as Political Action: Grounding Data Science in a Politics of Justice. *Journal of Social Computing*, vol. 2, no. 3. 2021.Disponível em: https://doi.org/10.23919/JSC.2021.0029. Acesso em: 29 mar. 2023.

GRIMMELMANN, James. The Structure of Search Engine Law. *Iowa Law Review*, v. 93, n. 1, 2007. NYLS Legal Studies Research Paper No. 06/07-23.Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=979568. Acesso em: 01 maio 2024.

GRINOVER, Ada Pellegrini *et al*. *Código Brasileiro de Defesa do Consumidor*. 13. ed. Reio de Janeiro: Forense, 2022.

GUERREIRO, José Tavares *et al*. *Comentários ao Código do Consumidor*. (José Cretella Júnior e René Ariel Dotti - coord). Rio de Janeiro: Forense, 1992.

HALL, Bronwyn H. *et al*. The importance (or not) of patents to UK Firms. 2013. *NBER Working Paper* No. 19089. Disponível em: http://www.nber.org/papers/w19089. Acesso em: 9 abr. 2024.

HARTMANN, Ivar; MONTEIRO, Julia. Fake News no Contexto de Pandemia e Emergência Social: os Deveres e Responsabilidades das Plataformas de Redes Sociais na Moderação de Conteúdo Online: entre a Teoria e as Proposições Legislativas. *Revista de Direito Público*. v. 17, n. 94, p. 388-414, jul./ago. 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4607. Acesso em: 03 abr. 2024.

HARVEY, David. *A loucura da razão econômica*. Marx e o capital no século XXI. São Paulo: Boitempo, 2018.

HERT, Paulo de. Accountability and system responsibility: new concepts in data protection law and human rights. *In*: GUAGNIN, Daniel *et al.* (org). *Managing Privacy through Accountability*. London: Palgrave Macmillan UK, 2012.

HESSE, Konrad. *A força normativa da constituição*. Tradução: Gilmar Ferreira Mendes. Porto Alegre: Sergio Antonio Fabris Editor, 1991.

HILDEBRANDT, Mireille. Algorithmic regulation and the rule of law. *Philosophical Transactions Royal Society Publishing*. A 376, n. 20170355, 2018. Disponível em: http://dx.doi.org/10.1098/rsta.2017.0355. Acesso em: 19 out. 2023.

HILDEBRANDT, Mireille. Defining profiling: a new type of knowledge? In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. *Profiling the European citizen*: cross-disciplinary perspectives. [S.l.]: Springer Netherlands, 2008.

HILDEBRANDT, Mireille. Preregistration of Machine Learning Research Design. Against P-hacking. *In*: BAYAMLIOLGU, Emre; BARALIUC, Irina; JANSSENS, Lisa; HILDEBRANDT, Mireille (eds.). *Being Profiled*: Cogitas Ergo Sum. Amsterdam University Press, 2018.

HILDEBRANDT, Mireille. *Smart Technologies and the End(s) of Law*. Novel Entanglements of Law and Technology. Northampton, MA: Edward Elgar Publishing, 2015.

HOFFMANN-RIEM, Wolfang. *Teoria do Direito Digital*: transformação digital: desafios para o Direito. Rio de Janeiro: Forense, 2022.

IETA, Vânia Siciliano. O Impacto Eleitoral Resultante da Manipulação das Fake News no Universo das Redes Sociais: a Construção da Desinformação. *Revista Interdisciplinar do Direito* - Faculdade de Direito de Valença, [S. l.], v. 18, n. 1. 2020. Disponível em: https://revistas.faa.edu.br/FDV/article/view/848. Acesso em: 01 maio 2024.

INSTITUTO Igarapé. Infográfico: Reconhecimento Facial no Brasil. *Igarapé*. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 25 abr. 24; Instituto Igarapé. Mais Câmeras, Mais Segurança. Disponível em: https://igarape.org.br/mais-cameras-mais-seguranca/. Acesso em: 25 abr. 2024.

IRTI, Natalino. A ordem jurídica do mercado. *Revista de direito mercantil, industrial, econômico e financeiro*. Publicação do Instituto Brasileiro de Direito Comercial Comparado e Biblioteca Tullio Ascarelli do Departamento de Direito Comercial da Faculdade de Direito da Universidade de São Paulo. Ano XLVI (nova série), janeiro-março/2007. Malheiros Editores.

JAMAR, Steven D. Trade Secrets from an IP Social Justice Perspective (November 16, 2021). Trade Secrets from an IP Social Justice Perspective, in Cambridge Handbook on IP-SJ (Steven D. Jamar & Lateef Mtima editors (forthcoming Cambridge University Press 2022). *Howard Law Research Paper*. Disponível em: http://dx.doi.org/10.2139/ssrn.3964977. Acesso em: 19 fev. 2024.

JANAL, Ruth. Data portability under the GDPR: A blueprint for access rights? *In*: German Federal Ministry of Justice and Consumer Protection | Max Planck Institute for Innovation and Competition (eds.). *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos. 2021.

JOH, Elizabeth E. Feeding the Machine: Policing, Crime, Data & Algorithms. *J. Willians & Marry Bill of Rights Journal*, vol. 26, issue 2, article 3, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3020259. Acesso em: 11 dez. 2023.

KAMINSKI, Margot E. Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability. *South California Law Review*, v. 92. 2019. Disponível em: https://scholar.law.colorado.edu/faculty-articles/1265/. Acesso em: 17 mar. 2024.

KAMMOURIEH, Lenah *et al*. Group Privacy in the Age of Big Data. *In*: TAYLOR, Linnet; FLORIDI, Luciano; VAN DER SLOOT, Bart. *Group Privacy*: New Challenges of Data Technologies. Springer, 2017.

KARTIK, Hosanagar; MILLER, Alex P. Who Do We Blame for the Filter Bubble. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020.

KAUFMAN, Dora; JUNQUILHO, Tainá; REIS, Priscila. Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e direitos humanos. *Revista de Direitos e Garantias Fundamentais*, [S. l.], v. 24, n. 3. p. 43–71, 2023. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/2198. Acesso em: 17 abr. 2024.

KELLY, Kevin. *New Rules for the New Economy*: 10 radical strategies for a connected world. New York: Viking Penguin, 1998 e POSNER, Richard. Antitrust in the New Economy. *Antitrust Law Journal*, v. 68, 2001. p. 926. Disponível em: https://www.jstor.org/stable/40843502. Acesso em: 03 fev. 2024.

KIESLICH, Pascal J.; HENNINGERA, Felix; WULFF, Dirk U.; HASLBECKE, Jonas M. B.; SCHULTE-MECKLENBECK, Michael. (in press). Mouse-tracking: A practical guide to implementation and analysis. *In*: SCHULTE-MECKLENBECK, Michael; KÜHBERGER, Anton; JOHNSON, Joseph G. (eds.). *A Handbook of Process Tracing Methods*. New York, NY: Routledge, 2019.

KITCHIN, Rob. Thinking critically about and researching algorithms. *Information, Communication & Society*, *20:*1, 2016. Disponível em: https://doi.org/10.1080/1369118X.2016.1154087. Acesso em: 03 jan. 2024;

KLOZA, Dariusz *et al*. The concept of impact assessment. *In*: KLOZA, Dariusz; BUGRESS, J. Peter (org.) *Border Control and New Technologies*: addressing integrated impact assessment. Brussel: ASP, 2021.

KLUTTZ, Daniel N.; KOHLI, Nitin; MULLIGAN, Deirdre K. Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020.

KORS, Jorge Alberto. *Los secretos industriales y el know how*. Buenos Aires: La Ley, 2007.

KOTLIAR, Dan M. The Return of the Social: Algorithmic Identity in an Age of Symbolic demise. *New Media Society,* v. 22, n. 7.

KREMER, Bianca. Os agentes de tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020.

KUENZLER, Adrian. *Restoring Consumer Sovereignty*. How Markets Manipulate Us and What the Law Can do About It. New York: Oxford University Press, 2017.

LA DIEGA, Guido Noto; SAPPA, Cristiana. The Internet Of Things At The Intersection Of Data protection And Trade Secrets. Non-Conventional Paths To Counter Data Appropriation And Empower Consumers. 3 *Revue européenne de droit de la consommation / European Journal of Consumer Law*. 2020. Disponível em: https://ssrn.com/abstract=3772700. Acesso em: 08 fev. 2024.

LA ROSA, Fernanda Carvalho Frustockl; DA SILVA, Silvio Bitencourt. Delimitação e Proteção Jurídica do Know-How nos Contratos de Franquia a Partir da Visão Baseada em Conhecimento. *Revista de Direito, Inovação, Propriedade Intelectual e Concorrência*. v. 6, n. 2. Jul/Dez. 2020. Disponível em: https://www.indexlaw.org/index.php/revistadipic/article/download/7125/pdf. Acesso em: 18 nov. 2023.

LAIDLAW, Emily. Private Power, Public Interest: An Examination of Search Engine Accountability. International Journal of Law and Information Technology, Vol. 17, Issue 1, p. 113-145, 2009. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1357967. Acesso em: 15 nov. 2023.

LAIDLAW, Emily. Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility. Cambridge University Press, 2015.

LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren; ANGWIN, Julia. How We Analyzed the COMPAS Recidivism Algorithm. *Pro Publica*. 2016. Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. Acesso em: 12 maio 2024)

LASH, Scott. Power after Hegemony: Cultural Studies in Mutation? *Theory, Culture & Society*, v. 24, n.

LATOUR, Bruno. *Reassembling the Social*: An Introduction to Actor-Network-Theory. Oxford: Clarendon, 2005.

LEISTNER, Matthias. The existing European IP rights system and the data economy – An overview with particular focus on data access and portability. *In*: German Federal Ministry of Justice and Consumer Protection | Max Planck Institute for Innovation and Competition (eds.). *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos. 2021.

LEITE, Márcio Junqueira; ALMEIDA, Marcus Elidius M.; SISTER, Tatiana D. Da Proteção do Know-how nos Contratos de Franquia. *PEER Review*. Vol. 5, n. 15, 2023. Disponível em: https://www.peerw.org/index.php/journals/article/download/733/454. Acesso em: 18 nov. 2023;

LEMLEY, Mark A. The Surprising Virtues of Treating Trade Secrets as IP Rights. *Stanford Law Review*, v. 61, 2008. Disponível em: https://law.stanford.edu/sites/default/files/publication/258632/doc/slspublic/Lemley%20Surprising.pdf. Acesso em: 03 mar. 2024.

LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. *In*: DONEDA, Danilo *et al*. (coord). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

LESSIG, Lawrence. *Code 2.0*. New York: Basic Books, 2006.

LESSIG, Lawrence. The architecture of Privacy. *Taiwan Net '98 conference*, in Taipei, March, 1998. Disponível em: https://cs.wellesley.edu/~cs342/fall10/papers/LessigArchitectureOfPrivacy.pdf. Acesso em: 19 jul. 2023.

LEVINE, David S. Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure. *Florida Law Review*. 2007. Disponível em: https://ssrn.com/abstract=900929. Acesso em: 26 maio 2024.

LICHTMAN, Douglas. Property Rights in Emerging Platform Technologies. *The Journal of Legal Studies*, v. 29, n. 2. p. 615–648, 2000. Disponível em: https://www.jstor.org/stable/10.1086/468087. Acesso em: 19 fev. 2024.

LIEBENAU, Diana. What intellectual property can learn from informational privacy, and vice versa. *Harvard Journal of Law & Technology*. 30, 1, 285-307, 2016.

LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento automatizado de dados pessoais*. Como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021..

LINDOSO, Maria Cristine; DE MATOS, Amanda Visoto. O risco discriminatório da automatização decisória no poder judiciário: perspectivas e horizontes. *In*: PINHO, Anna Carolina (coord.). *Manual de Direito na Era Digital*. Processual. Indaiatuba, SP: Foco, 2023.

LINDOSO, Maria Cristine. Automatização na justiça criminal: Mapeamento dos riscos e considerações sobre o aspecto político da automatização. *In*: MENDES, Gilmar; FREITAS, Matheus Pimenta (org.). *Constituição, Direito Penal e Novas Tecnologias*. São Paulo: Almedina, 2023.

LISPECTOR, Clarice. Um sopro de vida (pulsações). Rio de Janeiro: Nova Fronteira, 1978). A categoria jurídica, contudo, não é cercada por esse tipo de mistério.

LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability (December 20, 2018). *International Journal of Law and Information Technology*, Vol. 27, Issue 2, p. 122-141 (2019). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313916. Acesso em: 10 jan. 2024.

LYONS, Henrietta; VELLOSO, Eduardo; MILLER, Tim. Conceptualising Contestability: Perspectives on Contesting Algorithmic Decisions. *Proceedings of the ACM Human-Computer Interaction*, Volume 5, CSCW1, Article 106, 2021. Disponível em: https://dl.acm.org/doi/10.1145/3449180. Acesso em: 12 maio 2024.

MACCARTHY, Mark. New Directions In Privacy: Disclosure, Unfairness and Externalities. *I/S*: A Journal of Law and Policy for the Information Society. 425. 2011. Disponível em: https://ssrn.com/abstract=3093301. Acesso em: 27 nov. 2023.

MACHADO, Diego; MENDES, Laura Schertel. A proteção dos dados sensíveis inferidos: um comentário ao caso c-184/20 do Tribunal de Justiça Europeu. *In*: *Revista de Direito do Consumidor*. São Paulo: Revista dos Tribunais, vol. 144, nov-dez./2022.

MACHADO, Diego. *Algoritmos e Proteção de Dados Pessoais*. Tutela de direitos na era dos perfis. São Paulo: Almedina, 2023.

MACHADO, Diego. Considerações iniciais sobre o conceito de dado pessoal no ordenamento jurídico brasileiro. *Civilistica.com*, Rio de Janeiro, v. 12, n. 1. p. 1–34, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/843. Acesso em: 4 maio. 2024.

MADISON, Michael J. Open Secrets. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011.

MAGER, Astrid. ALGORITHMIC IDEOLOGY. How capitalist society shapes search engines. Information, Communication & Society, 15:5, 1-19, 2012. Disponível em: http://dx.doi.org/10.1080/1369118X.2012.676056. Acesso em: 11 nov. 2023.

MAGIOLINO, Mariateresa. EU Trade Secret Law and Algorithmic Transparency. *Bocconi Legal Studies Research Paper* No. 3363178, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363178. Acesso em: 04 abr. 2024).

MAIA FILHO, Mamede S.; JUNQUILHO, Tainá A. Projeto Victor: perspectivas de aplicação da inteligência artificial ao direito. *Revista de Direitos e Garantias Fundamentais*, [S. l.], v. 19, n. 3. p. 218–237, 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1587. Acesso em: 25 abr. 2024.

MAIA, Roberta Mauro Medina. A natureza jurídica da titularidade dos dados pessoais. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020.

MAIA, Roberta Mauro Medina. O legítimo interesse do controlador e o término do tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020.

MALGIERI, Gianclaudio. Trade Secrets v Personal Data: A Possible Solution for Balancing Rights. *International Data Privacy Law*, Volume 6, Issue 2. maio de 2016. Disponível em: https://ssrn.com/abstract=3002685. Acesso em: 02 maio 2024

MARANHÃO, Juliano Souza de Albuquerque; JUNQUILHO, Tainá Aguiar; TASSO, Fernando Antônio. Transparência sobre o emprego de Inteligência Artificial no Judiciário: um modelo de governança. *Suprema - Revista de Estudos Constitucionais*, Distrito Federal, Brasil, v. 3, n. 2. p. 145-187, 2023. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/231. Acesso em: 17 maio 2024.

MARANHÃO, Juliano. COZMAN, Fábio Gagliardi; ALMADA, Marco. Concepções de explicação e do direito à explicação de decisões automatizadas. *In*: VAINZOF, Rony; GUTIERREZ, Andrei Guerrero (coord.). *Inteligência* artificial [livro eletrônico]: sociedade, economia e Estado. São Paulo: Thomson Reuters, 2021.

MARTINS-COSTA, Judith. *A boa-fé objetiva no direito privado* – sistema e tópica no processo obrigacional. São Paulo: RT, 2000.

MARX, Karl. *O capital*. Livro 1. São Paulo: Boitempo, 2014.

MATTEI, Ugo; NADER, Laura. *Plunder*: When the rule of law is illegal. Blackwell Publishing Ltd., 2008.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data*: A Revolution That Will Transform How We Live, Work and Think. London: John Murray, 2013.

MAZZUCATO, Mariana. *O estado empreendedor*: desmascarando o mito do setor público vs. setor privado. São Paulo: Portfólio-Pinguim, 2014.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. *In*: *I/S*: A Journal of Law and Policy. Vol. 4:3, 2008: Privacy Year in a Review Issue. Disponível em: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf. Acesso em: 09 set. 2023.

MEDEIROS, Marcelo. *Os ricos e os pobres*. O brasil e a desigualdade. São Paulo: Companhia das Letras, 2023.

MEDON, Felipe. *Inteligência Artificial e Responsabilidade Civil*: autonomia, riscos e solidariedade. São Paulo: Editora JusPodivm, 2022.

MEJIAS, Ulises A.; COULDRY, Nick. Datafication. *Internet Policy Review*, 8 (4), 2019. Disponível em: https://doi.org/10.14763/2019.4.1428. Acesso em: 11 nov. 2023.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito Constitucional*. 9. ed. rev. e atual. São Paulo: Saraiva, 2014.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, Passo Fundo, vol. 16, n. 1, p. 1-33, Janeiro-Abril, 2020.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Revista Pensar*. Fortaleza, v. 25, n. 4. p. 1-18, out./dez. 2020. Disponível em: https://ojs.unifor.br/rpen/article/view/10828. Acesso em: 23 jun. 2023.

MENDES, Laura Schertel; FONSECA, Gabriel Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista de Estudos Institucionais*, v. 6, n. 2, p-507-533, maio/ago 2020. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 11 mar. 2023.

MENDES, Laura Schertel. Decisão Histórica do STF reconhece direito fundamental à proteção de dados pessoais: Novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. *JOTA*. 2020. Disponível em:

https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 10 mar. 2024.

MENDONÇA, Ricardo F.; FILGEURIAS, Fernando; ALMEIDA, Virgílio. *Algorithmic Institutionalism*. The Change Rules of Social and Political Life. United Kingdom: Oxford University Press, 2023.

MILANEZ, Giovanna. A utilização de tecnologias de reconhecimento facial para fins de segurança pública e persecução penal no Brasil: mapeando discussões e possíveis caminhos regulatórios. *In*: MENDES, Gilmar; FREITAS, Matheus Pimenta (org.). *Constituição, Direito Penal e Novas Tecnologias*. São Paulo: Almedina, 2023.

MILLER, Megan Marie. Data as the New Oil: A Slippery Slope of Trade Secret Implications Greased by the California Consumer Privacy Act. *Cybaris®*: Vol. 12: Iss. 1, Article 1, 2021. Disponível em: https://open.mitchellhamline.edu/cybaris/vol12/iss1/1/. Acesso em: 08 fev. 2024.

MITTELSTADT, Brent. Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, v. 1, 2019. Disponível em: https://www.nature.com/articles/s42256-019-0114-4. Acesso em: 03 abr. 2024.

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. *Direitos Fundamentais & Justiça*, ano 13, n. 41. p. 183-212, jul./dez. 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/811. Acesso em: 14 mar. 2024.

MOORE, Taylor R. Trade Secrets and Algorithms as Barriers to Social Justice. *CDT Free Expression Fellow*. 2017. p. 10. Disponível em: https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf. Acesso em: 2 maio 2024.

MORATO, Antonio Carlos; CHINELLATO, Silmara Juny Abreu. Direitos Básicos de Proteção de Dados Pessoais, o Princípio da Transparência e a Proteção dos Direitos Intelectuais. *In*: DONEDA, Danilo *et al*. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

MOROZOV, Evgeny. *Big Tech*: A ascensão dos dados e a morte da política. UBU Editora, 2018.

MULHOLLAND, Caitlin; OLIVEIRA, Samuel Rodrigues. Uma Nova Cara Para a Política? Considerações sobre Deepfakes e Democracia. *Revista Direito Público*, v. 18.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). In: *Revista de Direitos e Garantias Fundamentais*, vol. 19, n. 3, p.159-180, set.-dez 2018.

NAVES, Márcio Bilharinho. *Marx*: Ciência e Revolução. São Paulo: Moderna, Campinas, SP, Editora da Universidade de Campinas, 2000.

NAVES, Márcio Bilharinho. *Marx*: Ciência e Revolução. São Paulo: Moderna, Campinas, SP, Editora da Universidade de Campinas, 2000.

NERY JUNIOR, Nelson. Segredo de Negócio - Livre Iniciativa. Soluções Práticas. vol. 1. set/2010. *Revista dos Tribunais*

NISSENBAUM, Helen. *Privacy in context*: technology, policy and the integrity of social life. Palo Alto: Stanford University Press, 2010.

NISSENBAUM, Helen. *Privacy, Big Data, and the Public Good*. Frameworks for Engagement. Cambridge University Press, 2014.

NOBLE, Safiya Umoja. Algorithms of Oppression. How Search Engines Reinforce Racism. New York University Press, 2018..

Norma de Fiscalização da ANPD. Disponível em: https://www.gov.br/participamaisbrasil/norma-de-fiscalizacao-da-anpd. Acesso em: 06 jan. 2024.

NOVAES, Henrique; DAGNINO, Renato. O fetiche da tecnologia. *ORG & DEMO*, v. 5 n. 2. p. 189-210, 2004. Disponível em: https://revistas.marilia.unesp.br/index.php/orgdemo/article/view/411. Acesso em: 15 out. 2023;

O'BRIEN, Kevin J. Austrian Law Student Faces Down Facebook. *The New York Times*. 2012. Disponível em: https://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html. Acesso em: 02 maio 2024.

O'NEIL, Cathy. *Weapons of math destruction*. How big data increases inequality and threatens democracy. New York: Crown Publishers, 2016.

OCAÑA, Teresa Trallero. *The Notion of Secrecy*. A Balanced Approach in the Light of the Trade Secrets Directive. NOMOS. Munich Intellectual Property Law Center. München: The Deutsche Nationalbibliothek, 2020.

OECD. Policy Roundtables. Information Exchanges Between Competitors under Competition Law. *OECD*. 2010. Disponível em: https://www.oecd.org/daf/competition/48379006.pdf. Acesso em: 18 fev. 2024.

OELDORF-HIRSCH, Anne; NEUBAUM, German. What Do We Know About Algorithmic Literacy? the Status Quo and a Research Agenda for a Growing Field. *SocArXiv*. November 18, 2021. Disponível em: https://doi.org/10.31235/osf.io/2fd4j. Acesso em: 20 dez. 2023).

OHLY, Ansgar. Jurisdiction and Choice of Law in Trade Secrets Cases: The EU Perspective. *In*: SANDEEN, Sharon K.; RADEMACHER, Christoph; OHLY, Ansgar (eds.). Research Handbook on Information Law and Governance. Edward Elgar, 2021. Disponível em: https://ssrn.com/abstract=4020416. Acesso em: 12 out. 2023.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *A Lei Geral de Proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019.

PACHUKANIS, Evguiéni B. *Teoria Geral do Direito e Marxismo.* São Paulo: Editora Acadêmica, 1988.

PASQUALE, Frank A. Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries. *Northwestern University Law Review*. 1 out. 2010. Disponível em: https://ssrn.com/abstract=1686043. Acesso em: 22 abr. 2024.

PASQUALE, Frank A.; BRACHA, Oren. Federal Search Commission? Access, Fairness and Accountability in the Law of Search. *Cornell Law Review*, setembro 2008. U of Texas Law, Public Law Research Paper No. 123, Seton Hall Public Law Research Paper No. 1002453. Disponível em: https://ssrn.com/abstract=1002453. Acesso em: 27 abr. 2024.

PASQUALE, Frank. Secret Algorithms Threaten the Rule of Law. *MIT Technology Review*. 2017. Disponível em: https://www.technologyreview.com/2017/06/01/151447/secret-algorithms-threaten-the-rule-of-law/. Acesso em: 12 maio 2024.

PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PASQUALE, Frank. The troubling consequences of trade secret protection of search engine rankings. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011.

PELE, Antônio; MULHOLLAND, Caitlin. On Facial Recognition, Regulation, and 'Data Necropolitics'. *Indiana Journal of Global Legal Studies*, v. 30. 2023. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2023/07/On-Facial-Recognition-Regulation-and-Data-Necropolitics-Pele-Mulholland.pdf. Acesso em: 02 maio 2024.

PEREL, Maayan; ELKIN-KOREN, Niva. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, n. 181, 2017. Disponível em: https://scholarship.law.ufl.edu/flr/vol69/iss1/5/. Acesso em: 18 fev. 2024;

PERES FILHO, José Augusto de Souza; TEPEDINO, Gustavo. Autodeterminação informativa e a interseção da proteção de dados com a defesa do consumidor. *In*: MARQUES, Claudia Lima *et al*. (coord). *5 anos de LGPD*: estudos em homenagem a Danilo Doneda [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2023.

PERLINGIERI, Pietro. *Perfis do direito civil*: introdução ao direito civil constitucional. 3. ed. Rio de Janeiro: Renovar, 2007.

PETERS, Michael A. Algorithmic Capitalism in the Epoch of Digital Reason. *Fast Capitalism*, vol. 14, n. 1, 2017. Disponível em: https://doi.org/10.32855/fcapital.201701.012. Acesso em: 10 mar. 2024.

PIKETTY, Thomas. *O Capital no Século XXI.* Rio de Janeiro: Intrínseca, 2014.

PISTOR, Katharina. Ideology and Institutions in the Evolution of Capital. Analyse & Kritik, v. 43, p. 23, 2021.

PISTOR, Katharina. *The Code of Capital.* How the Law Creates Wealth and Inequality. Princeton University Press, 2019.

PODER360. Dino aciona Defesa do Consumidor contra o Google por PL das fake news. *Poder 360*. 2023. Disponível em: https://www.poder360.com.br/governo/dino-aciona-defesa-do-consumidor-contra-o-google-por-pl-das-fake-news/. Acesso em: 01 dez. 2023; LESSA, Henrique. Após multa de R$ 1 milhão por hora, Google retira do ar link contrário a PL. *Correio Braziliense*. 2023. Disponível em: https://www.correiobraziliense.com.br/politica/2023/05/5091532-apos-multa-de-rs-1-milhao-por-hora-google-retira-do-ar-link-contrario-a-pl.html. Acesso em: 01 dez. 2023.

POLANYI, Karl. The Economy as Instituted Process. *In*: GRANOVETTER, Mark; SWEDBERG, Richard. (Eds). *The Sociology of Economic Life*. Boulder, Westview Press, 1992.

PONTES DE MIRANDA, Francisco Cavalcanti. *Tratado de Direito Privado*. Parte Especial. 4. ed. São Paulo: Revista dos Tribunais, v. 16, 1983.

POSNER, Richard. Intellectual Property. Case Compliments of Versuslaw. *Rockwell Graphic Systems*, Inc. v. Dev Industries, Inc., 925 F.2d 174 (7th Cir. 1991), tradução nossa. Disponível em: https://biotech.law.lsu.edu/cases/ip/ts/Rockwell_v_Dev_I.htm. Acesso em: 20 mar. 2024.

POWLES, Julia; NISSENBAUM, Helen. The Seductive Diversion of 'Solving' Bias in Artificial Intelligence. Trying to "fix" A.I. distracts from the more urgent questions about technology. One Zero, 2018. Disponível em: https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53. Acesso em: 1 out. 2023.

POWLES, Julia. The Corporate Culpability of Big Tech. *In*: BANT, Elise. (ed.). *The Culpable Corporate Mind*. Hart Publishing, Oxford: 2023. p. 100-101; AUSTIN, Lisa M. *Enough About Me*: Why Privacy is About Power. A World Without Privacy? What Can / Should Law Do. Cambridge, 2014.

PRATA DE CARVALHO, Angelo. O papel da estratégia de segurança da informação nos mecanismos de compliance de dados: em busca de uma abordagem integrada. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021.

QUELLE, Claudia. *Privacy, proceduralism and Self-Regulation in Data Protection Law*. Teoria e Critica della Regolazione Sociale. 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3139901. Acesso em: 16 set. 2023.

RADAUER, Alfred; SEARLE, Nicola; BADER, Martin A. The possibilities and limits of trade secrets to protect data shared between firms in agricultural and food sectors. *World Patent Informatio*n, Volume 73, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S0172219023000133. Acesso em: 28 fev. 2024.

Regulamento Geral de Proteção de Dados (GDPR). *EDPB*. 2022. p. 2. Disponível em: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf. Acesso em: 27 fev. 2024;

RODOTÀ, Stéfano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIK, Dani. *Straight Talk on Trade*. Ideas for a Sane World Economy. New Jersey: Princeton University Press, 2018. p. 260; HASKEL, Jonathan; WESTLAKE, Stian. *Capitalism without capital*. The rise of the intangible economy. Princeton & Oxford: Princeton University Press, 2018.

RUDZITE, L. Algorithmic Explainability and the Sufficient-Disclosure Requirement under the European Patent Convention. *Juridica International*, [S. l.], v. 31. p. 125–135, 2022. p. 128. Disponível em: https://ojs.utlib.ee/index.php/juridica/article/view/19323. Acesso em: 15 abr. 2024.

RUDZITE, Liva. Algorithmic Explainability and the Sufficient-Disclosure Requirement under the European Patent Convention. *Juridica International*, [S. l.], v. 31. 2022. Disponível em: https://ojs.utlib.ee/index.php/juridica/article/view/19323. Acesso em: 15 abr. 2024.

RUSSO, Raffaele. Reflections about the Implications of Platforms and Technology for Taxation and Taxpayers' Rights. *In*: WEBER, Dennis (ed.). *The Implications of Online Platforms and Technology on Taxation*. The Netherlands: IBFD, 2023.

RYAN, Meghan J. Secret Algorithms, IP Rights, and the Public Interest. *Nevada Law Journal*, v. 21, n. 1. 2020. Disponível em: https://ssrn.com/abstract=3691765. Acesso em: 02 maio 2024.

SANCHEZ-GRAELLS, Albert. Ensuring algorithmic transparency through public contracts? *The Digital Constitutionalist*, 24 de novembro de 2022. Disponível em: https://digi-con.org/ensuring-algorithmic-transparency-through-public-contracts/. Acesso em: 28 abr. 2024.

SANDEEN. Sharon K. The limits of trade secret law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on which it is based. *In*: DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds.). *The Law and Theory of Trade Secrecy*: A Handbook of Contemporary Research. Cheltenham: Edward Elgar, 2011.

SAPPA, Cristiana. How data protection fits with the algorithmic society via two intellectual property rights – a comparative analysis. *Journal of Intellectual Property Law & Practice*, Volume 14, Issue 5, May 2019. Disponível em: https://academic.oup.com/jiplp/article-abstract/14/5/407/5369198. Acesso em: 19 fev. 2024.

SARLET, Gabriela B. S.; RODRIGUEZ, Daniel P. A Autoridade Nacional de Proteção de Dados (ANPD): Elementos para uma Estruturação Independente e Democrática na Era da Governança Digital. *Revista Direitos Fundamentais & Democracia*, [S. l.], v. 27, n. 3. 2022. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285. Acesso em: 14 mar. 2024.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana.

Civilistica.com. Rio de Janeiro, ano 8, n. 1, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 7 abr. 2024.

SARLET, Ingo Wolfgang. Proteção de Dados Pessoais como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo para a Construção de uma Dogmática Constitucionalmente Adequada. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 14, n. 42. p. 179–218, 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 26 maio 2024.

SCHECHTER, Roger E.; THOMAS, John R. *Intellectual Property*: The Law of Copyrights, Patents and Trademarks. United States of America: Hornbook Series, 2003. p. 531-532.

SCHIRRU, Luca. Direito autoral e inteligência artificial: autoria e titularidade nos produtos da IA. Orientador: Allan Rocha de Souza. Tese (doutorado) – UFRJ, 2020.

SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016.

SCHWARTZ, Paul M. Internet privacy and state. *Connecticut Law Review*, v. 32. 2000. Disponível em: https://paulschwartz.net/wp-content/uploads/2019/01/SCHWARTZ-CK1A-1.pdf. Acesso em: 27 nov. 2023

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, Vol. 86. 2011. Disponível em: https://www.nyulawreview.org/issues/volume-86-number-6/the-pii-problem-privacy-and-a-new-concept-of-personally-identifiable-information/. Acesso em: 16 nov. 2023).

SELDAM, Björn tem; BRENNINKMEIJER, Alex. The Dutch benefits scandal: a cautionary tale for algorithmic enforcement. EU Law Enforcement.2021. Disponível em: https://eulawenforcement.com/?p=7941. Acesso em: 12 maio 2024.

SIEMS, Jasper. Protecting Deep Learning: Could the New EU-Trade Secrets Directive Be an Option for the Legal Protection of Artificial Neural Networks? *In*: EBERS, Martin; GAMITO, Marta Cantero (eds.). *Algorithmic Governance and Governance of Algorithms*. Springer, 2021.

SILVA, Priscila Regina. Os Direitos dos Titulares de Dados. *In*: MULHOLLAND, Caitlin. *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 203.

SILVEIRA, João Marcos. A proteção jurídica dos segredos industriais e de negócio. *Revista da ABPI*. Vol. 53, jul/ago 2001. Disponível em: https://abpi.org.br/bfd_download/edicao-53-mes-julho-agosto-ano-2001/. Acesso em: 22 maio 2024.

SOLOVE, Daniel J. I've got Nothing to Hide and other misunderstandings of privacy. *San Diego Law Review*, vol. 44, 2007. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565. Acesso em: 25 ago. 2022

SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, v. 126, n. 7, 2013. Disponível em: https://harvardlawreview.org/print/vol-

126/introduction-privacy-self-management-and-the-consent-dilemma/. Acesso em: 19 maio 2023.

SOMBRA, Thiago Luís. Planos de Resposta a incidentes de segurança com dados pessoais e a construção de uma governança responsiva. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021.

SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023.

SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. *In*: DONEDA, Danilo *et al*. (coord). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

SOUZA, Ilan Fonseca. *Dirigindo Uber*: A subordinação jurídica na atividade de um motorista de aplicativo. Curitba: Juruá Editora, 2024.

SOUZA, Michel R. O; ZANATTA, Rafael A. F. The Problem of Automated Facial Recognition Technologies in Brazil: Social Countermovements and the New Frontiers of Fundamental Rights. *Latin American Human Rights Studies*, v. 1, 2021. Disponível em: https://revistas.ufg.br/lahrs/article/view/69423. Acesso em: 01 maio 2024.

SPECHT-RIEMENSCHNEIDER, Louisa. Data access rights – A comparative perspective. *In*: German Federal Ministry of Justice and Consumer Protection | Max Planck Institute for Innovation and Competition (eds.). *Data Access, Consumer Interests and Public Welfare*. Alemanha: Nomos, 2021.

STIGLITZ, Joseph E.; GREENWALD, Bruce C. *Creating a Learning Society*: a new approach to Growth, Development and Social Progress. New York: Columbia University Press, 2015.

STINGHEN, João Rodrigo de Morais; ANDRADE, Aline Rodrigues de. *Os riscos à privacidade do novo cadastro positivo e o papel da ANDP*. Revista dos Tribunais. vol. 1025. ano 110. p. 203-223. São Paulo: Ed. RT, março 2021.

STUCKE, Maurice E.; GRUNES, Allen P. Big Data and Competition Policy. Oxford University Press, 2016.

STUEBER, Karsten R. Understanding Versus Explanation? How to Think about the Distinction between the Human and the Natural Sciences. *Inquiry*, v. 55, n. 1. 2012. Disponível em: https://doi.org/10.1080/0020174X.2012.643621. Acesso em: 12 mar. 2024.

SUÁREZ-GONZALO, Sara. Personal data are political. A feminist view on privacy and big data. *In*: *Recerca*, Revista de Pensament i Anàlisi, n. xx. 2019. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 11 nov. 2023.

SUNSTEIN, Cass. *Republic.com*. Princeton, NJ: Princeton University Press, 2001.

SUPERIOR TRIBUNAL DE JUSTIÇA, REsp 1.419.697, j. 12.11.2014, rel. Min. Paulo de Tarso Sanseverino. Trecho do voto. p. 35. Acesso em: 15 fev. 2024.

SUPREMO TRIBUNAL FEDEAL. STF recebe propostas de uso de inteligência artificial para agilizar serviços. *STF*. 2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=522767&ori=1. Acesso em: 02 jun. 2024.

SUPREMO TRIBUNAL FEDERAL, Rel. Min. Rosa Weber, j. 07 maio de 2020.

SUSTEIN, Carl. *Republic*: Divided Democracy in the Age of Social Media. Princeton University Press, 2017.

TAUK, Caroline Somesom; CUEVA, Ricardo Villas Bôas. Propriedade intelectual, segredo do negócio e transparência: a proteção do código-fonte, do algoritmo e do banco de dados. In: CUEVA, Ricardo Villas Bôas ... [et al.]. *Direitos fundamentais e novas tecnologias*: homenagem ao professor Danilo Doneda. 1ª ed. Rio de janeiro: GZ, 2024.

TAYLOR, Linnet; FLORIDI, Luciano; VAN DER SLOOT, Bart. Introduction: A New Perspective on Privacy. *In*: TAYLOR, Linnet; FLORIDI, Luciano; VAN DER SLOOT, Bart. *Group Privacy*. New Challenges of Data Technologies. *Philosophical Studies Series*. Dordrecht: Springer, 2017.

TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology & Intellectual Property*, v. 11. p. 239, 2013. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip. Acesso em: 16 nov. 2023.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil* – RBDCivil: Belo Horizonte, v. 25. p. 83-116, jul./set. 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521. Acesso em: 13 ago. 2024.

TEPEDINO, Gustavo. A pessoa jurídica e os direitos da personalidade. *In*: TEPEDINO, Gustavo. *Temas de direito civil*. Rio de Janeiro: Renovar, 1999.

TEPEDINO, Gustavo. *A Tutela da Personalidade no Ordenamento Civil-Constitucional Brasileiro*. Temas de Direito Civil. 3. ed. São Paulo: Renovar, 2004.

TEUBNER, Gunther. Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution. *Italian Law Journal*, v. 3, n. 2. p. 485–510, 2017. Disponível em: https://www.jura.uni-frankfurt.de/70299574/InternetHorizontalConstRightsENGItalJ2017.pdf?.%20. Acesso em: 12 abr. 2023.

TEUBNER, Gunther. Societal constitutionalism: alternatives to state-centered constitutional theory. *In*: JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther (eds.). *Constitutionalism and transnational governance*. Oxford: Hart Publishing, 2004.

TIMCKE, Scott. *Algorithms and the end of politics*: How Technology Shapes 21st-Century American Life. Bristol University Press, 2021.

TOKARCZUK, Olga. Discurso do Prêmio Nobel de Literatura. In:TOKARCZUK, Olga *Escrever é muito perigoso*: ensaios e conferências; tradução Gabriel Borowski. 1ª ed.. São Paulo: Todavia, 2023.

TRIBUNAL SUPERIOR DO TRABALHO, Tutela Cautelar Antecedente 1000825-67.2021.5.00.0000. Rel. min. Douglas Alencar Ribeiro, j. 28 maio 2021.

TSCHANG, Hi-Chu. The Squeeze at China's Baidu. *Businessweek*, 2009. Disponível em: https://www.bloomberg.com/news/articles/2008-12-30/the-squeeze-at-chinas-baidu. Acesso em: 23 abr. 24.

TUNHOLI, Murilo. Ataque hacker gerou prejuízo de R$ 3,5 milhões ao Governo Federal. *giz_br*. 2024. Disponível em: https://encurtador.com.br/fnM5x. Acesso em: 13 jul. 2024; ANDRADE, Henrique. Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar. *CNN*. 2021. Disponível em: https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/. Acesso em: 13 jul. 2024.

TURKLE, Sherry. *Alone Together*. Why We Expect More From Technology and Less from Each Other. New York: Basic, 2011.

UITSPRAKEN. *Rechtbank Den Haag*. 2020. Disponível em: https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878. Acesso em: 12 maio 2024.

UNGER, Roberto Mangabeira. *The Critical Legal Studies Movement*. Cambridge, Massachusetts: Harvard University Press, 1986.

VALE; Sebastião Barros; ZANFIR-FORTUNA, Gabriela. *Automated Decision-Making Under the GDPR*: Practical Cases from Courts and Data Protection Authorities. *Future of Privacy Forum*. May 2022. Disponível em: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf. Acesso em: 2 maio 2024.

VALENTE, Jonas C. L. O poder das plataformas digitais e impactos econômicos e políticos sobre a América Latina. *In*: PARANÁ, Edemilson; KAMINSKI, Ricardo S. *Tecnologia e Desenvolvimento nas Américas*. Novas Fronteiras e Dilemas do Capitalismo Contemporâneo. Curitiba: CRV, 2021.

VAROSANEC, Ida. Silence is golden, or is it? Trade secrets versus transparency in ai systems. *The Digital Constitutionalist*. 2022. Disponível em: https://digi-con.org/silence-is-golden-or-is-it/ Acesso em: 09 mar. 2024.

VEDDER, Adam. Privacy 3.0. *In*: GROOTHUIS, Marga; HOF, Simone van der. *Innovating Government*. The Hague: Asser Press, 2011.

VÉLIZ, Carissa. *Privacidade é poder*. Por que e como você deveria retomar o controle de seus dados. São Paulo: Editora Contracorrente, 2021.

VÉLIZ, Carissa. *The Ethics of Privacy and Surveillance*. Oxford: Oxford University Press.

VERBICARO, Dennis. Determinismo algorítmico: uma ameaça real à individualidade do consumidor. *In*: MARQUES, Claudia Lima *et al*. (coord). *5 anos de LGPD*: estudos em homenagem a Danilo Doneda. São Paulo: Thomson Reuters Brasil, 2023 [livro eletrônico].

VERONESE, Alexandre. Os direitos de explicação e de oposição diante das decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD Brasileira. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2023.

VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual*. 2. ed. São Paulo: Almedina, 2020. BASSO, Maristela. Os fundamentos atuais do direito internacional da propriedade intelectual. *Revista CEJ*. Brasília, v. 7, n. 21, jun. 2003. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/541. Acesso em: 22 maio 2024.

VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual.* 2. ed. São Paulo: Almedina, 2020.

VOGT, Sander. Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence—Part II. *In*: *The Journal of Robotics, Artificial Intelligence & Law* (Fastcase), Volume 5, No. 5, September–October 2022, Full Court Press, an imprint of Fastcase, Inc. Disponível em: https://www.crowell.com/en/insights/publications/show-me-your-secrets-how-the-use-of-trade-secrets-relates-to-the-demand-for-transparent-artificial-intelligence-part-ii. Acesso em: 24 mar. 2024.

VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. The Spread of True and False News Online. *Science*, 359: 1146-1151. 2018. Disponível em: https://www.science.org/doi/10.1126/science.aap9559. Acesso em: 01 ago. 2023;

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, v. 31, n. 2, 2018. Disponível em: https://ssrn.com/abstract=3063289. Acesso em: 4 maio 2024.

WEISER, Mark. The Computer for the 21st Century. *CalmTechnology* (Originally published 09-91: Scientific Americ). Disponível em: https://calmtech.com/papers/computer-for-the-21st-century. Acesso em: 19 jan. 2024.

WIMMER, Miriam; PIERANTI, Octavio Penna. Programas de compliance e a LGPD: a interação entre autorregulação e a regulação estatal. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance e Política de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2021.

WU, Tim. *The Attention Merchants*. The epic Scramble to Get inside Our Heads. New York: Vintage Books, 2016.

YU, Howard. GDPR Isn’t Enough To Protect Us In An Age Of Smart Algorithms: Facebook and Google already face a legal complaint in the wake of the new data protection law, but the most precious data still isn't covered. *IMD - International Institute for Management Development*. 2018. Disponível em: https://www.imd.org/research-knowledge/data-analytics/articles/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms/. Acesso em: 03 abr. 2024.

ZANATTA, Rafael Augusto Ferreira. O Uso da Lei Geral de Proteção de Dados Pessoais por Gestores Públicos: Origens e Funções Procedimentais em Políticas Públicas no Brasil. *Revista de Estudos em Organizações e Controladoria-REOC*, ISSN 2763-9673, UNICENTRO, Irati-PR, v. 3, n. 2. jul./dez., 2023. Disponível em: https://revistas.unicentro.br/index.php/reoc/article/view/7614. Acesso em: 08 jun. 2024.

ZUBOFF, Shoshana. Big Other: Capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda *et al*. *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018.

ZUBOFF, Shoshana. Caveat Usor: Surveillance Capitalism as Epistemic Inequality. *In*: WERBACH, Kevin. *After the Digital Tornado*. Networks, Algorithms, Humanity. Cambridge: Cambridge University Press, 2020.

ZUBOFF, Shoshana. *The age of surveillance capitalism.* The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.