UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

Rafael Carvalho Bueno

LEI GERAL DE PROTEÇÃO DE DADOS, SEGREDO DE NEGÓCIO E DECISÕES AUTOMATIZADAS: a suficiência da análise contrafactual para verificação de aspectos discriminatórios

Florianópolis
2023

Rafael Carvalho Bueno

LEI GERAL DE PROTEÇÃO DE DADOS, SEGREDO DE NEGÓCIO E DECISÕES AUTOMATIZADAS: a suficiência da análise contrafactual para verificação de aspectos discriminatórios

Dissertação submetida ao Programa de Pós-Graduação da Universidade Federal de Santa Catarina para a obtenção do título de mestre em Direito.

Orientadora: Profa. Dra. Liz Beatriz Sass

Florianópolis
2023

Bueno, Rafael Carvalho
LEI GERAL DE PROTEÇÃO DE DADOS, SEGREDO DE NEGÓCIO E DECISÕES AUTOMATIZADAS : a suficiência da análise contrafactual para verificação de aspectos discriminatórios /Rafael Carvalho Bueno ; orientadora, Liz Beatriz Sass , 2023.
110 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito, Florianópolis, 2023.

Inclui referências.

1. Direito. 2. proteção de dados. 3. segredo de negócio. I. Sass , Liz Beatriz . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Direito. III. Título.

Rafael Carvalho Bueno

Lei Geral de Proteção de Dados e Decisões Automatizadas: a suficiência da análise contrafactual para verificação de aspectos discriminatórios

O presente trabalho foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Marcelo Markus Teixeira, Dr.
Instituição Universidade Comunitária da Região de Chapecó - UNOCHAPECÓ

Profa. Melissa Ely Melo, Dra.
Instituição Universidade Federal de Santa Catarina - UFSC

Profa. Liz Beatriz Sass, Dra.
Instituição Universidade Federal de Santa Catarina - UFSC

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para a obtenção do título de mestre em Direito.

Documento assinado digitalmente
Claudio Macedo de Souza
Data: 19/11/2023 10:53:21-0300
CPF: ***.565.726-**
Verifique as assinaturas em https://v.ufsc.br

_____

Coordenação do Programa de Pós-Graduação em Direito

Documento assinado digitalmente
Liz Beatriz Sass
Data: 14/11/2023 17:11:22-0300
CPF: ***.411.100-**
Verifique as assinaturas em https://v.ufsc.br

_____

Profa. Liz Beatriz Sass, Dra.
Orientadora

Florianópolis
2023

Aos meus pais, os principais pilares de apoio durante esta jornada acadêmica. O sucesso deste trabalho é, em grande parte, o resultado da educação, valores e orientação que recebi de vocês. Agradeço-lhes pela paciência e pelo contínuo incentivo, fundamentais para a realização deste feito.

AGRADECIMENTOS

Geralmente, o trabalho de pesquisa é uma atividade solitária e introspectiva. No entanto, seria injusto afirmar que enfrentei sozinho os desafios encontrados ao longo do caminho. Tenho que reconhecer as contribuições daqueles que, de uma maneira ou de outra, participaram da intensa jornada que foi o mestrado em Direito.

Em particular, agradeço aos meus pais pelo constante incentivo, pelas palavras de conforto nos momentos de incerteza e pelo apoio incondicional.

Aos amigos, agradeço a paciência para ouvir sobre o trabalho incontáveis vezes, assim como sobre todo o aprendizado que este mestrado me trouxe. Suas palavras de incentivo e apoio forneceram a força necessária para continuar.

Finalmente, à minha orientadora, não posso deixar de expressar minha sincera gratidão. Agradeço a oportunidade, por acreditar na pesquisa proposta quando era apenas uma ideia embrionária. Sua orientação, paciência e conhecimento foram imprescindíveis para transformar essa ideia em um trabalho completo. A cada etapa, você me desafiou a pensar mais profundamente, a questionar e a buscar a excelência. Foi um privilégio aprender com você e sou grato pelas lições inestimáveis que vou levar adiante em minha carreira acadêmica.

“O melhor professor, o fracasso é.”

Yoda, Mestre Jedi

RESUMO

A presente dissertação se propõe a investigar se a análise contrafactual pode ser utilizada como metodologia para a realização da auditoria prevista pelo art. 20, § 2º, da Lei Geral de Proteção de Dados (LGPD), voltada à identificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, sem, contudo, comprometer o segredo de negócio. A questão central é entender se essa abordagem contrafactual atende adequadamente aos preceitos da LGPD, garantindo transparência e proteção no tratamento automatizado de dados pessoais, preservando simultaneamente os segredos comerciais dos agentes envolvidos. Baseando-se na hipótese de que a auditoria através da análise contrafactual é viável e suficiente para tal finalidade, o trabalho se debruça, em um primeiro momento, sobre a LGPD, traçando suas origens, propósitos e o tratamento dado ao segredo de indústria no direito brasileiro. No segundo capítulo, o foco recai sobre o tratamento automatizado de dados pessoais, visando discernir seus riscos e as salvaguardas estabelecidas pela LGPD. Já no terceiro capítulo, a dissertação se aprofunda na análise da auditoria do art. 20, § 2º, da LGPD, ponderando a eficácia da análise contrafactual diante dos preceitos legais e da proteção dos titulares. Utilizando uma abordagem indutiva e qualitativa, o estudo se constrói por meio de um procedimento bibliográfico, abrangendo variadas fontes doutrinárias, bem como análises jurisprudenciais e legais. Ao término da investigação, almeja-se elucidar a capacidade da análise contrafactual em promover uma auditoria conforme a LGPD, equilibrando direitos individuais e segredos de negócio no ambiente digital contemporâneo.

Palavras-chave: Proteção de dados. Segredo de negócio. LGPD. Dados Pessoais. Decisões Automatizadas. Análise Contrafactual. Aspectos discriminatórios.

ABSTRACT

The present dissertation aims to investigate whether counterfactual analysis can be used in the context of the audit provided for in art. 20, § 2º, of the General Data Protection Law (LGPD) to identify discriminatory aspects in automated personal data processing, without compromising business secrets. The central question is to understand if this counterfactual approach adequately meets the precepts of the LGPD, ensuring transparency and protection in the automated processing of personal data while simultaneously preserving the commercial secrets of processing entities. Based on the hypothesis that the audit through counterfactual analysis is viable and sufficient for this purpose, the study first delves into the LGPD, tracing its origins, purposes, and the treatment given to industry secrets in Brazilian law. In the second chapter, the focus is on the automated processing of personal data, aiming to discern its risks and the safeguards established by the LGPD. In the third chapter, the dissertation delves deeper into the analysis of the audit in art. 20, § 2º, of the LGPD, weighing the efficacy of counterfactual analysis against legal precepts and the protection of data subjects. Using an inductive and qualitative approach, the study is constructed through a bibliographic procedure, covering various doctrinal sources, as well as jurisprudential and legal analyses. At the conclusion of the investigation, the goal is to elucidate the capability of counterfactual analysis in promoting an audit according to the LGPD, balancing individual rights and business secrets in today's digital environment.

Keywords: Data Protection. Trade Secret. LGPD. Personal Data. Automated Decisions. Counterfactual Analysis. Discriminatory Aspects.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
API	*Aplication Programming Interface*
CDC	Código de Defesa do Consumidor
CLT	Consolidação das Leis Trabalhistas
CNIL	*Commission Nationale Informatique & Libertés*
DPD	Diretiva de Proteção de Dados
ICO	*Information Commissioners's Office*
LGPD	Lei Geral de Proteção de Dados Pessoais
LPI	Lei de Propriedade Industrial
MCI	Marco Civil da Internet
OMC	Organização Mundial do Comércio
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
RGPD	Regulamento Geral de Proteção de Dados
TRIPS	*Agreement on Trade-Related Aspects of Intellectual Property Rights*
TRT1	Tribunal Regional do Trabalho da 1ª Região
UE	União Europeia
XAI	*Explainable Artificial Intelligence*

SUMÁRIO

INTRODUÇÃO

Diante da acentuada evolução tecnológica experienciada nas últimas décadas, que trouxe diversas mudanças à sociedade, uma das mais marcantes é a vivenciada pela economia global, na medida em que esse forte avanço tecnológico permitiu o desenvolvimento de novos mercados e a criação de novos setores.

Danilo Doneda afirma que o processo de mercantilização da internet despertou receio para possíveis violações, principalmente em razão da prática da "economia de vigilância", em que há o desprezo do direito à privacidade dos usuários para maximizar os lucros, o que é feito, por vezes, com uso indevido de dados pessoais (DONEDA, 2019).

Para compreender a amplitude da discussão, é válido ressaltar que toda a informação sobre a pessoa é considerada dado pessoal, tais como nome, idade, sexo, renda, entre outras. Tudo o que serve para identificar e distinguir um indivíduo é considerado dado pessoal (ALMEIDA, 2019). Dessa maneira, o tratamento de dados está inserido em larga escala no modelo econômico atual.

Nesse contexto é que se desenvolveu a chamada economia dos dados, calcada na geração de valor a partir da utilização das informações pessoais dos indivíduos. Em função disso, dados pessoais passam a representar uma nova *commodity* cujo valor cresce exponencialmente. Formas de coleta e tratamento são trabalhadas em busca de maior eficiência no processamento informacional, sendo que muitas dessas metodologias se valem de soluções de inteligência artificial e *machine learning* para melhorar os resultados do tratamento de dados pessoais.

Essa conjuntura faz com que cresça a preocupação sobre a maneira como são processadas as informações sobre as pessoas, enfatizando o debate sobre os limites do tratamento automatizado de dados pessoais e sobre a relação entre benefícios e malefícios da prática.

Outro aspecto que reforça a dimensão do debate é a sensação de liberdade na rede, que esconde um processo oculto de violação à privacidade, com a finalidade de manipular o usuário por meio do impulsionamento estratégico de conteúdo. Isto é, o usuário pode ser manipulado por meio do uso de seus próprios dados.

A ideia de regulamentar aspectos do mundo digital, porém, não é unânime, sobretudo porque, junto com a disseminação da internet, também foi

disseminada a ideia de que o ambiente virtual estaria além do poder regulatório dos estados.

Seguindo essa linha de pensamento, Pereira defende que a internet emergiu de um cenário tumultuado, em um processo que pode ser comparado ao *big-bang*. Ela seguiu uma direção anárquica, onde os especialistas em tecnologia acreditavam que não havia necessidade de regulamentação por parte do Estado. Para esses profissionais, eventuais problemas poderiam ser resolvidos por mecanismos internos, como as tecnologias criptográficas. Nesse contexto, os juristas não seriam vistos como figuras legítimas nesse domínio, já que a internet responderia apenas aos códigos desenvolvidos por esses especialistas em tecnologia. O Estado, por sua vez, não exerceria autoridade, pois a internet transcende fronteiras territoriais. Assim, seus usuários não estariam atrelados a uma jurisdição específica e não teriam um domicílio definido (PEREIRA, 2001).

Também reforça essa ideia o seguinte excerto da carta conhecida como “A Declaração de Independência do Ciberespaço”, escrita por John Perry Barlow:

> Governos do Mundo Industrial, seus cansados gigantes de carne e aço, eu venho do Ciberespaço, a nova casa da Mente. Em nome do futuro, eu exijo a vocês do passado para nos deixar em paz. Vocês não são bem-vindos entre nós. Vocês não possuem autoridade soberana no lugar em que nos reunimos.
>
> Governos derivam seus poderes justamente do consentimento daqueles que por eles são governados. Vocês nem solicitaram ou receberam o nosso. Nós não convidamos vocês. Vocês não nos conhecem, nem conhecem o nosso mundo. O Ciberespaço não se limita às suas fronteiras. Não pensem que vocês podem construí-lo, como se fosse uma obra de construção civil. Vocês não podem. É uma força da natureza, e ela cresce através das nossas ações coletivas. (BARLOW, 1996, p. 1)

Não obstante, com o crescimento da conscientização sobre os riscos oferecidos pelo acelerado avanço tecnológico, a necessidade de regulamentação de aspectos do mundo digital se torna cada vez menos controversa. Isto é, atualmente, devido aos notáveis progressos na ciência e tecnologia, que incluem a internet, clonagem, realidade virtual, monitoramento via satélite, acesso instantâneo a informações e a manipulação computadorizada de imagens e voz, a integridade da personalidade enfrenta novos desafios que requerem uma regulamentação para garantir sua proteção (GONÇALVES, 2012).

A preocupação com o respeito à privacidade, porém, não é recente. Conforme Schemkel (2005) destaca, a privacidade sempre ocupou um lugar de destaque ao longo da história humana. Desde os tempos antigos, nas origens das culturas hebraica, grega e chinesa, já existia uma sensibilidade em relação à proteção deste direito, frequentemente ligado ao "direito de estar só".

O autor, porém, percebe o aumento da preocupação face à evolução tecnológica. E um dos aspectos mais controversos da problemática diz respeito à utilização de critérios discriminatórios no tratamento de dados pessoais, sobretudo quando se fala em tratamento automatizado. O tema se torna ainda mais espinhoso quando se trata de soluções de inteligência artificial e *machine learning*, seara em que, muitas vezes, os agentes envolvidos não têm certeza quanto aos critérios utilizados pelos algoritmos envolvidos no tratamento.

Visando remediar a controvérsia, a Lei Geral de Proteção de Dados (LGPD), por meio de seu art. 20, franqueou aos titulares de dados o direito à revisão de decisões tomadas a partir de tratamento automatizado de dados pessoais e garantiu aos titulares direito à informação clara sobre os critérios utilizados. O direito à informação, contudo, é limitado pela observância dos segredos industrial e comercial, hipótese em que a Autoridade Nacional de Proteção de Dados (ANPD) é autorizada a realizar auditoria buscando identificar a existência de aspectos discriminatórios no tratamento de dados pessoais.

Diante deste cenário, a presente pesquisa tem por objetivo discutir a articulação entre os direitos dos titulares de dados pessoais, sobretudo o direito à transparência, e a proteção dos segredos de negócio dos agentes envolvidos no tratamento de dados pessoais. Portanto, parte-se da seguinte problemática: a análise contrafactual pode ser utilizada para fins da auditoria de que trata o art. 20, § 2º, da Lei Geral de Proteção de Dados (LGPD), com o fito de esclarecer a existência de aspectos discriminatórios em tratamento automatizado de dados pessoais e, ao mesmo tempo, preservar o segredo de negócio?

A hipótese aventada é de que a referida auditoria pode ser realizada por meio de análise contrafactual, que seria suficiente para auferir a existência de aspectos discriminatórios no tratamento de dados pessoais e garantir a transparência dos processos automatizados de tomada de decisão com base no processamento de dados, garantindo-se, ao mesmo tempo, a preservação do

segredo de negócio. Essa hipótese é fundada nos princípios da LGPD e na forma como a lei busca resguardar os direitos dos titulares de dados pessoais e garantir-lhes amplo acesso a informações claras e precisas acerca da maneira como é realizado o tratamento dos dados.

A importância do tema deriva da natureza dos bens jurídicos envolvidos no debate. Isso porque, cada vez mais, ativos intangíveis se tornam fundamentais para os agentes econômicos. É o caso do segredo de negócio, porquanto, com o avanço da tecnologia, o acesso ao público consumidor é democratizado, o que acentua o caráter competitivo dos mercados e aumenta a importância de qualquer vantagem que os agentes tenham. Ademais disso, com o acesso facilitado às tecnologias, a reprodução de segredos dessa natureza também é facilitada, o que incrementa a necessidade de protegê-lo.

Para essa pesquisa, o método científico adotado é o indutivo, a abordagem é qualitativa, e o procedimento é bibliográfico, abarcando doutrina – sendo utilizados artigos científicos, livros, publicações avulsas, pesquisas, monografias, dissertações e teses – bem como análise jurisprudencial e legal.

Assim, a dissertação está estruturada em três capítulos: no primeiro, analisa-se a LGPD, buscando compreender não apenas seu *modus operandi*, mas suas origens e sua razão de ser, questões de suma importância à interpretação da legislação, e como o segredo de indústria é tratado no direito brasileiro; no segundo capítulo, o estudo será focado no tratamento automatizado de dados pessoais, para compreender quais riscos essa modalidade de tratamento traz consigo e quais salvaguardas a LGPD oferece aos titulares de dados pessoais; por fim, no terceiro capítulo, será realizada uma análise sobre a auditoria prevista no art. 20, § 2º, da LGPD, visando entender se a feitura de análise contrafactual é suficiente para atender aos preceitos da lei e garantir a proteção dos titulares.

Portanto, o capítulo inicial aborda a origem e evolução das legislações relativas à proteção de dados pessoais e segredos de negócio, destacando a imprecisão da LGPD ao tratar sobre a observância dos segredos de negócio e as consequências de suas disposições. Particularmente, o art. 20 da lei discute os efeitos da observância dos segredos industriais, propondo possíveis revisões de decisões baseadas em tratamento automatizado de dados. A lei, por sua vez,

introduz a ideia de auditorias pela ANPD, mas não define parâmetros claros para essas auditorias.

O propósito do capítulo é criar uma base teórica que permita compreender a origem e o progresso da proteção de dados e dos segredos empresariais em âmbito global e local.

Todavia, antes de dar início à investigação quanto à melhor forma de auditar o tratamento automatizado de dados em busca de aspectos discriminatórios, é necessário tratar do que é tratamento automatizado de dados pessoais, para compreender os riscos que essa modalidade oferece ao titula de dados, o que será feito no segundo capítulo do trabalho

Assim, no segundo capítulo, discute-se a definição e relevância do tratamento automatizado de dados pessoais. Essa modalidade, que é extremamente valiosa no atual cenário tecnológico, permite a análise massiva de informações e pode oferecer vantagens competitivas. Porém, também acarreta riscos devido à despersonalização das relações.

Por fim, o terceiro capítulo se aprofunda na auditoria proposta pelo art. 20, § 2º, da LGPD, analisando a interpretabilidade em modelos que usam tratamento automatizado de dados pessoais e explorando o método contrafactual. O equilíbrio entre transparência, proteção de dados e proteção dos segredos comerciais é crucial, bem como entender os desafios da auditoria. A discussão se concentra em avaliar a tensão entre a transparência exigida e a proteção de segredos empresariais, tendo em vista a aplicação eficaz dos sistemas de tratamento de dados pessoais e os princípios norteadores da LGPD.

É sabido que a LGPD se pauta por uma série de princípios e é fundamental ponderá-los para concluir qual a melhor forma de aplicar seus dispositivos. Nessa linha, a pesquisa visa cotejar todos esses elementos para entender se a auditoria prevista no art. 20, § 2º, da LGPD pode ser realizada por meio de análise contrafactual.

1. PROTEÇÃO DE DADOS PESSOAIS E SEGREDO DE NEGÓCIO

A era digital trouxe consigo uma avalanche de informações, que se tornaram uma fonte inesgotável de conhecimento e oportunidade para as organizações. No entanto, juntamente com essas oportunidades, surgiram também desafios consideráveis no que diz respeito à proteção de dados e ao segredo de negócio.

Este capítulo busca explorar o desenvolvimento histórico e o estado atual das legislações de proteção de dados, com especial foco no Brasil e seu contexto jurídico único. O Brasil tem enfrentado desafios significativos em equilibrar a necessidade de proteção aos segredos de negócio e a imposição de obrigações legais rígidas para a proteção de dados pessoais.

O objetivo deste capítulo é fornecer um arcabouço teórico para a compreensão desses temas, traçando as origens e a evolução da proteção de dados e do segredo de negócio tanto a nível global quanto local. Além disso, será feita uma exploração detalhada da LGPD e de como ela afeta o cenário do segredo de negócio no Brasil.

A estrutura do capítulo seguirá a seguinte ordem: inicialmente, será apresentado o conceito de proteção de dados e seu contexto histórico, especialmente na Europa e nos EUA. Em seguida, será examinado o desenvolvimento da proteção de dados no Brasil antes da implementação da LGPD, exame que será seguido de uma avaliação da LGPD em si. Depois, o conceito e a história do segredo de negócio serão discutidos, com foco particular no Brasil e na intersecção do segredo de negócio com a LGPD.

Este capítulo serve como uma introdução aos temas que serão abordados de forma mais aprofundada nos capítulos subsequentes do trabalho. O conhecimento adquirido aqui será fundamental para entender se a análise contrafactual é um método adequado para a realização da auditoria prevista no art. 20, § 2º, da LGPD.

1.1 Proteção de dados pessoais e LGPD

De início, é importante compreender o que é um dado. Embora diferentes regramentos jurídicos possam atribuir conceitos distintos, para atingir os efeitos

específicos da tutela que buscam atribuir, alguns aspectos da definição de dado são comuns à vasta maioria deles. Dessa forma, em termos generalistas, é possível valer-se do conceito usado por Bruno Bioni, para quem:

> O dado é o estado primitivo da informação, pois não é algo *per si* que acresce conhecimento. Dados são simplesmente *fatos brutos* que, quando processados e organizados, se revertem em algo inteligível, podendo ser deles extraída uma informação. (BIONI, 2019, p. 35)

A proteção de dados pessoais tem como maior objetivo a proteção do titular dos dados, isto é, aquele a quem as informações se referem, sobretudo porque a tutela dos dados representa, em última instância a tutela da pessoa (BRASIL, 2010).

Devido ao avanço tecnológico vivenciado em todo o globo, a proteção de dados se tornou um tema de grande relevância nas últimas décadas. Empresas têm coletado e armazenado uma enorme quantidade de dados pessoais, que englobam informações como nome, endereço, idade, histórico de navegação na internet, histórico de compras e até mesmo dados biométricos, como impressões digitais e reconhecimento facial. Esses dados são utilizados para uma variedade de propósitos, desde publicidade até análises de mercado e desenvolvimento de produtos.

A maneira como plataformas digitais operam, valendo-se da internet, não possui precedentes na história humana e essa mudança pode ser explicada pela forma como a fonte de receita dos serviços ofertados ao público por intermédio dessas ferramentas é, em larga escala, proveniente das informações deixadas nas plataformas pelos usuários (BIONI, 2019).

Essa exponencial alteração no paradigma da coleta e processamento de dados pessoais, para Danilo Doneda, está associada a uma lógica utilitarista, na qual se busca obter o máximo proveito das informações disponíveis. Segundo o autor:

> Os dados pessoais dos consumidores sempre foram atraentes para o mercado. Com dados precisos sobre os consumidores é possível, por exemplo, organizar um planejamento de produtos e vendas mais eficiente, ou mesmo uma publicidade voltada às reais características dos consumidores, entre diversas outras possibilidades. Há pouco tempo atrás, o custo para se obter tais dados pessoais costumava restringir severamente a quantidade de destas informações que eram efetivamente coletadas e utilizadas. (BRASIL, 2010, p. 9)

À medida em que o volume de dados tratados aumenta, se torna cada vez mais relevante a criação de normas para assegurar a privacidade e a segurança dessas informações (CASTELLS, 2018). Entretanto, a proteção de dados vai além da simples garantia de privacidade e segurança, sendo também um componente essencial para impulsionar a inovação tecnológica (MAYER-SCHÖNBERG, 2018). Um ambiente seguro, no qual as pessoas se sintam confortáveis em compartilhar suas informações pessoais, é fundamental para o desenvolvimento de novos modelos de negócio e, consequentemente, para o surgimento de novas tecnologias.

Nesse contexto, o advento de tecnologias como a inteligência artificial e a internet das coisas ampliou as possibilidades de coleta e processamento de grandes volumes de dados em tempo real. Essa capacidade de coleta e processamento em larga escala é vital para garantir a eficácia e a precisão dos algoritmos, mesmo diante de possíveis barreiras à evolução da tecnologia em si, como nos ensina Kai-Fu Lee:

> [...] quando o poder da computação e os talentosos engenheiros atingem certo limite, a quantidade de dados se torna decisiva para determinar a potência e a precisão gerais de um algoritmo.
>
> No aprendizado profundo, não há nada melhor para os dados do que mais dados. Quanto mais uma rede for exposta a exemplos de um determinado fenômeno, mais precisamente poderá escolher padrões e identificar coisas no mundo real. (LEE, 2019, p. 24)

Na sequência, o cientista da computação esclarece que mesmo soluções menos sofisticadas podem oferecer resultados mais precisos quando dispõem de uma base de dados maior. *In verbis*:

> Com mais dados, um algoritmo projetado por um grupo de engenheiros de IA de nível médio geralmente supera um projetado por um pesquisador de aprendizado profundo de elite. Ter o monopólio dos melhores e mais brilhantes não significa ter os melhores resultados em termos práticos. (LEE, 2019, p. 24)

Com isso, é possível perceber a enorme importância da coleta da maior quantidade de dados possível, a fim de alimentar tais sistemas e permitir a obtenção de melhores resultados.

Ao estabelecer um equilíbrio entre a segurança e a utilização ética dos dados, oferecendo maior segurança aos titulares para que compartilhem seus dados, é possível promover um ambiente propício ao desenvolvimento sustentável e

responsável da tecnologia. Assim, a proteção de dados desempenha um papel crucial não apenas na preservação da privacidade e segurança das pessoas, mas também no impulsionamento da inovação e no avanço tecnológico em diversos setores.

Contudo, o crescimento exponencial do volume de dados compartilhados e armazenados não vem sendo acompanhado do crescimento da segurança associada a esses dados. Isso abre espaço para o mau uso dos dados pessoais, que se tornaram uma *commodity* valiosa e possuem alto valor econômico.

Hoje em dia existe uma verdadeira economia gravitando em torno dos dados pessoais, afinal, como explicam D'AVILA et al., "no século XXI, a informação passou a ser uma mercadoria de alto valor. Em tempos atuais, as maiores empresas do mundo, como Apple, Facebook, Google, Airbnb, Uber, dentre outras, se utilizam de forma massiva das informações" (2021, p. 19).

Sendo assim, corporações com maior capacidade de coleta e tratamento de dados pessoais se tornam cada vez mais lucrativas e se destacam das demais, o que lhes garante ainda mais capacidade de coleta e tratamento de dados. O acúmulo de informações pessoais na mão de poucos *players* é outro fator que enseja uma grande preocupação com a proteção de dados pessoais no contexto da sociedade atual (LANCIERI et al., 2021, p. 83).

Algumas empresas, como o Google e o Facebook, se destacam no mercado de dados pessoais. Essas empresas coletam informações dos usuários por meio de seus serviços e usam essas informações para criar perfis detalhados dos usuários, que são vendidos para anunciantes (SMYTH, 2019, p. 579).

Essa ânsia pela coleta massiva de dados se justifica pela inversão da lógica capitalista tradicional, em que o usuário é o cliente e as companhias tentam vender-lhe seus produtos; no paradigma atual, o usuário – mais especificamente a atenção do usuário – passa a ser o produto mercantilizado por essas grandes empresas (HARARI, 2018, p. 107).

Embora o mercado de dados pessoais tenha trazido benefícios para as empresas, também tem gerado preocupações em relação à privacidade e segurança dos titulares. Muitas vezes, os titulares não sabem como seus dados estão sendo utilizados e com quem estão sendo compartilhados. Além disso, existe risco de que esses dados sejam roubados ou utilizados de forma maliciosa.

De toda forma, o mercado de dados pessoais é altamente lucrativo, porquanto permite que as corporações compreendam melhor os seus clientes e criem produtos e serviços mais personalizados e direcionados.

Diante dessa conjuntura, se faz necessário o estabelecimento de normas, para orientar a forma de utilização dos dados pessoais coletados, permitindo o aproveitamento desses recursos para o desenvolvimento tecnológico e econômico, sem descuidar do resguarde à proteção de dados. Para Yuval Hoah Harari, que faz uma analogia com outros recursos importantes ao longo da história, a regulamentação é essencial para evitar uma grande concentração de poder nas mãos de uma pequena parcela da sociedade. *In verbis*:

> Se quisermos evitar a concentração de toda a riqueza e de poder nas mãos de uma pequena elite, a chave é regulamentar a propriedade dos dados. Antigamente a terra era o ativo mais importante no mundo, a política era o esforço por controlar a terra, e se muitas terras acabassem se concentrando em poucas mãos – a sociedade se dividia em aristocracia e pessoas comuns. Na era moderna, máquinas e fábricas tornaram-se mais importantes que a terra, e os esforços políticos focam no controle desse meio de produção. Se um número excessivo de fábricas se concentrasse em poucas mãos – a sociedade se dividiria entre capitalistas e proletários. Contudo no século XXI, os dados vão suplantar tanto a terra quanto a maquinaria como o ativo mais importante, e a política será o esforço por controlar o fluxo de dados. Se os dados se concentrarem em muito poucas mãos – o gênero humano se dividirá em espécies diferentes. (HARARI, 2018, p. 107)

Essa análise, que alça a informação ao patamar de elemento estruturante da sociedade, também é feita por Bruno Bioni, para quem:

> [...] a informação avoca um papel central e adjacente da sociedade: sociedade da informação. A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícolas, industrial e pós-industrial. (BIONI, 2019, p. 2)

Diante dessa conjuntura, regulamentação do tratamento de dados pessoais envolve aspectos como a transparência no uso dos dados, o consentimento informado dos titulares dos dados, a proteção contra acessos não autorizados e a garantia de que os dados sejam usados apenas para as finalidades para as quais foram coletados.

Nas palavras de TEPEDINO et al., a proteção de dados pessoais “compõe o aspecto essencial da tutela da dignidade da pessoa humana, haja vista

que busca evitar discriminações que não encontrem fundamento constitucional e afastar práticas que possam reduzir a liberdade e autonomia dos indivíduos" (2021, 305). Esse é um tema que vem sendo discutido há décadas. O jurista norte-americano Alan Westin já defendia a privacidade como um direito fundamental na década de 1960 (WESTIN, 1967).

Desde então, vários países têm tomado medidas para proteger a privacidade e segurança dos dados pessoais. No contexto geopolítico hodierno, se destacam a União Europeia e os EUA, que possuem modelos distintos de proteção, como será visto no próximo tópico.

1.1.1 Proteção de dados pessoais ao redor do mundo

A segunda metade do século XX marcou o início das discussões sobre a proteção dos dados pessoais. Em sessões do Conselho da Europa nos anos de 1967 e 1968, surgiu a questão da vulnerabilidade do direito à privacidade diante dos avanços tecnológicos.

A proteção à vida privada, assegurada pelo art. 8º da Convenção de Direitos Humanos da União Europeia (UE)[1], era considerada insuficiente, pois foi elaborada em 1950, quando as ameaças à privacidade não eram tão evidentes. Essas constatações levaram à aprovação, em 1970, de uma recomendação, que culminou em um relatório voltado à análise da problemática. Esse relatório encorajou o Conselho da Europa a emitir recomendações para regular o tratamento de dados por empresas privadas, visto que faltava proteção nos Estados-Membros e na Comunidade Europeia (TAVARES et al., 2017).

Pela falta de uma legislação supranacional capaz de forçar os Estados-Membros a regulamentarem a matéria domesticamente, foi proposta uma diretiva prevendo essa obrigação. Ao mesmo tempo, a questão deixou de ser apenas uma proteção à privacidade e se tornou também uma tutela dos direitos humanos: o Conselho da Europa desenvolveu a Convenção n. 108, instituída em 1981 em

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

Estrasburgo, na França, e ratificada por todos os países do bloco, com o objetivo de assegurar o respeito ao direito à privacidade dos cidadãos diante do tratamento de seus dados pessoais.

Tavares e Alvarez (2017) relatam que, após esses movimentos e uma recomendação da OCDE em 1980, alguns Estados começaram a aprovar leis. O nível de proteção, porém, era muito desigual, e, em resposta, a Diretiva para Proteção de Dados Pessoais (DPD) foi aprovada em 1995, com o objetivo de harmonizar as leis nacionais, permitindo a circulação dos dados na União Europeia.

A DPD é um exemplo proeminente da legislação europeia sobre proteção de dados. Essa diretiva buscou equilibrar a proteção da privacidade individual com a livre circulação de dados pessoais dentro da União Europeia. Essencialmente, ela estabelece limitações para a coleta e utilização de dados pessoais e solicita a formação de um organismo nacional em cada país signatário para supervisionar as atividades de processamento de dados.

Além disso, a DPD traz uma definição clara de "dados pessoais" em seu segundo artigo e estabelece princípios para a qualidade dos dados coletados. Por exemplo, os dados pessoais devem ser processados de maneira justa e legítima, coletados para finalidades específicas e legítimas, e devem ser precisos e atualizados, se necessário.

Outra importante disposição da DPD é a supervisão da aplicação de seus princípios e leis de proteção à privacidade individual, que é fundamental para todos os usuários. Outrossim, o Artigo 25º[2] ressalta a preocupação com a transferência de dados para países não pertencentes à UE, enquanto o Artigo 28º[3] enfatiza a importância de uma autoridade de supervisão de proteção de dados para monitorar

[2] Artigo 25º - Princípios - 1. Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adoptadas nos termos das outras disposições da presente Directiva, o país terceiro em questão assegurar um nível de proteção adequado. 2. A adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou setoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país. [...]

[3] Artigo 28º - Autoridade de controle - 1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adoptadas pelos Estados-membros nos termos da presente diretiva. Essas autoridades exercerão com total independência as funções que lhes forem atribuídas. [...]

a aplicação de suas normas em território nacional (UE, 2016).

A Carta dos Direitos Fundamentais da União Europeia, do ano 2000 e que recebeu caráter vinculativo após o Tratado de Lisboa, em 2009, elevou a proteção dos dados pessoais ao patamar de direito fundamental.

Em 2012, dezessete anos após a aprovação da DPD, a Comissão Europeia propôs uma reformulação da diretiva. Nesse ínterim, novos desafios surgiram, o que levou ao lançamento da proposta do Regulamento Geral de Proteção de Dados (RGPD) em 2015, aprovado em 2016 e em vigor desde 25 de maio de 2018.

O RGPD rege a transferência de dados para países terceiros com rigor e estabelece critérios para permitir o tráfego de dados, com avaliação periódica. Embora existam exceções, essas exigências se tornaram uma barreira para negócios, incentivando outros países a regulamentar o tema.

A abordagem dada pelos EUA à proteção de dados pessoais, noutro giro, é bastante complexa e diversa da adotada na UE. É crucial entender que o ordenamento jurídico dos EUA é composto por muitas partes diferentes, sendo comparado a um cubo mágico, com várias partes móveis e combinações possíveis (TALBOTT, 2016).

Diferentemente do averiguado em muitos outros países, o direito à privacidade nos EUA não está explicitamente inserido na Constituição, ele é o resultado de uma construção jurisprudencial e está previsto em diversas legislações esparsas. Na verdade, esse direito pode ser entendido de várias maneiras, seja como o direito de ser deixado em paz ou como direito fundamental garantido pela quarta emenda que assegura a inviolabilidade do lar, bens e objetos, por exemplo.

Dentre as normas que tratam da proteção de dados pessoais, se destaca o *Privacy Act*, de 1974, que coíbe práticas abusivas por parte do Estado, mais especificamente por parte das agências federais, as quais só podem usar e compartilhar os dados pessoais coletados para a finalidade consentida, garantindo ao titular o acesso, retificação ou complementação destes dados, além de estabelecer a responsabilidade civil das agências em caso de violação à norma.

Outro diploma relevante é o *Electronic Communications Privacy Act*, de 1986, motivado pelos inúmeros casos de violação ao direito à privacidade ocorridos durante a Guerra Fria e o escândalo de Watergate. Essa lei visa proteger as

informações pessoais disponíveis na internet, proibindo a espionagem estatal e de empresas privadas em todos os meios de comunicação digital, além de proibir o acesso e a interceptação de mensagens.

Além das leis mencionadas, existem outras leis setoriais nos EUA, como o *Right to Financial Privacy Act*, o *The Tax Reform Act* e o *Telecommunications Act*.

Entretanto, assim como ocorreu na Europa, as inovações tecnológicas colocaram em xeque a proteção ao direito à privacidade nos Estados Unidos, trazendo consigo a preocupação com a possibilidade de uma única pessoa ou organização ter acesso não autorizado a uma ampla gama de dados pessoais por intermédio de tecnologia.

Em relação aos dados de consumidores europeus, os EUA criaram a estrutura *Safe Harbor* para cumprir com os padrões de proteção de dados estabelecidos pela DPD. Contudo, em 2015, a Corte de Justiça Europeia declarou a insuficiência da estrutura *Safe Harbor* (UE, 2015).

Para superar essa deficiência, em 2016, a Comissão Europeia e os EUA concordaram em estabelecer um novo quadro para fluxos de dados, conhecido como *EU-US Privacy Shield*. O mesmo ocorreu com a Suíça, onde, em 2017, foi aprovado o *Swiss-US Privacy Shield* com a finalidade de cumprir os requisitos de transferência de dados pessoais da Suíça para os EUA. Esses novos quadros substituíram os anteriores, refletindo a contínua evolução das leis de proteção de dados.

Em suma, os EUA seguem um modelo de autorregulação, com regulamentação e normatização feita pelos próprios participantes e interessados diretos na proteção de seus direitos (TAVARES et al., 2017). Diferentemente da UE, os EUA optaram por adotar normas setoriais, ao invés de adotar um regulamento geral, aplicável a todas as atividades que envolvem o processamento de dados pessoais.

Como será visto a seguir, também é possível averiguar a evolução das legislações que abordam a problemática da proteção de dados pessoais no Brasil, com um substancial acréscimo de robustez às garantias oferecidas pela lei ao longo do tempo.

1.1.2 Proteção de dados pessoais na legislação brasileira

No Brasil, a questão da proteção de dados pessoais já era abordada na Constituição de 1988, vinte anos antes da aprovação da LGPD. Assim como faz a Carta dos Direitos Fundamentais da UE, a Carta Magna alça a privacidade ao patamar de direito fundamental (art. 5º, X[4]), além de proteger a inviolabilidade do sigilo das correspondências, das comunicações telegráficas, dos dados e das comunicações telefônicas (art. 5º, XII[5]) (BRASIL, 1988).

Ainda no âmbito constitucional, o *habeas data*, um dos remédios legais estabelecidos no art. 5º da Constituição (LXXII[6]), permite que o cidadão acesse e solicite a retificação de suas informações pessoais armazenadas em bases de dados de entidades governamentais ou de caráter público (BRASIL, 1988).

Além da Constituição, no âmbito interno brasileiro, em 1990 foi aprovado o Código de Defesa do Consumidor (CDC), que assegura, ao consumidor, algum controle sobre suas informações pessoais dentro das relações de consumo. O CDC prevê a possibilidade de acesso, pelo consumidor, de suas informações presentes em cadastros, registros e dados pessoais, além da obrigação de descarte e proibição de compartilhamento de informações negativas armazenadas por mais de cinco anos (BRASIL, 1990).

Danilo Doneda aponta o pioneirismo dessa legislação no que diz respeito à transparência dada ao tratamento de dados pessoais. Veja-se:

> [...] a primeira das garantias a este respeito é a da transparência, como direito do consumidor de ser comunicado de que a informação a seu respeito está sendo processada (artigo 43, § 2º). Os outros direitos do consumidor estabelecidos pelo CDC no que toca à proteção de seus dados pessoais é o direito de acesso (correspondente ao princípio do livre acesso) e de retificação (correspondente ao princípio da qualidade). (DONEDA, 2006, p. 379)

---

[4] Art. 5º [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[5] Art. 5º [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

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

Vinte e um anos depois, em 2011, foi promulgada a Lei do Cadastro Positivo (Lei n. 12.414/2011)(BRASIL, 2011), responsável por estabelecer um banco de dados sobre bons pagadores. Em 2019, houve alterações significativas nessa lei com a aprovação da Lei Complementar n. 166, incluindo a inscrição automática do consumidor no cadastro positivo e a permissão para o gestor iniciar um registro de solvência dos consumidores sem seu consentimento prévio (BRASIL, 2019).

Essa lei, como explica Danilo Doneda, é responsável por inserir, no ordenamento jurídico brasileiro, uma base para o conjunto principiológico adotado posteriormente pela LGPD. Com efeito:

> A abertura de cadastro histórico de crédito depende do consentimento do titular dos dados, conforme o artigo 4º da lei, o que é a primeira diferença cabal deste regime em relação ao cadastro negativo. Mas os pontos mais relevantes da lei do ponto de vista da percepção dos princípios de proteção de dados, são a sua presença literal em artigos subsequentes. (DONEDA, 2006, p. 381)

Essas, porém, são leis cujo objetivo é regulamentar a proteção dos dados pessoais de maneira restrita, pois tratam de situações específicas. Em contrapartida, a aprovação e sanção do Marco Civil da Internet (MCI), em 2014, representa um marco significativo na proteção abrangente de dados pessoais no Brasil.

Nos termos do art. 1º, o MCI tem por objetivo estabelecer "princípios, garantias, direitos e deveres para o uso da internet no Brasil" (BRASIL, 2014). Para Bioni (2019), a legislação em questão decidiu salvaguardar os direitos e garantias dos usuários da rede por meio de um enfoque baseado em princípios, evitando técnicas regulatórias que poderiam restringir as liberdades individuais. Tal abordagem poderia criar obstáculos ao uso e ao estímulo da inovação no espaço digital.

O MCI declara que a orientação para a regulação do uso da internet no país envolve, entre outros, os princípios de proteção à privacidade e aos dados pessoais (art. 3º, II e III[7]). Além disso, com foco na privacidade e nos dados pessoais dos usuários, o acesso à internet é definido como uma ferramenta crucial para o exercício da cidadania (art. 7º[8])(BRASIL, 2014).

---

[7] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; [...]

[8] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...]

Noutro giro, o MCI determina medidas para a proteção de dados pessoais, especificando que a retenção e disponibilização desses dados e de comunicações privadas devem respeitar a privacidade, a vida privada, a honra e a imagem do titular (arts. 10 e 11[9])(BRASIL, 2014). Ademais, também determina que esses dados só podem ser disponibilizados mediante ordem judicial e estabelece a jurisdição da lei brasileira, nos casos em que o processamento de dados pessoais aconteça no território nacional, é aplicável a empresas estrangeiras que prestam serviço ao público brasileiro ou àquelas que, pertencendo a um grupo econômico, tenham filial no Brasil.

Embora o MCI seja inovador e tenha provocado um amplo debate sobre a proteção da privacidade e a tutela de dados pessoais no Brasil, ele regulamentou o tema de forma mais tímida em comparação com a abordagem adotada há mais de duas décadas pelo modelo de regulação implementado pela DPD da UE. Ainda que o MCI tenha inaugurado uma abordagem abrangente para a proteção de dados, falhou em estabelecer em seu próprio texto o conceito de dados pessoais, dados sensíveis e dados anonimizados, além de não assegurar o direito de acesso e retificação dos dados e não dispor sobre a criação de uma autoridade nacional independente, semelhante à prevista na DPD e no RGPD.

A edição do Decreto 8.771/2016 preencheu algumas dessas lacunas. O referido regulamento estabelece os conceitos de dado pessoal e tratamento (art. 14, I e II[10]). Além, o decreto designou a Agência Nacional de Telecomunicações (ANATEL) para atuar na regulação, fiscalização e apuração das violações (art. 17[11]),

[9] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. [...]

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. [...]

[10] Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[11] Art. 17. A Anatel atuará na regulação, na fiscalização e na apuração de infrações, nos termos da Lei nº 9.472, de 16 de julho de 1997.

atribuindo também competências para apuração de infrações setoriais à Secretaria Nacional do Consumidor e ao Sistema Brasileiro de Defesa da Concorrência (art. 18 e 19[12])(BRASIL, 2016).

Apesar das deficiências e da incapacidade do MCI de proteger adequadamente os dados pessoais face aos avanços tecnológicos e às muitas práticas abusivas de violações à privacidade, é notório que a legislação estabeleceu a autodeterminação informacional como princípio orientador na tutela dos dados pessoais e concedeu ao titular um controle efetivo sobre seus dados, o que é alcançado através do consentimento em todas as etapas do fluxo dos dados, incluindo a coleta, compartilhamento e o direito do titular de solicitar a exclusão de todos os seus dados ao se cumprir a finalidade de uma relação.

A demanda por proteção de dados averiguada globalmente, porém, não foi atendida no Brasil com o MCI, o qual, apesar de representar avanços, ainda trata a questão de maneira discreta. Para sanar esse problema, foi editada a LGPD, cujo texto, como será visto no próximo tópico, aproxima o Brasil do bloco europeu em termos de garantias legais relacionadas à proteção de dados pessoais.

1.1.3 Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018)

Em 2018, a LGPD foi aprovada, estabelecendo regras claras para coleta, processamento e armazenamento de dados pessoais. Essas medidas são importantes para garantir a proteção dos dados pessoais e a privacidade dos indivíduos, um direito fundamental que deve ser respeitado em todas as sociedades.

Dentre as grandes mudanças promovidas pela LGPD, se destacam a necessidade de consentimento explícito do titular dos dados, a garantia de acesso aos dados pessoais e a sua correção ou exclusão quando necessário.

A lei elenca como fundamentos para a proteção dos dados pessoais: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o

[12] Art. 18. A Secretaria Nacional do Consumidor atuará na fiscalização e na apuração de infrações, nos termos da Lei nº 8.078, de 11 de setembro de 1990.
Art. 19. A apuração de infrações à ordem econômica ficará a cargo do Sistema Brasileiro de Defesa da Concorrência, nos termos da Lei nº 12.529, de 30 de novembro de 2011.

livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º[13])(BRASIL, 2018).

Embora tenha entrado em vigor no ano de 2020, a elaboração e implementação da lei envolveu um longo processo, que contou com a participação de diversos atores, incluindo o governo, a sociedade civil e o setor empresarial.

Os debates sobre a temática iniciaram no país ainda em 2010, quando o Comitê Gestor da Internet promoveu o I Seminário de Proteção à Privacidade e aos Dados Pessoais, tendo o Ministério da Justiça lançado consulta pública para aferir opiniões a respeito de um anteprojeto de lei logo na sequência (BIONI, 2019). Em 2018, a LGPD foi aprovada pelo Congresso Nacional e sancionada pelo então presidente Michel Temer.

Após uma polêmica durante o processo legislativo, o governo brasileiro criou, por meio da Medida Provisória n. 869/2018, a ANPD para fiscalizar a implementação da LGPD e garantir que as empresas estejam cumprindo as regras estabelecidas pela lei (BRASIL, 2018). A criação da ANPD, assim como suas atribuições e seu papel na efetivação dos direitos previstos na LGPD será abordada com mais profundidade no último capítulo desta pesquisa, quando será estudada a auditoria prevista no art. 20, § 2º, da lei.

A LGPD também coloca o Brasil em linha com outras legislações internacionais, como o já abordado RGPD, da UE, que estabeleceu regras semelhantes para a proteção de dados em território europeu e exerceu forte influência sobre a LGPD. A LGPD tem como objetivo garantir direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, não sendo, portanto, abarcada pela proteção normativa as pessoas jurídicas.

Embora seja influenciada pelo RGPD, a LGPD possui algumas diferenças em relação a ele. Uma dessas diferenças é a forma como essas normas tratam o relacionamento jurídico entre controlador e operador. Enquanto o RGPD obriga que

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

o relacionamento seja regido por um contrato ou ato jurídico equivalente (art. 28º[14]) (UE, 2016), a LGPD não é tão exigente, determinando somente que o operador realize o tratamento segundo as instruções fornecidas pelo controlador (art. 39[15]) (BRASIL, 2018).

Além disso, outra diferença importante entre as leis é que o RGPD tem exigências mais rigorosas para empresas que processam dados pessoais considerados sensíveis, como informações sobre saúde ou orientação sexual. O RGPD, como regra geral, proíbe o uso de dados sensíveis (art. 9º[16])(UE, 2016); a LGPD, por sua vez, não é tão drástica, mas limita as possibilidades de tratamento desse tipo de informação.

Embora tenham algumas diferenças, a LGPD e o GDPR compartilham muitos princípios e buscam alcançar objetivos semelhantes.

Ambas as leis estabelecem regras para a coleta, processamento e armazenamento de dados pessoais. Outrossim, as organizações precisam obter o consentimento dos titulares dos dados antes de coletar e processar seus dados pessoais, além de garantir a privacidade e segurança desses dados. Na LGPD, essa necessidade é relativizada em algumas hipóteses (art. 7º, § 4ª[17])(BRASIL, 2018), o que, para Bioni (2019), não retira o caráter principal desse elemento na regulação da proteção dos dados pessoais, porque o legislador o inseriu reiteradas vezes ao longo do texto normativo.

As leis também estabelecem o direito dos titulares dos dados de acessar, corrigir e excluir seus dados pessoais, bem como estabelecem penalidades para empresas que não cumpram as regras.

---

[14] Artigo 28º - Subcontratante - 1. Quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados. [...]

[15] Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

[16] Artigo 9º - Tratamento de categorias especiais de dados pessoais - 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. [...]

[17] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; [...] § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. [...]

Assim como o regulamento europeu, a LGPD atinge a todos os setores da economia, sendo aplicável a entidades públicas e privadas, e possui efeito até mesmo extraterritorial, isto porque a norma é aplicável a qualquer operação de tratamento que seja efetuada por pessoa natural ou pessoa jurídica de natureza pública ou privada, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados, desde que a operação de tratamento tenha se realizado em território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; os dados pessoais objeto do tratamento tenham sido coletados no território nacional (art. 3º[18])(BRASIL, 2018).

De mais a mais, a LGPD não incorre na mesma omissão do MCI e, assim como faz o RGPD, conceitua e diferencia o que vem é dado pessoal, dado pessoal sensível e dado anonimizado (art. 5º[19])(BRASIL, 2018).

As prerrogativas instituídas pela lei são alinhadas com a linha principiológica traçada por ela. A LGPD estabelece, em seu art. 6º, os seguintes princípios: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas (BRASIL, 2018).

O princípio da finalidade estipula que o tratamento de dados pessoais deve ser feito com uma finalidade específica e legítima, e deve ser informada ao titular dos dados.

Por outro lado, o princípio da adequação determina que o tratamento de dados deve ser adequado à finalidade informada. Isto é, apenas dados necessários para atingir a finalidade específica devem ser coletados e tratados.

Ao seu turno, o princípio da necessidade institui que os dados pessoais

[18] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

[19] Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; [...]

coletados devem ser relevantes, proporcionais e não excessivos em relação à finalidade informada.

O princípio do livre acesso garante aos titulares acesso aos seus dados pessoais, além do poder de solicitar a correção ou exclusão de informações imprecisas. Tal princípio está alinhado com o princípio da qualidade dos dados, segundo o qual os dados pessoais devem ser precisos, atualizados e verdadeiros.

Noutro giro, o princípio da transparência determina que a organização responsável pela coleta dos dados seja transparente em relação à forma como eles são tratados, informando de maneira clara e acessível sobre as práticas de coleta e tratamento de dados. Esse princípio tem especial relevância na garantia do direito à autodeterminação informativa, afinal, para que o titular tome uma decisão consciente acerca da destinação de seus dados pessoais, é necessário que ele compreenda todas as etapas do tratamento.

Dessa maneira, esse princípio, nas palavras de Roberta Mauro Medina Maia (2020, p. 234) é “indispensável ferramenta legislativa para que a disparidade entre que aparta o controlador dos dados do titular dos mesmos possa ser mitigada”.

Outrossim, não basta que as informações sejam fornecidas aos titulares, é preciso que elas sejam acessíveis, isto é, sejam expostas em linguagem compreensível ao cidadão médio. Alinhado com esse entendimento, o § 6º do art. 14 da LGPD, que trata do fornecimento de informações acerca do tratamento de dados pessoais de crianças e adolescentes, é enfático:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> [...]
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. (BRASIL, 2018)

Com isso, o legislador instrumentaliza o princípio da transparência e orienta sua aplicação, esclarecendo que as informações fornecidas ao titular devem ser adequadas à sua capacidade de compreensão.

Na Europa, em função do RGPD, a Commision Nationale Informatique &

Libertés (CNIL), uma importante autoridade de proteção de dados, multou a rede de supermercados Carrefour em mais de € 3 milhões por fornecer informações complexas e imprecisas sobre o tratamento de dados pessoais[20].

Essa demanda por transparência, para Ingo Wolfgang Sarlet e Gabrielle B. Sales Sarlet, é uma consequência de um modelo monopolista. *In verbis*:

> Trata-se, de fato, de um cenário em face do qual se percebe uma nova roupagem para o conceito de Humanidade, sobretudo mediante a imposição de uma configuração relacionada com uma projeção/modelo dos monopólios, isto é, as chamadas Big techs, que, superando o poder estatal e dos diversos organismos internacionais, atualmente regem a área da tecnologia, implicando a necessidade de uma urgente mudança de rumo, permitindo que a opacidade ceda espaço à transparência, à auditabilidade e à compreensibilidade. Assim, em um panorama informacional, o escrutínio, a inclusão e a participação solidária e responsável deveriam ser cruciais e inalienáveis. (SARLET et al., 2022, p. 23)

Já o princípio da segurança, ao seu tempo, assegura que os responsáveis pelo tratamento de dados tomem medidas técnicas e organizacionais adequadas para protegê-los de acessos não autorizados, perda, destruição, alteração ou qualquer forma de tratamento inadequado.

Por fim, o princípio da não discriminação, um dos mais importante do arcabouço principiológico da LGPD (CARLOTO, 2020) tem como finalidade evitar que os dados pessoais sejam utilizados para discriminar pessoas, grupos ou comunidades. Esse princípio se mostra fundamental porque, com a elevada quantidade de informações tratadas e a elaboração de perfis para os usuários, certas características podem ser utilizadas para transpor formas já existentes de segregação para o mundo virtual.

Com esse princípio, a lei busca impor que os agentes de tratamento de dados atuem ativamente para evitar que esse o tratamento de dados pessoais seja orientado por preconceito. A preocupação ganha destaque em função do acelerado ritmo em que a tecnologia avança, responsável por permitir o surgimento de “formas obscuras de discriminação por raça, idade, gênero ou condição social” (CARNEIRO et al., 2020, p. 89).

Sendo assim, esse princípio está diretamente relacionado com característica de direito fundamental adquirida pela proteção de dados pessoais,

[20] Disponível em https://www.reuters.com/article/carrefour-privacy-idUKL8N2IC3NA. Acesso em 8 ago. 23

buscando assegurar tratamento isonômico, a despeito de características como etnia, gênero e orientação sexual.

Nessa toada, Julise Lemonje destaca que, embora os efeitos do princípio da não discriminação devam ser percebidos no tratamento de quaisquer informações, ele ganha especial relevo quando do tratamento de dados pessoais sensíveis. Com efeito:

> Embora todo e qualquer tratamento de dados deva se dar sob o manto do princípio que veda sua aplicação discriminatória, a preocupação com o princípio da não discriminação acentua-se quando do tratamento de dados pessoais sensíveis – quais sejam, aqueles que, conforme conceituação do artigo 5º, II, da LGPD, envolvam origem racial ou étnica, orientação sexual, opinião política, convicção religiosa, filiação sindical, ou informação de saúde, genética e biométrica de pessoa natural. (LEMONJE, 2022, p. 187)

Em sentido semelhante, Caitlin Mulholland (2018, p. 174) assevera que "esse princípio deve servir como base de sustentação da tutela dos dados sensíveis, especialmente quando estamos diante do exercício democrático e do acesso a direitos sociais, tais como o direito ao trabalho, à saúde e à moradia".

A autora, porém, argumenta que não é todo tipo de diferenciação que se caracteriza como ilícito e abusivo, de modo que é permitida a classificação de usuários em grupos diferentes. Veja-se:

> Em relação ao princípio da não discriminação, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. O legislador, ao relacionar o uso discriminatório às qualidades de ilicitude e abusividade, parece reconhecer a possibilidade de tratamento distintivo, desde que lícito e não abusivo. Isto é, aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas. (MULHOLLAND, 2018, p. 164)

Com isso, verifica-se que, embora a lei apresente algumas situações concretas, em muitos casos é necessário recorrer a ferramentas de interpretação para compreender qual agir é mais condizente com o conjunto principiológico da lei, que deve balizar sua interpretação, permitindo que eventuais conflitos sejam sanados por meio da análise do impacto das soluções nos direitos dos titulares de dados.

Nada obstante, observa-se, também, que alguns dos princípios são a gênese para normas objetivas, como é o caso do tratamento de dados pessoais

considerados sensíveis, enumerados no art. 5º, II, da LGPD[21]. Alicerçada no princípio da não discriminação, o art. 11 da LGPD[22] elenca as hipóteses nas quais o tratamento desse tipo de dado pessoal pode acontecer. O tratamento pode ser feito com o consentimento do titular dos dados ou para o cumprimento de uma obrigação legal ou regulatória. Ademais, o tratamento pode ocorrer quando é necessário proteger a vida ou a integridade física do titular ou de terceiros, para a tutela da saúde em procedimentos realizados por profissionais da área da saúde ou por autoridades sanitárias, para a execução de políticas públicas ou para a realização de estudos por órgãos de pesquisa.

Chama atenção a inserção, pela Lei n. 13.853/2019, do § 5º[23] ao dispositivo supramencionado (BRASIL, 2019). Com isso, é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde com a finalidade de seleção de riscos em qualquer modalidade de contratação e acréscimo ou retirada de beneficiários.

Essa inclusão revela que, para essa situação, prevalece o direito à privacidade dos titulares de dados pessoais em relação ao valor econômico que tais

---

[21] Art. 5º Para os fins desta Lei, considera-se: [...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[22] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[23] Art. 5º [...]

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

dados podem agregar às instituições responsáveis pela oferta de planos de saúde no mercado de consumo.

Ao mesmo tempo, as alíneas do inciso II do art. 11[24] revelam preocupação com a continuidade da utilização dessa categoria de dados para fins considerados indispensáveis ao legislador, como a execução de políticas públicas (alínea “b”) ou a realização de pesquisas científicas (alínea “c”) (BRASIL, 2018). Trata-se de um sopesamento dos princípios, feito pelo legislador quando da edição da lei.

Apesar dos avanços, ainda há desafios a serem enfrentados na proteção de dados. A implementação da LGPD é recente e muitas empresas e organizações ainda não se adequaram às suas regras. Outrossim, a velocidade com que novas tecnologias são desenvolvidas e adotadas torna difícil acompanhar os riscos e garantir a proteção dos dados. Por isso, é fundamental estudar o funcionamento dos mecanismos oferecidos pela Lei, para entender qual a melhor forma de aplicá-los, com base nos princípios e objetivos da LGPD.

Portanto, a proteção de dados é um assunto relevante e em constante evolução no ordenamento jurídico brasileiro. A implementação das leis e normas vigentes é essencial para garantir a privacidade e a segurança dos dados pessoais dos cidadãos e usuários, além de estimular o desenvolvimento de boas práticas por parte das empresas que lidam com essas informações. É importante que os cidadãos estejam conscientes de seus direitos e saibam como exercê-los, a fim de garantir que suas informações pessoais sejam tratadas de forma adequada.

A LGPD, porém, assegura prerrogativas também aos agentes envolvidos no tratamento de dados pessoais. Dentre essas prerrogativas, se destaca a garantia de proteção ao segredo de negócio, um conceito jurídico sempre tangenciado quando a proteção de dados é tema de discussão e alvo de análise no próximo

[24] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

tópico desta pesquisa.

1.2 Segredo de negócio

Como abordado no tópico anterior, a respeito da proteção de dados, a era digital, com seu avanço acelerado e a evolução constante de tecnologias, trouxe consigo uma ampliação das fronteiras da informação. Dados pessoais se tornaram ativos valiosos, gerando uma necessidade emergente de legislações protetivas, como observado nos panoramas europeu, norte-americano e, mais recentemente, brasileiro, com a instituição da LGPD.

Da mesma forma, o ambiente digital proporcionou um terreno fértil para inovações, desenvolvimentos tecnológicos e estratégias de negócios inéditas. Estas, por sua vez, estão frequentemente alicerçadas em informações vitais e exclusivas, que se enquadram na categoria de segredos de negócio. São esses segredos que, muitas vezes, garantem a uma empresa sua vantagem competitiva, posicionando-a de forma estratégica no mercado.

A preocupação com a proteção dos segredos de negócio, portanto, não é algo novo. Entretanto, assim como a proteção de dados, essa preocupação foi intensificada e reformulada no contexto do avanço tecnológico. Se outrora os segredos eram protegidos por cofres físicos e contratos de confidencialidade, hoje, eles são frequentemente guardados em servidores, na nuvem, e são suscetíveis a ataques cibernéticos, vazamentos e outras formas de exposição não autorizada.

Adicionalmente, em um mundo onde a transparência é cada vez mais valorizada, e legislações como a LGPD demandam clareza nas operações de tratamento de dados, é importante analisar como as organizações podem equilibrar a necessidade de proteger informações pessoais com a de salvaguardar os segredos de negócio.

1.2.1 Evolução e aplicação do segredo de negócio

De início, é crucial abordar a questão da nomenclatura atribuída ao instituto mencionado no título. Como existem diversos termos que podem ser usados para designar a mesma figura jurídica e, ao mesmo tempo, termos semelhantes, usados para designar figuras jurídicas diferentes, se faz necessário adotar terminologia mais abrangente. Neste trabalho, o termo "segredo de negócio" será

usado como descrição genérica e abrangente, da qual serão distintas figuras específicas, como o *know how* e o *trade secret*.

A ideia de segredo de negócio vem de longa data, podendo ter sido levada da China a Bizâncio ainda no século VI, como explica Ivana Maria Cyrne Lopes (2018, p. 18). A pesquisadora menciona, contudo, que a origem mais conhecida para os segredos de negócio vem do *common law*, de origem inglesa, no século XIX, e argumenta que “há um consenso geral de que a lei dos segredos comerciais como conhecemos fez sua primeira aparição na Inglaterra em 1817”.

Outro caso que ganha notoriedade quando se estuda o desenvolvimento histórico do instituto é Peabody v Norfolk, julgado pela Suprema Corte de Massachusetts em 1868 (MASSACHUSETTS, 1868). Nele, há uma descrição mais elaborada sobre o que seria um segredo de negócio. Com efeito:

> Se uma pessoa inventa ou descobre, e mantém em segredo, um processo de fabricação, seja ou não sujeito à patente, ele não tem direito exclusivo a ela contra o público ou contra aqueles que, de boa-fé, adquirem conhecimento dele, mas ele tem uma propriedade, que um tribunal de chancelaria protegerá contra aquele que, em violação do contrato, e uma quebra de confiança, se compromete a aplicá-lo para seu próprio uso ou para revelá-lo a terceiros. (MASSACHUSETTS, 1868, p. 7)

Há nesta decisão a citação de uma segunda, proveniente da Suprema Corte do Kansas, também sobre segredo de negócio, na qual a corte afirma que “um segredo de negócio pode existir em uma combinação de componentes, cada um destes, por si só, em domínio público, sendo a sua combinação um segredo” (KANSAS, 1968, p. 9).

Com a evolução tecnológica, marcada pela Revolução Industrial, o segredo de negócio passou a ser cada vez mais importante e ganhar mais relevância para as empresas (LOPES, 2019).

Um grande marco global para a proteção do segredo de negócio é a celebração do acordo *Trade Related Aspects of Itellectual Property Rights* (TRIPS), tratado internacional assinado em 1994, que veio para disciplinar aspectos do direito da propriedade intelectual relacionados ao comércio.

Esse acordo foi pioneiro no desenvolvimento de obrigação, para os adeptos, de proteção de informações confidenciais. Com isso, foram estabelecidas normas básicas sobre propriedade intelectual, que existiam em outros instrumentos internacionais ou nas jurisdições interna dos países (REICHMAN, 1995).

O acordo também institui parâmetros mínimos para a proteção de direitos de propriedade intelectual, relegando as regras nacionais ao patamar de subsidiárias em face do padrão de proteção uniformizado (BARBOSA, 2010, p. 177), e possui como objetivo fazer com que a proteção e a aplicação de normas de proteção dos direitos de propriedade contribuam para o avanço da tecnologia, bem como para sua disseminação em prol do bem-estar social e econômico (art. 7º[25])(OMC, 1994).

Nesse acordo, apenas o termo “informação confidencial” obteve unanimidade para tratar dos segredos de negócio (FEKETE, 2015). A conceituação de “informação confidencial”, porém, se confunde com a de segredo de negócio, tratando-se de:

> [...] 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, 2003, p. 420)

O acordo TRIPS faz alusão ao segredo de negócio, tratando-o como informação confidencial, em seu art. 39. Veja-se:

> ARTIGO 39
>
> 1. Ao assegurar proteção efetiva contra competição desleal, como disposto no ARTIGO 10 bis da Convenção de Paris (1967), os Membros protegerão informação confidencial de acordo com o parágrafo 2 abaixo, e informação submetida a Governos ou a Agências Governamentais, de acordo com o parágrafo 3 abaixo.
>
> 2. Pessoas físicas e jurídicas terão a possibilidade de evitar que informação legalmente sob seu controle seja divulgada, adquirida ou usada por terceiros, sem seu consentimento, de maneira contrária a práticas comerciais honestas, desde que tal informação:
>
> a) seja secreta, no sentido de que não seja conhecida em geral nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão, seja como um todo, seja na configuração e montagem específicas de seus componentes;
>
> b) tenha valor comercial por ser secreta; e c) tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta.

[25] ARTIGO 7 - Objetivos - A proteção e a aplicação de normas de proteção dos direitos de propriedade intelectual devem contribuir para a promoção da inovação tecnológica e para a transferência e difusão de tecnologia, em benefício mútuo de produtores e usuários de conhecimento tecnológico e de uma forma conducente ao bem-estar social econômico e a um equilíbrio entre direitos e obrigações.

> 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. (OMC, 1994)

Como se vê, o artigo deixa explícito que assegurar a proteção às informações confidenciais é assegurar "proteção efetiva contra competição desleal" e menciona o art. 10 bis da Convenção de Paris[26] (BRASIL, 1975), que trata sobre o tema.

O aludido artigo estabelece três requisitos para a proteção: a informação deve ser secreta, significando que não pode ser de conhecimento geral para as pessoas do mesmo ramo de atuação, o seu valor comercial deve existir em razão do segredo e o seu titular deve ter tomado medidas para garantir a manutenção do segredo sobre aquela informação (OMC, 1994).

Nessa conjuntura, a maior parte dos países costuma dividir segredos comercial e industrial em três categorias: informação técnica, o que incluiria informações sobre processos industrial e fórmulas; informação confidencial do negócio, como listas de consumidores, informações financeiras planos e negócio e outras informações relacionadas; e *know-how*, como métodos e passos para se chegar a determinado resultado (LIPPOLDT et al., 2014).

O Brasil, porém, não possui uma legislação muito sofisticada no que diz respeito aos segredos de negócio, instituto que, como será demonstrado no tópico seguinte, é trabalhado de maneira mais aprofundada pela doutrina no país.

---

[26] 1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3. 2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

1.2.2 Segredo de negócio no Brasil

Uma das consequências do tratamento raso dado pela legislação brasileira aos segredos de negócio é que não há, no Brasil, uma definição legal para o instituto. Segundo Kátia Braga de Magalhães, houve discussão acerca da inclusão de um capítulo dedicado a ele na Lei n. 9.279/1996 (Lei de Propriedade Industrial), com efeito:

> Ocorre que, a despeito das inúmeras discussões acerca do assunto e das tentativas, durante a tramitação, no Senado, do projeto que culminou na Lei de Propriedade Industrial em vigor (Lei nº 9.279/96), de nela incluir um capítulo autônomo sobre segredos de negócio, o ordenamento jurídico pátrio, em descompasso com o célere desenvolvimento das práticas comerciais, ainda não prevê uma conceituação legal expressa para este instituto. (MAGALHÃES, 2000, p. 75)

Para a autora, essa lacuna legislativa proporciona insegurança aos agentes econômicos e causa dificuldades ao Poder Judiciário na análise da temática. Veja-se:

> Tal omissão legislativa só pode gerar insegurança junto a todos os agentes econômicos responsáveis pelo desenvolvimento de técnicas de produção em caráter confidencial e, sobretudo, perplexidade perante o Poder Judiciário, ao ter de dirimir conflitos em torno de infrações a um conjunto de bens imateriais, cujas características não se acham elencadas em qualquer diploma legal. (MAGALHÃES, 2000, p. 75)

Uma consequência disso, enunciada por Newton Silveira, é que o tratamento dado pelo legislador ao segredo de negócio é genérico, com proteção conferida por meio das normas de repressão à concorrência desleal. Dessa forma, segundo o autor, o Direito não alicerçou o segredo ao patamar de bem imaterial objeto de propriedade (SILVEIRA, 2018).

Por outro lado, constitucionalmente, a proteção a esse tipo de informação se tem alicerce no direito fundamental de proteção as criações intelectuais, (art. 5º, XXIX[27]), além da proteção da intimidade e do sigilo da correspondência (FEKETE, 2018).

Outrossim, o acordo TRIPS foi ratificado pelo Brasil por meio Decreto n.

[27] Art. 5º [...] XXIX - a lei assegurará aos autores de inventos industriais privilégio temporário para sua utilização, bem como proteção às criações industriais, à propriedade das marcas, aos nomes de empresas e a outros signos distintivos, tendo em vista o interesse social e o desenvolvimento tecnológico e econômico do País;

1.355/1994. Como visto anteriormente, o acordo elenca, em seu art. 39, os elementos necessários à caracterização do segredo de negócio, de maneira que sua ratificação implica na possibilidade de transposição desses critérios para o ordenamento jurídico brasileiro. No mesmo caminhar, o Brasil havia ratificado a Convenção de Paris, em 1975, por meio do Decreto n. 75.572, de 8 de abril.

Apesar da inexistência de um conceito objetivo, a legislação interna, em alguns momentos, faz alusão ao segredo de negócio e assegura sua proteção. É o caso do art. 206 da Lei de Propriedade Intelectual (LPI), com efeito:

> Art. 206. Na hipótese de serem revelados, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, sejam segredo de indústria ou de comércio, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades. (BRASIL, 1996)

O mesmo diploma legal, em seu art. 195, ao tratar do crime de concorrência desleal, aborda a matéria nos incisos XI, XII e XIV. Veja-se:

> Art. 195. Comete crime de concorrência desleal quem:
>
> [...]
>
> XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;
>
> XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; ou
>
> [...]
>
> XIV - divulga, explora ou utiliza-se, sem autorização, de resultados de testes ou outros dados não divulgados, cuja elaboração envolva esforço considerável e que tenham sido apresentados a entidades governamentais como condição para aprovar a comercialização de produtos. (BRASIL, 1996)

Há ainda, na referida lei, o art. 209, que garante direito à indenização por perdas e danos quando houver violação a direitos de propriedade industrial e atos de concorrência desleal não previstos no diploma legal. Veja-se:

> Art. 209. Fica ressalvado ao prejudicado o direito de haver perdas e danos em ressarcimento de prejuízos causados por atos de violação de direitos de

> propriedade industrial e atos de concorrência desleal não previstos nesta Lei, tendentes a prejudicar a reputação ou os negócios alheios, a criar confusão entre estabelecimentos comerciais, industriais ou prestadores de serviço, ou entre os produtos e serviços postos no comércio. (BRASIL, 1996)

Por sua vez, a Consolidação das Leis Trabalhistas (CLT) também menciona segredo de empresa, elencando sua violação como constituinte de justa causa para rescisão do contrato de trabalho pelo empregador. *In verbis*:

> Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:
>
> [...]
>
> g) violação de segredo da empresa;

Diante da lacuna legislativa, a doutrina se encarrega de definir segredo de negócio como “o conjunto de métodos ou fórmulas empregados na fabricação de produtos, tais como particularidades de produção, uso de máquinas e ferramentas e manipulação de substâncias de certa procedência, em determinadas proporções” (MAGALHÃES, 2000, p. 75).

Trata-se, portanto, de uma forma de propriedade intelectual que protege informações confidenciais as quais dão às empresas vantagens competitivas. Dessa forma, a segurança desses segredos é preocupação crescente para as empresas em todo o mundo, uma vez que, com a digitalização dos processos produtivos, o risco de vazamento de informações confidenciais tornou-se ainda maior.

Nada obstante, a proteção do segredo de negócio é questão complexa, que pode ter implicações significativas para a concorrência e a inovação. Além de buscar a implementação de medidas técnicas que protejam essas informações, as empresas devem considerar os impactos mais amplos de suas decisões sobre o compartilhamento de informações.

Denis Barbosa enumera algumas figuras jurídicas que se amoldam ao conceito de segredo de negócio, por não serem objeto de exclusividade legal e serem construídas em torno de um segredo objetivo ou confidencialidade subjetiva. Dentre essas figuras jurídicas, elenca o *know how*, que, segundo o autor, “resume uma situação de fato: a posição de uma empresa que tem conhecimentos técnicos e de outra natureza, que lhe dão vantagem na concorrência, seja para entrar no mercado, seja para disputá-lo em condições mais favoráveis” (BARBOSA, 2010, p.

626).

Portanto, *know-how* é o conjunto de conhecimentos, não necessariamente técnicos, essenciais para conceder a uma empresa acesso, manutenção ou vantagem no mercado em que atua. Tal vantagem poderia ser conquistada de outras maneiras, como a concentração de recursos financeiros, posição legal privilegiada, competência dos gestores, acesso a fontes de matérias-primas e influência política, por exemplo.

Contudo, quando o acesso, manutenção ou vantagem de uma empresa no mercado resultam da forma como ela se organiza para produzir, seja em termos técnicos, administrativos ou comerciais, o *know-how* é representado pelo modelo dessa microestrutura de produção (BARBOSA, 2010). Destarte, o *know-how* engloba o conjunto de conhecimentos disponíveis sobre o modelo de produção específico de uma empresa, que lhe permite ter acesso a um mercado, manter-se nele ou obter vantagens em relação aos concorrentes.

Vale anotar que o *know how* se diferencia de outras figuras jurídicas associadas ao segredo industrial por estar diretamente associado à "falta de acesso por parte do público em geral ao conhecimento do modelo de produção de uma empresa" (BARBOSA, 2010, p. 627).

Para os fins desta pesquisa, entretanto, a figura jurídica que representa segredo de negócio mais relevante é a do segredo de fábrica, correlata ao *trade secret* do direito norte-americano.

Essa figura se encontra elaborada de forma mais consistente no direito norte-americano, que a define como:

> Um *trade secret* pode consistir em qualquer fórmula, padrão ou dispositivo ou compilação de informações que é usada em um negócio e lhe dá a oportunidade de obter vantagem sobre seus competidores que não o usam. Pode ser a fórmula de um composto químico, um processo de manufaturação, tratamento ou preservação de materiais, um padrão para uma máquina ou uma lista de consumidores. (AMERICAN LAW INSTITUTE, 1939, seção 757. p. 5, tradução nossa)

Paralelamente, existe uma ideia semelhante no direito francês, a de *secret de fabrique*. Denis Barbosa explica que se trata de "um conhecimento tecnológico, dotado de utilidade industrial e secreto: não se exige que seja novo nem que represente atividade inventiva - o que o distingue do invento patenteável" (BARBOSA, 2010, p. 637).

Segredo de fábrica, portanto, pode ser traduzido como uma solução técnica que se opta por manter em segredo.

Denis Barbosa (2010, p. 639) nos ensina que essa figura possui longo histórico no direito brasileiro, encontrando sua ressonância no art. 39, 6º, do Decreto n. 24.507, de 29 de junho de 1934, que tratava como ato de concorrência desleal a divulgação de “segredos de fábrica ou de negócio”[28] (BRASIL, 1934).

Posteriormente, o Decreto n. 7.903, de 27 de agosto de 1945, previa, no seu art. 178, XI e XI[29], repressão à utilização ou divulgação não autorizada de segredo comercial (BRASIL, 1945).

Atualmente, essa figura jurídica é protegida, no Brasil, pelo já mencionado art. 195 da LPI. Esse dispositivo elenca dois critérios à caracterização do segredo, quais sejam, a utilidade da informação, de uma perspectiva mercantil; e a não obviedade.

Vale destacar que o segredo não precisa ser absoluto, as informações podem ser compartilhadas dentro da organização ou com parceiros comerciais. O crucial, à caracterização do segredo de negócio, é que a informação não esteja facilmente acessível ao público. Outrossim, o público também não é, necessariamente, o público em geral, mesmo o livre acesso pelos concorrentes às informações ou obviedade delas para um técnico no assunto bastam para descaracterizar o segredo (BARBOSA, 2010).

Ademais, no bojo da aplicação da LPI, presume-se o contexto de concorrência. Caso não seja verificada tal concorrência, o remédio voltado à repressão da disseminação do segredo deverá ser buscado em outras legislações, como o Código Penal, especialmente seus arts. 153 e 154[30] (BRASIL, 1940)

---

[28] Art. 39. Constitui ato de concorrência desleal, sujeito às penalidades previstas neste decreto: [...] 6º, desvendar a terceiros, quando em serviço de outrem segredos de fábrica ou de negócio conhecidos, em razão do ofício;

[29] Art. 178. Comete crime de concorrência desleal que: [...] X. receber dinheiro ou outra utilidade, ou aceitar promessa de pagar ou recompensa, para faltando ao dever de empregado proporcionar à concorrente do empregador vantagem indevida; XI. divulga ou explora, sem autorização, quando a serviço de outrem, segredo de fábrica, que lhe foi confiado ou de que tece conhecimento em razão do serviço;

[30] Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: Pena - detenção, de um a seis meses, ou multa, de trezentos mil réis a dois contos de réis. Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de três meses a um ano, ou multa de um conto a dez contos de réis.

(BARBOSA, 2010).

Hodiernamente, no contexto da sociedade informacional, essa figura jurídica ganha especial relevância na medida em que se relaciona às formas de tratamento de dados pessoais. No cenário atual, em que o mercado informacional movimenta grandes quantias de dinheiro, os atores que possuem os melhores métodos de tratamento de dados têm uma clara vantagem em relação aos demais competidores. Isto é, no âmbito desse mercado, o tratamento de dados desempenha papel fundamental.

As organizações que conseguem coletar, armazenar, analisar e utilizar esses dados de maneira eficiente são capazes de obter informações valiosas sobre seus clientes, identificar tendências de mercado, personalizar produtos e serviços, e aprimorar a tomada de decisão estratégica. Esses métodos de tratamento de dados, que conferem uma vantagem competitiva, podem ser considerados segredos de negócio.

Naturalmente, a preocupação em manter a salvo esses segredos adquire grande relevância diante da crescente demanda por transparência no tratamento de dados pessoais. Dessa forma, é importante compreender quais ferramentas podem ser usadas pelas empresas, para evitar o compartilhamento dessas informações e, concomitantemente, satisfazer a necessidade de informações sobre a forma como é realizado o tratamento dos dados pessoais sob sua custódia.

Em função disso, a LGPD trata do assunto em alguns de seus artigos, traçando uma relação entre o segredo de negócio e a transparência dos processos de tratamento de dados pessoais, como será tratado no próximo tópico.

1.3 LGPD e segredo de negócio

No rasto do que foi previamente exposto, acerca da importância de salvaguardar os interesses dos titulares de dados pessoais, especialmente diante do elevado interesse econômico que gravita em torno do tratamento dessas informações, e da relevância que a confidencialidade de alguns métodos usados no tratamento desses dados possui para algumas empresas, a LGPD apresenta, em seu texto, algumas menções a segredo de negócio, referindo-se ao instituto como “segredo industrial”.

A mais significativa delas, para a intepretação dos comandos contidos na

lei, é a contida no art. 6º, VI, onde o princípio da transparência é apresentado. Segundo esse dispositivo, o princípio representa 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" (BRASIL, 2018).

Essa inserção, ao final do comando, é de suma importância, porque demonstra que a preocupação em salvaguardar os segredos de negócio possui papel importante na edição da norma, ocupando o mesmo espaço em que é estabelecido um dos princípios mais significativos da lei.

Ao todo, a LGPD menciona "segredos comercial e industrial" treze vezes. Além do art. 6º, o termo aparece no art. 9º, II; art. 10, § 3º; art. 18, V; art. 19, II e § 3º; art. 20, §§ 1º e 2º; art. 38; art. 48, § 1º, III; e art. 55-J, II, X e § 5º.

A maior parte das vezes em que a observância do segredo de negócio é mencionada, ela contrapõe um dever decorrente da instrumentalização do princípio da transparência. O art. 9º, por exemplo, trata do acesso do titular às informações acerca do tratamento de dados. Com efeito:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
>
> [...]
>
> II - forma e duração do tratamento, observados os segredos comercial e industrial;

Vê-se que, ao mesmo tempo, o legislador busca garantir ao titular um nível suficiente de informação a respeito da forma como seus dados pessoais serão tratados e proteger as empresas que obtém vantagens competitivas por meio desse tratamento.

Ao seu turno, o art. 10, § 3º, estatui que, quando a base para o tratamento for o legítimo interesse do controlador, a ANPD poderá relatório de impacto à proteção de dados. Essa demanda, porém, é limitada pela observância do segredo de negócio. Senão vejamos:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

> [...]
>
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

É hialino, portanto, o princípio da transparência possui limitações e não é mandatória a cessão de absolutamente qualquer informação a respeito do tratamento de dados. Contudo, também não se pode admitir que, nas situações em que a lei destaca o respeito ao segredo de negócio, o controlador e o operador podem se furtar irrestritamente de fornecer informações aos titulares e à ANPD, afinal, isso constituiria sério óbice à fiscalização do tratamento de dados pessoais.

Esse conflito também existe no âmbito europeu, onde o RGPD também contrapõe a ideia de transparência ao respeito aos segredos de negócio. A problemática é tão notória que, ao analisar os impactos do *Big Data* para os dados pessoais, a Autoridade Europeia para a Proteção de Dados (2015) sugeriu que disputas relacionadas a essa dualidade sejam resolvidas com a participação das autoridades nacionais de proteção de dados.

Malgieri, ao analisar esse conflito, avalia que, a princípio, em um conflito direto, os direitos à privacidade parecem prevalecer, mas uma avaliação criteriosa detido permite compreender que há apenas uma situação de não-prevalência imediata entre um e que a solução deve ser focada no caso específico (MALGIERI, 2016).

Assim, se estabelece um diálogo com Alexy (2006), referente à sua distinta separação entre regras e princípios, os quais são autênticos mandamentos de otimização. De fato, torna-se imperativo ponderar entre o direito de proteção de dados pessoais e o princípio da livre iniciativa, fundamental para o segredo empresarial.

Tratando da LGPD especificamente, essa imperatividade de ponderação surge reiteradamente, como visto na descrição do princípio da transparência, situação em que o legislador ressaltou a importância do segredo empresarial.

Assim, o cenário brasileiro se amolda à sugestão da Autoridade Europeia para a Proteção de Dados de que as autoridades nacionais sejam atores fundamentais em meio a essa controvérsia, pois, dentre as atribuições da ANPD, listadas no art. 55-J da LGPD, está o zelo tanto pela proteção dos dados pessoais

quanto pela observância dos segredos de negócio (incisos I e II[31])(BRASIL, 2018).

Dessa maneira, a análise quanto à quais aspectos do tratamento de dados podem ser mantidos em segredo e quais devem ser publicizados deve ser pautada na situação concreta. Isto é, é preciso considerar quais as consequências da publicização de aspectos do tratamento de dados pessoais que podem caracterizar segredo de negócio e quais as consequências da manutenção do sigilo dessas informações ao nível de compreensão que os titulares possuem sobre o que está sendo feito com seus dados.

Ana Frazão chama atenção para esse aparente conflito entre a proteção ao segredo de negócios e a transparência prescrita pela lei, destacando que a solução não é simples, algo confirmado pela própria LGPD, que "ao mesmo tempo em que prevê os princípios da transparência e da *accountability* e prestação de contas, também assegura, em diversos artigos, a proteção do segredo de negócios" (FRAZÃO, 2021, p. 2).

Uma das situações concretamente descritas na lei e que suscitam essa discussão é a prevista no art. 20 da LGPD. Tal dispositivo aborda a tomada de decisões de maneira automatizada, enunciando que:

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

Outrossim, o § 1º desse artigo, em observância ao princípio da transparência, franqueia ao titular de dados pessoais acesso a informações sobre o tratamento realizado, asseverando que:

> [...] o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. (BRASIL, 2021)

Nada obstante, a ressalva feita ao final do § 1º suscita uma série de questões, dentre elas a indagação sobre como assegurar a inexistência de aspectos

[31] Art. 55-J. Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; [...]

discriminatórios no tratamento automatizado de dados. Endereçando esse questionamento, o § 2º do mesmo dispositivo faz a seguinte previsão:

> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

A lei, como se observa, não informa parâmetros para a realização dessa auditoria, o que levanta dúvidas acerca dos métodos a serem utilizados pela ANPD.

No sentido do que foi exposto previamente, a escolha desse método deverá respeitar os comandos principiológicos da lei, de modo que permita, ao mesmo tempo, um entendimento claro do titular de dados e da ANPD sobre o tratamento, e não revele informações confidenciais que são de suma importância para o negócio.

Para melhor compreender como isso pode ou deve acontecer, se faz necessário compreender aspectos como a deleteriedade do tratamento automatizado de dados pessoais, bem como quais são as possíveis metodologias usadas para realizar o tratamento, de forma a compreender como isso, em face dos riscos à segurança dos dados, impacta a escolha do método, que serão abordados no próximo capítulo.

2. TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS

O advento das tecnologias de informação e comunicação, especialmente nas últimas décadas, revolucionou a maneira como coletamos, processamos e utilizamos dados. De plataformas de redes sociais a sistemas bancários, de assistentes virtuais a plataformas de *e-commerce*, a transformação digital deixou uma marca indelével em quase todos os aspectos da vida cotidiana.

Em meio a esse cenário de crescente digitalização, o tratamento automatizado de dados emergiu não apenas como uma tendência, mas como uma necessidade. Organizações de todas as dimensões, que atuam nos mais variados setores, buscam otimizar operações, tomar decisões mais informadas e oferecer experiências personalizadas aos usuários através da automação.

Entretanto, com essa transição acelerada, surgem questões intrincadas, sobretudo a respeito de como garantir que os dados pessoais sejam tratados de forma justa e transparente e como as leis e regulamentos se alinham à rápida evolução da tecnologia. E, mais profundamente, como equilibrar os imperativos de inovação e eficiência com os direitos fundamentais de privacidade e proteção de dados.

Diante desse panorama, é notório que o tratamento automatizado de dados desempenha um papel central na atual paisagem tecnológica e socioeconômica. Dessa forma, é fundamental compreender as nuances dessa modalidade de tratamento de dados pessoais não apenas do ponto de vista tecnológico, mas também suas implicações sociais, éticas e jurídicas.

A LGPD, por exemplo, não só reconhece a existência e relevância desse método de tratamento, como também estabelece salvaguardas específicas para proteger os direitos dos titulares cujos dados são submetidos a esse tipo de tratamento. Assim, este capítulo, além de aprofundar a compreensão sobre um fenômeno tecnológico emergente, também fundamenta a necessidade de um olhar crítico e informado sobre as interseções entre tecnologia, sociedade e direito, explorando o equilíbrio entre a eficiência trazida pelo tratamento automatizado e a proteção dos direitos fundamentais.

Dessa maneira, neste capítulo será feita uma análise acerca do que é tratamento automatizado, com o fito de desvendar suas facetas tecnológicas e as

motivações por trás de sua adoção. Ademais, serão investigados os benefícios e malefícios proporcionados por essa modalidade de tratamento de dados pessoais, bem como a maneira como a LGPD trata o assunto.

2.1 O que é tratamento automatizado de dados pessoais

Como dito previamente, o avanço tecnológico impulsionou a edição de legislações buscando estabelecer parâmetros seguros para a utilização de dados pessoais. A LGPD, dentre suas principais inovações, traz a menção ao tratamento automatizado de dados pessoais, modalidade que envolve a utilização de mecanismos computadorizados, como a inteligência artificial, para tomar decisões com base nas informações pessoais coletadas.

Nesse sentido, Ronaldo Lemos destaca a importância do avanço tecnológico para a disseminação de métodos automatizados de tratamento de dados, frisando que a evolução tecnológica serve como mola propulsora da coleta de dados, oferecendo uma vasta gama de opções para os agentes de tratamento e aumentando o risco de vazamento de dados. Veja-se:

> A quantidade de informações digitais é inesgotável: toda interação eletrônica, toda operação bancária e de crédito e cada simples assinatura de uma revista ficarão digitalmente gravados e ligados a indivíduos específicos, havendo notável risco de violação do sigilo desses dados para finalidades várias, inclusive ilícitas, ainda que inúmeros usuários da rede não tenham ciência do perigoso rastro que deixam a cada acesso. (LEMOS, 2014, p. 739-740)

Danilo Doneda também frisa que, por meio das plataformas existentes na internet, os dados pessoais podem ser coletados e tratados com grande velocidade. Essa administração eficaz, para o autor, foi viabilizada por uma técnica estatística que busca filtrar informações pertinentes para um serviço específico a partir do tratamento de vastas quantidades de informação não processada (DONEDA, 2010).

Também faz coro ao entendimento Bruno Bioni, para quem esse modelo de processamento de dados elimina a necessidade de estruturação preliminar para sua subsequente análise e permite a manipulação de vastos volumes de dados para variadas finalidades, economizando tempo e possibilitando a interrelação das informações para estimar a probabilidade de eventos futuros (BIONI, 2019).

Mesmo diante desse avanço tecnológico, é importante, ao falar de tratamento automatizado de dados pessoais, ressaltar a diferença existente entre o

processo decisório realizado por máquinas e o realizado por seres humanos. Enquanto seres humanos agem de forma consciente, com livre arbítrio, as máquinas agem com base em cálculos e serão fiéis aos resultados determinados pelo seu conjunto de instruções. Senão vejamos:

> A concepção de uma decisão automatizada envolve vários elementos, e somente se tornou possível com o uso de computadores eletrônicos. Na verdade, apenas em sentido metafórico se pode falar em "decisão" aqui, porque a máquina não age de modo consciente com algum propósito, mas apenas efetua cálculos aritméticos, segundo um programa (algoritmo) e conforme os dados que a alimentam. Logo, as máquinas apenas podem emular a parcela calculável da inteligência humana, não o livre-arbítrio, nem sentimentos, nem emoções. (REIS, 2021, p. 84)

Isto é, quando uma máquina realiza um processo de tomada de decisão, ela usa dados de entrada para fazer uma previsão. Essa previsão será dependente do processo de aprendizado do modelo ou algoritmo durante a fase de treinamento. Ao combinar essa previsão com o julgamento, que se traduz na escolha de uma solução conforme as diretrizes expressas no algoritmo ou modelo, a máquina indica uma ação (AGRAWAL et al., 2018).

Antes de continuar tratando sobre tratamento automatizado de dados, é importante diferenciar algoritmo e modelo. Enquanto um algoritmo pode ser explicado como uma sequência de raciocínios, instruções ou operações para alcançar um objetivo, um conjunto de regras voltadas à solução de problemas; um modelo, ao seu turno, pode ser descrito como "o resultado de poderosos algoritmos de *machine learning* aplicados a grandes e complexos bancos de dados" (KEARNS, et al., 2019, p. 9).

Essa distinção é especialmente importante para os fins do presente trabalho porque o algoritmo, enquanto código, pode ser protegido pelo direito autoral, fugindo, portanto, do âmbito de incidência das regras atinentes ao segredo de negócio. O conceito de modelo, por outro lado, seria mais adequado à constituição de um segredo de negócio, porque pressupõe a simbiose do algoritmo com uma base de dados, voltada à resolução de um problema concreto.

Outrossim, os modelos usados no tratamento de dados pessoais têm progredido cada vez mais, especialmente em função da melhora das soluções de inteligência artificial, as quais permitem que o aprendizado de máquina aconteça com cada vez menos interferência humana, aumentando exponencialmente a

capacidade de aprimoramento das soluções empregadas no processo de tomada de decisão. Segundo Nazareno Reis, essa é a base da revolução que estamos vivendo atualmente. Com efeito:

> Na base de toda essa revolução está a Inteligência Artificial e os múltiplos usos que ela é capaz de fazer do grande volume de dados disponíveis na internet ou fora dela, sobretudo por meio do chamado Aprendizado de Máquina (*Machine Learning*). O conjunto dos efeitos sociais desses usos ainda é um território desconhecido, pleno de possibilidades, de esperanças e de muitos receios também. (REIS, 2021, p. 13)

Os resultados da tomada automatizada de decisão são especialmente beneficiados com esse progresso, pois passam a contar com auxílio dos chamados meta-algoritmos, soluções algorítmicas que “otimizam o trabalho de construção do modelo, mediante a revisão sistemática dos dados de saída, segundo o resultado desejado pelo programador, para melhor agrupá-los e interrelacioná-los” (NAZARENO, 2021, p. 86).

Esse processo pode ser descrito a partir de uma relação simples, em que os dados de entrada, processados com base em uma relação de implicação condicional, geram dados de saída como resultado.

Dessa forma, como dito no capítulo anterior, é notório que os resultados estão sobremaneira ligados aos dados de entrada, cuja qualidade pode, inclusive, superar em importância a sofisticação do modelo. Peter Norvig, diretor de pesquisa do Google, corroborou essa ideia quando afirmou: “Nós não temos melhores algoritmos. Nós temos apenas mais dados” (MCAFEE et al., 2012).

Esses métodos elaborados de tratamento de dados pessoais possibilitam a utilização de informações esparsas, relacionando-as de maneira inicialmente impensável. É o que ensina Nazareno Reis:

> Com efeito, métodos sofisticados de tratamento de dados, chamados genericamente de Inteligência Artificial, permitem a recopilação de dados dispersos para reconstituir ações humanas e para analisar, prever ou mesmo induzir comportamentos futuros. Enfim, permitem formar uma imagem completa do indivíduo, a partir dos vestígios digitais dos seus movimentos nas redes, prognosticando as suas ações, características, interesses e até pensamentos. (REIS, 2021, p. 160)

Sendo assim, verifica-se constantemente o alcance de resultados que pareceriam impossíveis há algum tempo, porquanto as soluções de inteligência artificial têm se mostrado capazes de identificar relações que antes passavam

despercebidas.

Originalmente, os programadores indicam ao modelo qual é a conexão esperada entre os dados. A partir de então, o modelo passa a reproduzir esse padrão, replicando-o seguidas vezes e aprimorando cada vez mais seus critérios, identificando novas relações e sutilezas nas relações previamente informadas. Conforme o modelo vai sendo aplicado, “os usuários também acabam ajudando o modelo a melhorar, por meio de suas interações, que nada mais são do que rotulações para o modelo” (REIS, 2021, p. 106).

Sendo assim, é possível afirmar que o modelo está “aprendendo por experiência” quando, partindo de parâmetros pré-determinados, consegue implementar a acurácia dos resultados obtidos a partir da análise dos resultados de interações anteriores (MITCHELL, 1997).

Dentro das soluções de inteligência artificial, destacam-se os modelos que trabalham com *machine learning*. Esse tipo de modelo busca emular o funcionamento do cérebro humano. Por meio desse tipo de solução, é possível transformas os dados pessoais em conhecimento, como leciona Nazareno Reis:

> É por meio do Aprendizado de Máquina (*Machine Learning*), o tipo de programação mais usado em aplicações práticas, que dados pessoais podem ser transformados em informações e em conhecimento, por dispositivos que funcionam de forma autônoma, mediante associações, agregações e desagregações, arranjos e rearranjos de dados; análises de padrões em vastos conjuntos de dados; inferências estatísticas e estimativas probabilísticas — enfim, técnicas matemáticas convenientes para extrair conhecimentos de dados, mimetizando o funcionamento da inteligência humana, ou, pelo menos, a parte computável da inteligência humana. (REIS, 2021, p. 89)

Analisar a forma como o padrão busca imitar a mente humana pode promover uma interessante reflexão sobre nossa própria racionalidade, que se fundamenta na observação do mundo e busca organizá-lo intelectualmente, conforme padrões identificados no passado, para antecipar o futuro.

Ingo Wolfgang Sarlet e Gabrielle B. Sales Sarlet também destacam a semelhança entre os processos decisórios de natureza humana e os produzidos por soluções de inteligência artificial, com destaque para técnicas de *machine learning*:

> A artificialização da inteligência, deve-se sublinhar, tem como suporte o uso de máquinas que, mediante o armazenamento, o tratamento e o compartilhamento de dados passam a encetar algumas ações de

> reconhecimento, de perfilhamento, dentre outras, que, produzem processos de natureza decisória equiparáveis aos humanos. Para tanto, destaca-se *machine learning* como sendo uma subárea da IA que possui a aptidão para detectar padrões de forma automática, utilizando-os para realizar prognoses, e, assim, atuar em processos decisórios. (SARLET et al., 2022, p. 20)

É possível afirmar que os modelos buscam aumentar a precisão do modelo por meio do uso de diversas combinações de variáveis, "criando neurônios e utilizando pesos que otimizem a sua performance, independentemente de elas fazerem ou não sentido para nós, seres humanos" (MUSSA, 2020, p. 86).

Essa potencial convergência entre as novas tecnologias e o funcionamento do cérebro humano é digna de nota porque, em função da crescente evolução na capacidade de processamento, a qual passa pela implementação da capacidade de *hardware*, as soluções estão alcançando o ponto de superar a capacidade humana em certas atividades (SARLET, 2022, p. 20).

2.1.1 Benefícios do tratamento automatizado de dados pessoais

Em função do acentuado progresso destacado no tópico anterior, essas técnicas, quando empregadas ao tratamento de dados pessoais, podem trazer inúmeras vantagens, notadamente a agilidade e eficiência na tomada de decisões. Além disso, compreendem usos muito diversificados, que vão desde a análise da capacidade de pagamento até o diagnóstico de doenças e a detecção de objetos por imagens.

No caso de agentes que lidam com quantidades muito grandes de dados, como governos e empresas, a velocidade de resposta tem papel fundamental na adoção de soluções dessa natureza. É o que leciona Nazareno Reis:

> O que leva as empresas e os governos a automatizarem os seus processos decisórios é, sem dúvida, o aumento da capacidade e da velocidade de resposta a demandas repetitivas e a redução de custos que isso proporciona. Por isso mesmo, decisões políticas ou que contenham elementos discricionários ou de estratégia negocial normalmente permanecem sob a governança estritamente humana, embora possam ser subsidiadas por tratamentos automatizados de dados. (REIS, 2021, p. 102)

Assim, é possível, com o emprego dessas soluções, abandonar diversos percalços relacionados à baixa capacidade de oferta de serviços com alta demanda, usualmente verificados nas repartições públicas.

Isto é, a utilização dessas ferramentas gera um valor para o mercado consumidor, especialmente para as empresas de publicidade e marketing digital. Usando esses mecanismos, elas realizam publicidade segmentada, um método comunicativo que visa incentivar o consumo entre um público que tem maior probabilidade e interesse em adquirir um produto específico (BIONI, 2019).

Outrossim, são examinados dados que até recentemente não existiam, como os *cookies*, usados pelas empresas para "rastrear a navegação do usuário e, por conseguinte, inferir seus interesses para correlacioná-los aos anúncios publicitários" (BIONI, 2019, p. 16).

Vale dizer, os resultados alcançados são muito expressivos. Modelos de *deep learning* alcançam acurácia de 95% em situações não excepcionais, observadas em uma grande diversidade de contextos, o que revela a robustez das soluções e seu grande potencial (MUSSA, 2020, p. 91).

Essa alta precisão, aliada à alta velocidade e à progressão da capacidade computacional, se adotada uma perspectiva otimista, pode pavimentar o caminho para uma sociedade de abundância, na qual os dados são analisados e convertidos em informações relevantes, que serão aplicadas ao mundo real, em um ciclo operado a nível global (HITACHI, 2018).

Adriano Mussa comenta esse ciclo, explicando como ele pode ser aplicado ao desenvolvimento de produtos e serviços cada vez melhores. Veja-se:

> Em linhas gerais, o ciclo funciona da seguinte forma: se a organização desenvolver um produto ou serviço de qualidade satisfatória, ela conseguirá alguns usuários iniciais. Os usuários iniciais, ao utilizarem o produto ou serviço, gerarão dados que serão coletados e armazenados pela organização. Esses dados, se bem tratados por técnicas de Inteligência Artificial, principalmente Machine Learning, possibilitarão a melhoria do produto ou serviço. O produto ou serviço aperfeiçoado levará à aquisição de mais usuários. Mais usuários gerarão mais dados; mais dados levarão à melhoria do produto ou serviço e esse ciclo seguirá continuamente. (MUSSA, 2020, p. 105)

Ao caminhar nessa direção, a evolução tecnológica pode culminar, em última instância, em uma revolução social, alterando paradigmas consagrados do capitalismo. Pode-se dizer, a partir desse prisma, que o capitalismo, responsável por alimentar a evolução tecnológica, está pavimentando o caminho para seu fim – ou para mudanças significativas em suas bases.

Essa, naturalmente, é uma visão otimista dos resultados que possíveis de

se alcançar, enquanto sociedade, por meio do tratamento automatizado de dados em larga escala. Mas essa modalidade de tratamento também traz consigo grandes preocupações em relação à proteção dos direitos dos titulares de dados.

2.1.2 Riscos do tratamento automatizado de dados pessoais

Todo o avanço nos métodos computadorizados de tratamento de dados pessoais evoca uma série de questões não apenas práticas, mas também éticas. A preocupação com privacidade nunca esteve tão em voga e o grau de acesso que grandes companhias possuem a aspectos íntimos da vida de seus usuários fomentam uma série de debates sobre a temática.

O cofundador do *Whatsapp*, Brian Acton, por exemplo, levantou essa preocupação ao afirmar que havia vendido privacidade dos seus usuários[32] após a venda da empresa para o *Facebook* por US$ 22 bilhões[33].

Além disso, hodiernamente não existem mais dados irrelevantes, por conta do processamento computadorizado, sobretudo porque, sendo os dados projeções da personalidade, o seu tratamento, seja qual for, potencialmente pode violar direitos fundamentais (MENDES et al., 2018).

Também é necessário destacar que, mesmo dependendo de uma série de ações humanas para ser aplicados inicialmente, modelos usados para tratar dados em larga podem alcançar estágios de funcionamento autônomo. Nesses estágios, a supervisão das atividades desempenhadas por esses modelos se torna muito difícil, se não impossível, devido ao elevadíssimo volume de operações realizadas em um curtíssimo espaço de tempo.

Ademais, apesar de apresentarem resultados muito animadores, não há um modelo que consiga trabalhar com todas as variáveis possíveis, o que torna impossível a missão de desenvolver um modelo que resulte em uma predição correta em 100% das vezes. Isso se deve ao fato de que, como demonstram os teoremas da incompletude de Gödel, a conversão de eventos do mundo material em dados computáveis leva a um grau de incerteza em nível matemático (HILDREBRANDT, 2019).

---

[32] Disponível em: <https://olhardigital.com.br/2018/09/26/noticias/criador-do-whatsapp-se-declara-um-vendido-por-entregar-app-ao-facebook/>. Acesso em: 14 nov. 23.

[33] Disponível em: < https://g1.globo.com/economia/negocios/noticia/2014/10/preco-de-compra-do-whatsapp-pelo-facebook-sobe-us-22-bilhoes.html>. Acesso em: 14 nov. 23.

Soma-se a isso o fato de que a otimização matemática é implacável, o que significa que o modelo não se deterá diante de nenhuma circunstância, a menos que seja programado para fazê-lo. É dizer, há incerteza no momento em que os fatos do mundo real são transpostos a uma forma de informação compreensível pelo modelo, mas o modelo trabalhará com essa informação de modo inflexível.

Além disso, esses modelos apresentam vieses, muitas vezes ligados ao contexto cultural em que as pessoas envolvidas no seu desenvolvimento estão inseridas. Também é preciso compreender quais desses vieses são adequados à finalidade do tratamento de dados pessoais, como explica Terrence Sejnowski:

> Todas as redes neurais que classificam entradas são tendenciosas. Em primeiro lugar, a escolha das categorias de classificação incorpora um viés que reflete o preconceito humano na forma como esmiuçamos o mundo. Por exemplo, seria útil treinar uma rede para detectar ervas daninhas em gramados. Mas como identificá-la? A erva daninha de um homem pode ser a flor silvestre de outro. A classificação é um problema muito mais amplo, que reflete vieses culturais. Essas ambiguidades precisam integrar os conjuntos de dados usados para treinar a rede (SEJNOWSKI, 2019, p. 135).

Isso se dá porque “definir a organização do conhecimento em bibliotecas e arquivos é um trabalho classificatório artificial, com impactos na representação de indivíduos e grupos, assim como na descoberta, no resgate ou na recepção de produção intelectual” (SILVA, 2022, p. 156).

O viés, portanto, pode estar na base de dados usada pelo modelo para trabalhar e se aprimorar. Sendo assim, como a inteligência artificial tem sido frequentemente usada para a tomada de decisões, a vida das pessoas fica cada vez mais vulnerável a tratamentos discriminatórios, até mesmo em investigações policiais (BRAYNE, 2020).

Os vieses, propositais ou não, serão replicados indefinidamente nas decisões. Por sua vez, essa eventual replicação de um padrão discriminatório possibilita o surgimento de situações em que uma determinada parcela dos titulares é sistematicamente prejudicada em função de alguma característica. As consequências desses prejuízos, então, podem impactar diretamente aspectos da vida desses indivíduos, o que fará com que os dados gerados por eles dali em diante sejam afetados pelo viés original, fato que alimentará outros modelos, em um ciclo vicioso no qual são perpetuados aspectos discriminatórios no tratamento de dados pessoais.

Nesse cenário, é possível que, em função de um viés algorítmico presente no modelo original, o modelo passe a disseminar esse viés, fazendo com que ele se materialize. Ou seja, é necessário compreender o modelo não apenas como algo capaz de interpretar a realidade, mas também de alterá-la.

Há alguns casos notáveis em que o tratamento automatizado de dados pessoais resultou em prejuízo a cidadãos pertencentes a minorias. Um dos mais famosos aconteceu em Los Angeles, na Califórnia, e diz respeito ao reconhecimento facial em locais públicos (GARVIE et al., 2016). Na fase de aplicação do modelo, foi constatado que o sistema de reconhecimento facial da polícia apresentava uma taxa de erro maior ao identificar pessoas negras em comparação com pessoas brancas. Essa disparidade ocorreu porque, durante a fase de aplicação do modelo, a maioria das pessoas procuradas era de origem negra, enquanto na fase de treinamento do modelo foram expostas predominantemente faces brancas, resultando em um melhor reconhecimento natural dessas faces em detrimento das outras.

Outro caso emblemático é o de um experimento divulgado por Nicolas Kayser-Bril, membro do *AlgorithmWatch*, em que a ferramenta *Google Vision*, quando confrontada com a foto de uma pessoa segurando um termômetro portátil, item muito comum durante a pandemia da covid-19, etiquetava a foto de maneira diferente conforme a etnia da pessoa retratada. Para a foto de uma mão negra, etiquetas como “arma” e “arma de fogo” apareciam entre as mais recomendadas, ao passo em que, para a foto de uma mão branca, os rótulos mais indicados eram relacionados a tecnologia[34].

Em nota, a Google se desculpou e reconheceu que, quando o viés é descoberto, muitas pessoas já foram afetadas pelas decisões enviesadas que o modelo tomou[35].

Outra grande empresa, a Amazon, também já esteve no epicentro de um escândalo envolvendo discriminação algorítmica. Nesse caso, a empresa dispunha de um sistema voltado à admissão de funcionários. Contudo, a base de dados com a qual o modelo foi treinado contava com informações de currículos recebidos ao longo de uma década. Como a maior parte dos selecionados no período era do sexo

[34] Disponível em: <https://racismandtechnology.center/2021/02/19/racist-technology-in-action-gun-or-electronic-device/>. Acesso em: 14 nov. 23

[35] Disponível em: <https://algorithmwatch.org/en/google-vision-racism/>. Acesso em: 14 nov. 23

masculino, o modelo priorizava candidatos homens[36].

O exemplo da Amazon reforça que o viés, muitas vezes, está na base de dados. Acerca do assunto, Chiara Teffé reforça a importância que as bases de dados possuem nos resultados e como essa é uma temática especialmente importante hodiernamente, frente à presença cada vez maior da tecnologia na vida das pessoas. Nesse sentido, afirma a autora:

> Como se sabe, a depender da base de dados utilizada para treinar o algoritmo e/ou de como ele foi programado, ele poderá oferecer um resultado discriminatório. Tão importante quanto o algoritmo é a base de dados a ele subjacente e o enviesamento que pode vir a reboque. Como a inteligência artificial tem sido frequentemente usada para a tomada de decisões, a vida das pessoas fica cada vez mais vulnerável a tratamentos discriminatórios, como em situações que envolvem análise de probabilidade de cometimento de crimes, tutela da saúde, concessão de crédito e participação em processos seletivos de emprego. (TEFFÉ, 2021, p. 378)

É possível atribuir esse tipo de resultado à natureza da automação, um processo essencialmente estatístico-matemático, no qual são identificados padrões nos dados, permitindo que o modelo os reconheça e os associe às decisões desejáveis. Em essência, é estabelecida uma conexão lógica entre os dados de entrada e as decisões desejáveis para um futuro previsível. A máquina adquire essa capacidade de imputação e, a partir desse ponto, pode operar de forma autônoma quando novos dados são introduzidos. O viés pode estar, portanto, no banco de dados com o qual o modelo trabalha ou na forma como o modelo identifica o que é uma decisão acertada.

Agrava mais esse risco o fato de que mesmo o programador original do modelo pode não ter conhecimento completo sobre como o modelo chegou a determinada combinação, devido à imensa quantidade de cálculos e arranjos testados pela máquina. Essas camadas intermediárias atuam como uma verdadeira "caixa preta", ocultando a maior parte do processo de tomada de decisão automática (REIS, 2021, p. 108). Tal opacidade, que torna o modelo altamente robusto para obter as respostas desejadas, também dificulta a compreensão do processo de tomada de decisão.

Isso é ainda mais profundo em problemas de maior complexidade, porque

[36] Disponível em: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-re cruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>/ Acesso em: 14 nov. 23

o modelo é capaz de criar um maior número de camadas ocultas, com suas respectivas combinações e pesos, a fim de aumentar a precisão. No entanto, a cada camada adicionada, se torna mais difícil compreender os critérios de cálculo, resultando em uma "caixa-preta" mais densa. Por isso, “embora possam dar resposta correta para um problema, atualmente não sabemos como as redes neurais chegam a ela” (SEJNOWSKI, p. 134).

De mais a mais, se não é possível entender como o modelo chegou a um determinado resultado, também não é possível entender como ele atuará no futuro e, obviamente, não é possível alimentá-lo com dados futuros, para ajustar mecanismos que possam apresentar resultados inesperados. Essa é outra grande limitação das soluções de *machine learning* (HILDEBRANDT, 2019).

Em um contexto em que a precisão das decisões tomadas com base em tratamento automatizado de dados pessoais está intimamente relacionada à base de dados e às relações traçadas entre esses dados, desponta um outro problema em potencial à privacidade dos titulares: a perfilização. Uma vez que tais informações são necessárias à tomada de qualquer tipo de decisão, a construção de perfis individuais aparece sempre associada a todo tipo de julgamento feito por máquina (REIS, 2021).

É dizer, “os dados pessoais estabelecem perfis e, a partir deles, é possível criar seleções e códigos que vão influenciar a escolha da sociedade em qualquer área, surgindo daí inúmeras possibilidades” (GUNTHER, 2022, p. 145). Além disso, a caracterização da Inteligência Artificial se baseia fundamentalmente na capacidade de aprendizado, geralmente através da construção de perfis taxonômicos (SARLET, 2022).

Danilo Doneda também trata sobre o *profiling*, que envolve a criação de perfis de comportamento individual ou de um grupo de pessoas, com base em informações pessoais fornecidas voluntariamente ou coletadas (DONEDA, 2006, p. 173).

Outro que trata do tema é Roger Clarke, que afirma:

> [*profiling* é] uma técnica em que um conjunto de características de uma determinada classe de pessoa é inferido a partir de experiências passadas e, em seguida, dados armazenados são pesquisados para indivíduos com um ajuste quase perfeito a esse conjunto de características. (CLARKE, 1993, p. 173)

Embora essa prática exista há algumas décadas, a forma como a capacidade computacional foi expandida recentemente permite uma utilização muito mais ampla de informações pessoais para a construção de perfis.

Os riscos oferecidos por essa técnica já foram anunciados pelo Tribunal Federal Alemão, afirmou que a elaboração de um perfil completo da personalidade por meio de “sistemas automatizados integrados sem que o interessado pudesse controlar de forma suficiente sua correção e utilização” (BVerfGE 65, 1983, p. 5).

Frente a essa conjuntura, a quantidade massiva de informações coletadas concomitantemente, relacionadas a diversos aspectos da vida cotidiana, dificulta o controle desses dados, mesmo por parte de atores que dispõem de grande arsenal técnico, como governos e grandes companhias. Essas informações vão se agrupando em grandes conglomerados, se unindo, separando e remodelando, como uma espécie de organismo vivo em constante adaptação (HILDEBRANDT, 2019).

Diante desse contexto, muitas questões são levantadas acerca dos riscos trazidos pelo avanço tecnológico desmedido e seus impactos na sociedade. Essa preocupação tem sido especialmente significativa diante da automatização do processo de tomada de decisões com base em soluções de inteligência artificial.

Em razão disso, em 2019, o High-Level Expert Group on AI apresentou o guia denominado “Ethics Guidelines for Trustworthy Artificial Intelligence”, estabelecendo que “a inteligência artificial tem de poder ser supervisionada por humanos, tem de ser segura, transparente e não pode discriminar” (COMISSÃO EUROPEIA, 2019).

A respeito do tema, Erik Fontenele Nybo argumenta que é necessário assegurar a supervisão por humanos de algoritmos responsáveis pela tomada de decisões. Segundo o autor:

> Necessário criar métodos e processos de revisão por humanos da tomada de decisões dos algoritmos para evitar erros que podem ser replicados ao longo do tempo ou, até mesmo, atingir uma escala maior. O ponto é que os dados utilizados para ensinar algoritmos representam sempre uma situação do passado. Por isso, é necessário identificar a qualidade dos dados que vão ensinar um algoritmo a tomar decisões. (NYBO, 2019, p. 134)

Por conta dessas preocupações, as legislações que tratam de proteção de dados de todo o globo têm estabelecido salvaguardas aos titulares de dados pessoais, visando evitar que eles sejam prejudicados em função de aspectos

discriminatórios do tratamento automatizado de dados.

A LGPD, por sua vez, segue essa tendência e institui uma série de medidas voltadas ao resguarde dos direitos dos titulares, como será tratado no tópico seguinte.

2.2 Salvaguardas aos titulares de dados pessoais em caso de tratamento automatizado

Em virtude dos riscos inerentes ao processamento automatizado de informações pessoais, a LGPD estabeleceu uma série de medidas com o intuito de prevenir ou mitigar os danos sofridos pelos titulares de dados devido ao uso de suas informações pessoais. Assim, a LGPD não proíbe o tratamento automatizado de dados, mas estabelece uma série de regras e limites para sua utilização, visando proteger os dados, preservar a privacidade dos titulares e proporcionar um ambiente propício ao aproveitamento das vantagens oferecidas por essa modalidade de tratamento de dados.

É indubitável que o tratamento automatizado de dados pessoais está se tornando cada vez mais comum e importante na era digital. No entanto, é crucial que essa tecnologia seja utilizada de forma responsável, respeitando a privacidade e os direitos dos titulares dos dados. As regras e os limites estabelecidos pela LGPD para o tratamento automatizado de dados pessoais têm como objetivo garantir a proteção desses dados e a preservação da privacidade dos titulares. Portanto, é fundamental que as organizações se adequem aos requisitos da lei, não apenas para evitar sanções, mas também para manter a confiança dos titulares e permitir a contínua expansão tecnológica associada aos processos que envolvem o tratamento de dados.

Nesse contexto, o artigo 18 da LGPD[37] traz um conjunto de direitos dos

[37] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

titulares, aplicáveis aos dados submetidos a qualquer forma de tratamento, seja ele realizado com o auxílio de máquinas ou não. No entanto, alguns aspectos dessas garantias se mostram especialmente relevantes para essa modalidade de tratamento de dados.

Esse dispositivo confere ao titular, por exemplo, o direito de confirmar se uma organização está realizando o tratamento de seus dados pessoais e o direito de solicitar acesso a esses dados. Em outras palavras, o titular tem a possibilidade de obter uma cópia das informações pessoais que a organização possui em seus arquivos.

Essa garantia é particularmente importante quando se fala em tratamento automatizado de dados, uma vez que é comum que o titular tenha dúvidas sobre o uso de dados obtidos no ambiente virtual, posto que sua captação acontece de forma muito mais simples e, por vezes, sua autorização demanda muito pouco esforço do titular, que precisa apenas assinalar uma caixa de diálogo em uma página da *web* antes de acessar o conteúdo no qual realmente possui interesse. Dados de navegação são um exemplo de informação cuja coleta no ambiente virtual é muito facilitada e acerca dos quais os usuários costumam ter pouco ou nenhum grau de conhecimento.

Outro direito do titular de dados é o de solicitar a correção de dados pessoais que estejam incompletos, inexatos ou desatualizados. Por exemplo, se houver uma mudança de endereço, número de telefone ou estado civil, o titular pode requerer a atualização dessas informações. Além disso, o titular tem o direito de solicitar a anonimização, bloqueio ou exclusão de dados quando eles forem considerados "desnecessários, excessivos ou tratados em desconformidade" com a LGPD (art. 18, IV).

A LGPD também prevê o direito à portabilidade dos dados, ou seja, a transferência das informações pessoais do titular para outro fornecedor de serviço ou produto. Esse direito visa garantir que o titular tenha o poder de decisão sobre o que será feito com suas informações, evitando uma situação denominada *"vendor lock-in"*, na qual o usuário fica preso a um fornecedor de serviço devido ao custo excessivo de mudança (MALDONADO, 2019).

Novamente, trata-se de uma garantia que, embora aplicável a todas as

---

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

formas de tratamento de dados pessoais, assume papel crucial no caso do tratamento automatizado. Isso ocorre porque o uso de informações pessoais dos usuários no ambiente virtual possibilita a oferta de serviços personalizados. Dessa forma, o direito à portabilidade oferece aos usuários a oportunidade de escolher entre diferentes fornecedores de serviços sem comprometer a qualidade dos serviços obtidos devido à concentração excessiva de informações em um único prestador do qual desejam se desvincular.

Outra prerrogativa assegurada pela LGPD é o direito do titular de saber exatamente com quem o controlador dos dados está compartilhando suas informações. Isso inclui tanto entidades públicas quanto privadas, que devem ser nomeadas explicitamente, e não apenas mencionadas de forma genérica. Essa prerrogativa também representa uma proteção especialmente importante para os titulares cujas informações são tratadas de maneira automatizada, uma vez que o ambiente virtual gera muitas incertezas sobre quais agentes têm acesso aos dados pessoais e como eles recebem essas informações.

É muito comum, por exemplo, que um usuário, ao acessar uma página da *web* pela primeira vez, se depare com uma série de instruções personalizadas – até mesmo formulários pré-preenchidos. Isso pode ser consequência das opções de navegação do usuário, mas também pode acontecer em função do compartilhamento de suas informações pessoais pelos agentes envolvidos no tratamento desses dados.

Além dessas, também existem prerrogativas relacionadas ao consentimento, quando essa é a base legal para o tratamento de dados. Entre elas, destaca-se o direito à informação sobre a possibilidade de não fornecer consentimento. A premissa do consentimento é que ele seja solicitado e concedido de maneira clara, transparente e totalmente livre. Para garantir isso, o titular de dados tem o direito de ser informado sobre a opção de não fornecer o consentimento e quais serão as consequências caso essa opção seja negada.

Por exemplo, um usuário pode ser convidado a consentir ou não com o uso de *cookies* em um site. Se não consentir, pode ser informado de que isso afetará sua experiência de navegação ou impedirá o acesso a determinadas ferramentas.

O titular também tem o direito de revogar o consentimento e solicitar a

exclusão dos dados coletados com base nesse consentimento. No entanto, existem situações em que esse direito não pode ser exercido, mormente quando a organização precisa manter os dados para cumprir uma obrigação legal ou regulatória.

Essas prerrogativas, como mencionado anteriormente, são aplicáveis a todas as formas de tratamento de dados pessoais, embora tenham aspectos diretamente relacionados ao tratamento automatizado de dados. No entanto, como essa modalidade de tratamento apresenta riscos específicos, a lei também estabelece mecanismos que se aplicam especificamente a esse cenário.

Nesse sentido, a LGPD estabelece que a ANPD tem o papel de fiscalizar e orientar as empresas e instituições que realizam o tratamento automatizado de dados, garantindo assim a conformidade com as normas estabelecidas na lei. A atuação da ANPD desempenha um papel crucial na regulamentação do tratamento automatizado de dados e na proteção dos direitos dos titulares de informações pessoais no Brasil.

Além disso, em consonância com o princípio da transparência, a LGPD estipula que o titular dos dados deve ser informado de maneira clara e acessível sobre a utilização do tratamento automatizado, incluindo a existência de decisões automatizadas e a possibilidade de revisão das decisões tomadas com base nesse tipo de tratamento.

A possibilidade de revisão das decisões decorre do disposto no art. 20 da LGPD[38], responsável por conferir ao titular dos dados o direito de solicitar a revisão de decisões tomadas por meio do tratamento automatizado de dados pessoais que afetem seus interesses. Essa questão é destacada por Caitlin Mulholland ao ressaltar a importância do direito à explicação, especialmente quando se trata de direitos considerados essenciais. Segundo ela:

> Em casos envolvendo decisões automatizadas que concedem ou negam

[38] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

> determinados bens jurídicos, é essencial avaliar a natureza desses bens. Quando esses bens estão relacionados a funções sociais constitucionalmente asseguradas, como a concessão de financiamento de crédito estudantil ou a obtenção de crédito para aquisição de moradia, concretizando direitos essenciais, a compreensão e o exercício do direito à explicação são de extrema importância. (MULHOLLAND, 2020)

No entanto, a mesma autora ressalta que o direito à revisão não se confunde com o direito de forçar o controlador a alterar o resultado do tratamento automatizado. Caso contrário, a utilização de métodos automatizados de tratamento perderia sua finalidade (MULHOLLAND, 2020).

De acordo com Souza, Perrone e Magrani, o direito à revisão estabelecido pela LGPD aproxima-se dos sistemas de proteção de dados implementados no Reino Unido e na Irlanda. Eles afirmam:

> É importante frisar que a regulamentação brasileira estabeleceu que o direito garantido é o da revisão. Isso parece aproximar o país dos sistemas implementados no Reino Unido e na Irlanda, que, como vimos, definiram o direito de contestação como o direito de solicitar uma reconsideração ou apelação, respectivamente. (MAGRAN et al., 2021, p. 277)

É válido observar que o § 3º do art. 20, que previa a possibilidade de revisão por pessoa natural, foi vetado pelo Poder Público. Nas razões do veto[39], consta que essa proposta:

> [...] ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas.

É importante destacar que a revisão de decisões tomadas unicamente com base em tratamento automatizado, mesmo quando realizada por um ser humano, não implica necessariamente a eliminação de aspectos discriminatórios. Pelo contrário, pode resultar na introdução de outros aspectos discriminatórios, dependendo das pessoas envolvidas.

Também é necessário mencionar que, para alguns autores, a escolha legislativa revela uma desresponsabilização dos agentes responsáveis pelo tratamento de dados pessoais. Isso ocorre porque o exercício desse direito só pode ocorrer após a tomada de decisão, sem a obrigação de revisão prévia. Nesse

[39] Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm>. Acesso em: 14 nov. 23.

sentido, Marco Almada destaca:

> Outra consequência da escolha do legislador brasileiro por um direito à revisão é que o dispositivo da LGPD estabelece que o direito do titular de dados é uma resposta ao fato que gera a lesão ou ameaça a interesse juridicamente tutelado. Os controladores de sistemas de automação ficam, pois, desobrigados de intervenções ex ante ao longo do ciclo de desenvolvimento, que permitiriam o envolvimento mais direto dos titulares de dados e de suas perspectivas. (ALMADA, 2019, p. 7)

A prerrogativa mais relevante para os propósitos desta pesquisa, contudo, é a da explicação, calcada no princípio da transparência e que impõe aos agentes de tratamento o dever de oferecer informações acerca da maneira como está tratando os dados pessoais.

Um exemplo de materialização desse direito pode ser encontrado no § 1º do art. 20, que garante ao titular de dados pessoais o acesso a informações sobre o tratamento realizado. Essa disposição, inspirada no RGPD, estabelece o direito à explicação em situações de decisões automatizadas como uma medida inicial contra a falta de transparência. No entanto, conciliar esse direito com a proteção dos segredos comerciais e industriais representa um grande desafio prático.

Outro aspecto que merece atenção é a inexistência, na LGPD, de uma conceituação objetiva para o termo "decisão automatizada". Embora o termo seja sugestivo e indique um processo decisório realizado por meio de processos autônomos, uma caracterização precisa se mostra importante para reduzir a incerteza sobre os casos em que é permitido ao titular exercer as prerrogativas estabelecidas no § 1º do art. 20.

Por exemplo, pode-se questionar qual nível de intervenção humana é suficiente para descaracterizar a automatização. A presença de intervenção humana na coleta dos dados seria suficiente para que a decisão não seja considerada automatizada? Seria o simples exame superficial dos resultados, sem envolvimento nas razões por trás da tomada de decisão, suficiente para impedir o exercício desse direito?

Com o intuito de esclarecer essa dúvida, o Projeto de Lei do Senado nº 4.496/2019, de autoria do senador Styvenson Valentim (Podemos/RN), propõe a inclusão da definição de "decisão automatizada" no rol de conceitos do art. 5º, por meio da inserção do inciso XX, nos seguintes termos:

> XX - decisão automatizada: processo de escolha, classificação, aprovação ou rejeição, atribuição de nota, medida, pontuação ou escore, cálculo de risco ou probabilidade, ou outro processo semelhante, realizado por meio do tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, inteligência artificial, aprendizado de máquina ou outra técnica computacional. (BRASIL, 2019)

Na justificativa da proposta, o parlamentar destaca a necessidade de evitar que a ambiguidade do conceito seja usada para sonegar informações importantes aos titulares de dados pessoais.

Essa medida revela uma preocupação com a concretização do direito à explicação, uma prerrogativa especialmente significativa quando se refere o tratamento automatizado de dados, em que a transparência e a revisão das decisões são fundamentais para garantir a proteção dos direitos dos titulares de informações pessoais e mitigar os possíveis impactos discriminatórios.

O direito à explicação na LGPD, de maneira similar ao RGPD, pode ser fundamentado a partir de três pontos principais: o princípio da transparência, o direito de acesso à informação e como um pressuposto para o exercício dos outros direitos, especialmente o direito de requerer a revisão de decisões automatizadas (SOUZAet al., 2021, p. 273).

Dessa forma, é possível compreender esse tipo de meta-direito como uma forma de concretizar o princípio da transparência e o direito à informação, fornecendo uma base para o exercício de outros direitos relacionados à proteção de dados.

No entanto, é crucial compreender o que caracteriza uma explicação, levando em consideração as particularidades, especialmente técnicas, que permeiam os processos de tomada de decisão automatizada. Nesse contexto, a ANPD poderá desempenhar um papel semelhante ao da ICO (Information Commissioner's Office), a autoridade britânica de proteção de dados, que esclareceu que as informações relevantes sobre a lógica e o significado das consequências previstas em um processo devem ser claras, descrevendo aspectos como o tipo de informação coletada ou utilizada na criação do perfil ou na tomada de decisão automatizada; o motivo pelo qual a informação é considerada relevante; e os possíveis impactos sobre o indivíduo[40].

[40] INFORMATION COMMISSIONER'S OFFICE — ICO. [Site institucional]. Disponível em: < https://ico.org.uk/for-the-public/your-rights-relating-to-decisions-being-made-about-you-without-human-involvement/>. Acesso em 14 nov. 23.

Nesse sentido, Doshi-Velez e Kortz (2017) afirmam que uma decisão é explicada quando pode ser interpretada em termos humanos, compreendendo, no mínimo, quais critérios levaram à decisão, como a alteração de algum desses critérios afetaria a decisão e por que casos semelhantes resultaram em decisões diferentes.

É importante ressaltar que a exigência de explicação gera um custo adicional para o uso do modelo, e em contextos de baixo impacto ou escala mínima do modelo, a necessidade de uma explicação desse tipo pode inviabilizar seu uso.

Além disso, é necessário observar que, em muitos casos, atender a todos esses critérios é incompatível com o funcionamento do modelo, devido ao aumento de diversas camadas de processamento. Dependendo da forma como a explicação é solicitada, considerando questões econômicas e estruturais, essa regulamentação pode impor uma determinada arquitetura de modelos. Como explicam Caitilin Mulholland e Isabella Frajhof:

> Em certas circunstâncias, o direito à explicação pode se confundir com o direito ao design adequado. Quando a explicação buscada não é apenas para um caso específico, mas sim para o funcionamento geral do modelo, é mais apropriado falar em deciframento do próprio design, e não da explicação de uma decisão. (MULHOLLAND et al., 2020, p. 281).

No entanto, esse direito está sujeito à salvaguarda do segredo de negócio, conforme a ressalva mencionada no § 1º. Essa exceção levanta uma série de questões, incluindo a preocupação de como garantir a inexistência de aspectos discriminatórios no tratamento automatizado de dados. Para abordar essa questão, o § 2º do mesmo dispositivo prevê que "em caso de não fornecimento das informações mencionadas no § 1º deste artigo com base na observância do segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificar aspectos discriminatórios no tratamento automatizado de dados pessoais".

Portanto, a ANPD tem a prerrogativa de realizar auditorias para identificar aspectos discriminatórios no tratamento automatizado de dados quando o controlador se recusar a fornecer informações claras sobre os critérios utilizados no tratamento dos dados pessoais. No entanto, Caitlin Mulholland enfatiza que "a discricionariedade da autoridade nacional para realizar a auditoria ocorre apenas quando o controlador se recusa a fornecer as informações elencadas no parágrafo primeiro" (MULHOLLAND, 2020, p. 272).

Diante disso, percebe-se que a previsão de auditoria para verificar aspectos discriminatórios no tratamento de dados pessoais pode incentivar as empresas a fornecerem, desde o início, informações claras e precisas sobre o tratamento dos dados sob sua custódia, a fim de evitar auditorias por parte da ANPD, funcionando como uma espécie de prevenção.

No entanto, caso a companhia opte por não fornecer detalhes sobre o tratamento de dados, a lei não estabelece parâmetros para a realização dessa auditoria, o que levanta várias dúvidas, especialmente em relação aos métodos que devem ser utilizados para sua realização.

Métodos mais aprofundados tendem a comprometer os segredos comerciais do detentor do modelo, ou, no mínimo, agravar o risco de comprometimento. Por outro lado, é necessário que as soluções sejam adequadas para garantir a qualidade das informações transmitidas ao titular e a confiabilidade dos resultados, a fim de evitar a continuidade do uso de modelos que apresentem aspectos discriminatórios.

A discussão do próximo capítulo, então, será acerca dos métodos que podem ser utilizados, com enfoque no método contrafactual, e quais os impactos da escolha de uma metodologia, tanto na proteção ao segredo de comércio quanto na salvaguarda aos direitos do titular de dados pessoais.

3. AUDITORIA PARA AVERIGUAÇÃO DE ASPECTOS DISCRIMINATÓRIOS NO TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS: A SUFICIÊNCIA DA ANÁLISE CONTRAFACTUAL EM CASOS DE TUTELA DO SEGREDO DE NEGÓCIO

Como dito nos capítulos anteriores, a preocupação com a proteção de dados pessoais tem crescido em função do advento de novas tecnologias, que permitem a realização de operações maiores e mais complexas. Essas possibilidades expandidas, contudo, carregam consigo importantes questões legais e éticas sobre privacidade e direitos dos titulares de dados.

Neste capítulo, o foco da pesquisa será aprofundar o entendimento sobre a auditoria prevista no art. 20, § 2º, da LGPD. Para tanto, será explorado, inicialmente, o conceito de interpretabilidade aplicado aos modelos que trabalham com tratamento automatizado de dados e, posteriormente, pormenores de uma metodologia contrafactual, que busca averiguar como o modelo se comportaria se lhe fossem fornecidos dados diferentes. As implicações dessas práticas de auditoria não são apenas técnicas, mas precisam assegurar o equilíbrio entre a necessidade de transparência, a proteção de dados e a proteção dos segredos de negócio.

Entender a dinâmica e os desafios da auditoria prevista no art. 20, § 2º, é fundamental para avaliar a eficácia dos mecanismos contidos na LGPD. Além disso, a discussão permite analisar possíveis conflitos entre a transparência requerida pela auditoria e a necessidade de proteger segredos de negócios, um aspecto crítico para as empresas que utilizam esses modelos de tratamento de dados.

Este capítulo, portanto, se desdobrará em várias seções. Inicialmente, serão abordados aspectos importantes da auditoria, passando por quando ela pode ser realizada e quais suas finalidades; em seguida, será feita uma análise sobre quem poderá conduzir a auditoria, tratando sobre a instituição da autoridade reguladora de proteção de dados no Brasil; e, por derradeiro, serão avaliados aspectos críticos da interpretabilidade de modelos, para aferir se é possível realizar a auditoria por meio de análise contrafactual.

3.1 Aspectos relevantes da auditoria para averiguação de aspectos discriminatórios

Uma auditoria consiste em uma avaliação sistemática e independente

realizada para verificar a veracidade de informações e processos dentro de uma organização.

Tratando especificamente da auditoria prevista no art. 20, § 2º, da LGPD, seu objetivo é averiguar se existem aspectos discriminatórios no tratamento de dados pessoais realizado de maneira automatizada. Isto é, averiguar se os resultados do tratamento são diferentes em função de características que não se relacionam com os objetivos do tratamento.

Partindo dessa premissa, uma auditoria eficaz pode ajudar a prevenir violações às prerrogativas dos titulares de dados, melhorar a confiabilidade dos sistemas de processamento de dados e aumentar a confiança do público nas organizações.

No entanto, essa auditoria não é isenta de desafios e é preciso, inicialmente, compreender em que hipóteses ela poderá ser realizada. Isso porque o processo envolve uma série de custos e deve haver alguma razão para acreditar que um erro ocorreu (ou ocorrerá) no processo de tomada de decisão. Analisando por essa perspectiva, só é possível exigir explicações quando algum elemento do processo de tomada de decisão conflita com a expectativa de como a decisão será ou deveria ser feita (DOSHI-VELEZ, 2017).

A LGPD, por meio do art. 20[41], estabelece a possibilidade de auditoria nos casos de não oferecimento de informações a respeito dos critérios e do procedimento utilizados para a tomada de decisão automatizada com base na observância dos segredos de negócios.

A partir da leitura desse dispositivo, então, poder-se-ia compreender que a auditoria só pode acontecer nos casos em que o agente envolvido no tratamento se recusa a informar o titular a respeito dos parâmetros usados para a tomada automatizada de decisão.

Por outro lado, o § 1º do art. 20 indica a necessidade de fornecimento de

[41] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

informações “claras e precisas”. Sendo assim, a lei abre espaço para uma análise quanto à qualidade das informações cedidas aos titulares. Afinal, é possível que o agente envolvido no tratamento e o titular não concordem quanto à suficiência dos esclarecimentos prestados.

Nos casos em que não houver consenso quanto à qualidade das informações prestadas aos titulares, a lei não determina com precisão qual será a solução para o melindre, tampouco se o fornecimento de informações consideradas insuficientes pode ensejar a realização de auditoria e qual o procedimento a ser adotado em tais casos.

Contudo, o art. 55-J da LGPD atribui diversas incumbências à ANPD, dentre elas a de realizar ou determinar a realização de auditorias sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento (inciso XVI[42]). Em função dessa prerrogativa, existe um elastecimento das possibilidades de realização de auditoria e, por conseguinte, há alicerce legal para a realização de investigação, a critério da ANPD, nos casos em que as informações prestadas forem consideradas insuficientes.

Porém, o foco do presente estudo reside na hipótese em que o controlador se recuse a fornecer informações com base na observância de segredos de negócio. Em tais hipóteses, o § 2º do art. 20 é categórico ao instituir a possibilidade de auditoria.

Vale dizer, a escolha dos agentes de tratamento de dados, por fornecer as informações ou se submeterem à auditoria prevista no art. 20, será diretamente influenciada pela maneira como a auditoria será conduzida. Uma auditoria mais rígida e invasiva pode demover agentes da ideia de não fornecer informações claras e precisas; por outro lado, uma auditoria mais branda pode estimulá-los a optar por essa solução.

3.1.1 Quem realizará a auditoria

À medida em que há o aprofundamento quanto aos pormenores técnicos das auditorias, é fundamental esclarecer o papel crucial da entidade que será

[42] Art. 55-J. Compete à ANPD: [...] XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

responsável por operacionalizá-las: a ANPD.

Constituída como o órgão centralizador, regulador e supervisor do cumprimento das normas de proteção de dados pessoais no Brasil, a ANPD é o ponto de convergência onde os princípios fundamentais de privacidade se encontram com a prática cotidiana de coleta, processamento e armazenamento de dados. Neste tópico, serão investigadas de maneira mais detalhada as competências dessa autoridade, sua estrutura operacional e as responsabilidades decorrentes de sua função, permitindo assim uma melhor compreensão da sua relevância no contexto da auditoria prevista pelo art. 20, § 2º, da LGPD.

Para melhor compreender a função e estrutura da ANPD, cabe apontar que, quando promulgada, a LGPD sofreu diversas modificações em relação ao texto originalmente aprovado pelo Congresso Nacional, resultantes de vetos presidenciais. Um dos mais significativos envolvia justamente a proposta de estabelecer a ANPD como parte da Administração Pública Indireta, sujeita a regime autárquico especial e vinculada ao Ministério da Justiça.

A especificidade dada à organização pelo dispositivo vetado se caracterizava pela independência administrativa, não-submissão a uma hierarquia, mandato fixo de seus líderes e autonomia financeira. Michel Temer, então Presidente da República, justificou o veto argumentando que “as disposições contrariam a constitucionalidade do processo legislativo, por violar o artigo 61, § 1º, II, ‘e’[43], juntamente com o artigo 37, XIX[44], da Constituição” (BRASIL, 2018).

A base para o veto, portanto, estava em um possível defeito de competência na criação da ANPD, pois, de acordo com os citados dispositivos constitucionais, somente o Presidente da República pode propor um projeto de lei que disponha sobre criação de cargos, funções ou empregos públicos na administração direta e autárquica.

---

[43] Art. 61. A iniciativa das leis complementares e ordinárias cabe a qualquer membro ou Comissão da Câmara dos Deputados, do Senado Federal ou do Congresso Nacional, ao Presidente da República, ao Supremo Tribunal Federal, aos Tribunais Superiores, ao Procurador-Geral da República e aos cidadãos, na forma e nos casos previstos nesta Constituição. § 1º São de iniciativa privativa do Presidente da República as leis que: [...] e) criação e extinção de Ministérios e órgãos da administração pública, observado o disposto no art. 84, VI;

[44] Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: [...] XIX - somente por lei específica poderá ser criada autarquia e autorizada a instituição de empresa pública, de sociedade de economia mista e de fundação, cabendo à lei complementar, neste último caso, definir as áreas de sua atuação;

Posteriormente, o então Presidente da República editou a Medida Provisória n. 869, em 27 de dezembro de 2018 (BRASIL, 2018), modificando a Lei n. 13.709/2018, e adicionando o art. 55-A, o qual instituiu, sem aumento de despesa, a ANPD. O texto inicial da medida provisória previa a instituição da autoridade nacional como órgão da Administração Pública Federal, incluída na Presidência da República e integrante da Administração Pública Direta, logo, sem autonomia e independência administrativa, econômica e financeira.

Durante o processo legislativo, a Medida Provisória n. 869/2018 recebeu 176 emendas ao seu texto original, sendo alterada pelos parlamentares e aprovada como o Projeto de Lei de Conversão n. 7/2019, resultando na Lei n. 13.853/2019, sancionada em 8 de julho de 2019 (BRASIL, 2019).

A redação, que modifica a LGPD, estabeleceu a autoridade nacional como órgão da Administração Pública Direta, mas concedeu ao Presidente da República o direito de decidir, após dois anos da vigência da LGPD, sobre a possível transformação da ANPD em órgão da Administração Pública Indireta.

A constituição da ANPD como entidade sem independência impactaria diretamente a eficácia de todo o aparato normativo da LGPD. Isso é confirmado pelo parecer do Ministério Público Federal, através de Nota Técnica, emitido antes do veto presidencial ao texto original da LGPD. *In verbis*:

> É essencial a criação de uma autoridade nacional de proteção de dados, com autonomia para assegurar a legítima proteção aos titulares dos dados sujeitos a tratamento. Não é adequado repetir o erro do Marco Civil da Internet (Lei n° 12.965), que não estabeleceu o órgão responsável pela proteção dos direitos dos usuários de internet, embora tenha diversas disposições sobre proteção de dados, inclusive um regime sancionatório.
>
> [...]
>
> Além da existência autônoma, é imprescindível que essa autoridade de proteção de dados possa responder às demandas dos cidadãos, fornecendo-lhes meios para conhecer onde estão guardadas suas informações pessoais e com autoridade para exigir cumprimento da norma geral e de aplicar sanções nos ilícitos relativos a sua zona de atribuição. É essencial, ademais, que emita relatórios anuais sobre sua atuação e a situação da proteção de dados nos país e que tenha possibilidade de editar atos infralegais e realizar outras ações que atendam o atingimento dos seus objetivos de existência.

> [...]
>
> Esta estrutura estatal, com as atribuições descritas, confere ao cidadão os meios para conhecer com facilidade os bancos de dados onde suas informações estejam arquivadas e apresentar demandas para sua supressão ou correção. Ao contrário, a ausência de órgão estatal protetor com essas características torna na prática impossível saber onde estão dados pessoais de cada cidadão e, na hipótese desse conhecimento, implicam em aumentar os ônus para a eventual regularização da situação (MINISTÉRIO PÚBLICO FEDERAL, 2018, p. 7-10).

Então, por meio da Medida Provisória n. 1.124/2022, posteriormente convertida na Lei n. 14.460/2022 (BRASIL, 2022), o presidente à época, Jair Messias Bolsonaro, transformou a ANPD em autarquia de regime especial, parte da Administração Pública Indireta. Com isso, foi concluído o processo de conversão iniciado pelo governo anterior e a autoridade passou a contar com mais autonomia.

Internamente, a ANPD é organizada pelo seu Regimento Interno, estabelecido pela Portaria n. 1, de 8 de março de 2021 (ANPD, 2021). Para os fins desta pesquisa, é necessário ressaltar que o regimento instituiu, por meio do seu art. 17, a Coordenação-Geral de Fiscalização, cujas atribuições incluem a realização ou determinação de realização de auditorias no âmbito das ações fiscalizatórias e especificamente no caso do art. 20 (inciso IV[45]).

Além disso, há a Coordenação-Geral de Tecnologia e Pesquisa, instituída por meio do art. 18 do regimento interno, que, dentre suas atribuições, tem a de auxiliar tecnicamente a coordenação-geral de fiscalização em auditorias e ações de fiscalização (inciso IX[46]).

Esses dois setores são de suma importância porque é crucial que a auditoria seja conduzida por uma equipe multidisciplinar, que reúna competências tanto em aspectos técnicos quanto jurídicos.

Os aspectos técnicos são necessários para compreender o funcionamento intrincado dos modelos que coletam, processam e analisam os

---

[45] Art. 17. São competências da Coordenação-Geral de Fiscalização, sem prejuízo de outras previstas na Lei nº 13.709, de 2018, no Decreto nº 10.474, de 2020, e na legislação aplicável: [...] IV - realizar auditorias, ou determinar sua realização, no âmbito das ações de fiscalização, assim como para a verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, na hipótese de não atendimento ao disposto no § 1º do art. 20 da Lei nº 13.709, de 2018;

[46] Art. 18. São competências da Coordenação-Geral de Tecnologia e Pesquisa, sem prejuízo de outras previstas na Lei nº 13.709, de 2018, no Decreto nº 10.474, de 2020, e na legislação aplicável: [...] IX - auxiliar tecnicamente a Coordenação-Geral de Fiscalização na análise de relatórios de impacto de proteção de dados pessoais, bem como em auditorias e ações de fiscalização;

dados, pois é nesse âmbito que a discriminação pode ser inadvertidamente incorporada ou perpetuada. Profissionais com formação em ciência da computação, estatística, análise de dados e campos relacionados podem fornecer a expertise necessária para desvendar o complexo funcionamento dos modelos de aprendizado de máquina.

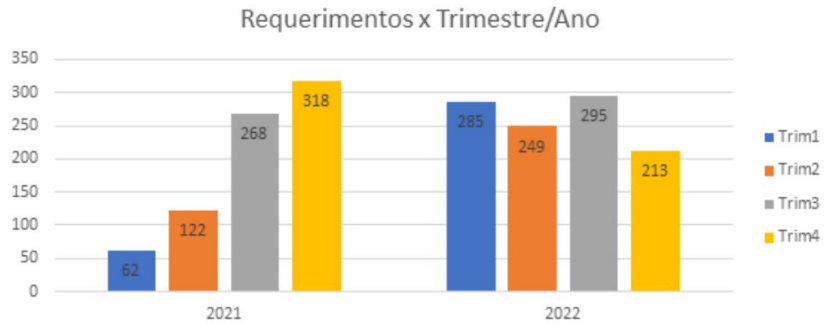
No entanto, a auditoria não se limita apenas a entender como os dados são tratados. É igualmente importante determinar se esse tratamento gera resultados discriminatórios. Isso exige conhecimento jurídico especializado em direito de privacidade e proteção de dados. Assim, juristas especialistas em direito de dados são componentes fundamentais de uma equipe de auditoria, capazes de avaliar se o uso dos dados está em conformidade com a LGPD e outras regulamentações relevantes.

Portanto, uma equipe multidisciplinar é essencial para garantir uma avaliação abrangente e eficaz, abordando tanto o como (aspectos técnicos) quanto o porquê (aspectos jurídicos) do tratamento automatizado de dados.

Até o momento, a ANPD não reportou oficialmente a realização de nenhuma auditoria com base na negativa do controlador em oferecer informações com o fito de proteger segredo de negócios. Em verdade, os números relacionados ao número de requerimentos feitos por titulares de dados são bastante tímidos.

Para os anos de 2021 e 2022, a ANPD reportou um total de 740 e 1042 requerimentos, respectivamente. É possível observar, no gráfico elaborado pela autoridade, que, enquanto no primeiro ano o número de requerimentos cresceu de maneira constante ao longo dos trimestres, no segundo ano ele variou menos. Com efeito:

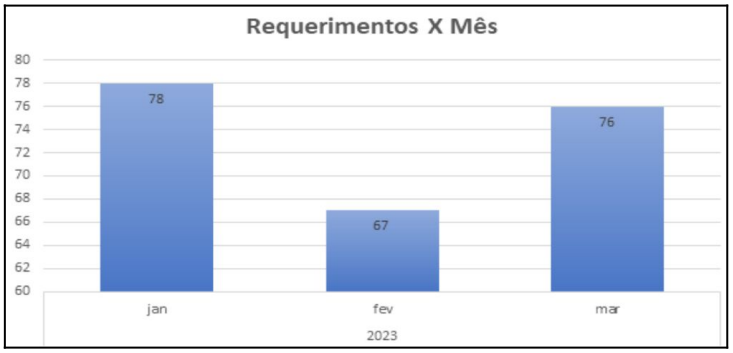
Figura 1 - Requerimentos feitos à ANDP em 2021 e 2022



Fonte: ANPD (2023) [47]

Neste ano (2023), os dados revelam que o número de requerimentos no primeiro trimestre acompanhou a ordem de grandeza averiguada em média no ano de 2022 – 221 e 260,5, respectivamente. Veja-se:

Figura 2 - Requerimentos feitos à ANDP em 2023



Fonte: ANPD (2023)[48]

Ao tratar dos processos de fiscalização, a agência não esclarece se existe algum em curso para a averiguação de aspectos discriminatórios do tratamento, mas indica uma série de processos em curso para a "verificação de conformidade do tratamento de dados pessoais"[49].

Dessa maneira, apesar da novidade da legislação e, por conseguinte, da escassez de dados a respeito de investigações conduzidas pela ANPD – o que se justifica, em parte, pela necessidade de preservação do sigilo dos agentes envolvidos no tratamento –, há fortes indícios de que a auditoria será realizada pela Coordenação-Geral de Fiscalização, com apoio técnico da Coordenação-Geral de Tecnologia e Pesquisa.

3.1.2 Transparência e segredo de negócio

Também é necessário apontar o tênue equilíbrio que deverá haver entre a transparência do processo de auditoria e o respeito aos segredos de negócio

[47] Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao>. Acesso em: 14 nov. 23.
[48] Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao>. Acesso em: 11 ago. 23.
[49] Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao>. Acesso em: 14 nov. 23.

envolvidos. Afinal, ao mesmo tempo em que um dos alicerces da LGPD é a transparência e a informação dos titulares quanto à forma como seus dados são tratados, a lei faz várias menções à proteção do segredo de negócio.

Isso acontece porque, na economia moderna, fortemente calcada em soluções tecnológicas e em maximizar as vantagens competitivas auferidas por quem detém poder informacional, a forma como um agente trata dados pessoais pode ser o alicerce da lucratividade de sua atividade.

Na era digital, os dados pessoais se tornaram insumos valiosos, alimentando uma economia cada vez mais orientada pela informação. No entanto, o processo de coleta e tratamento desses dados é frequentemente caracterizado por uma opacidade preocupante, conforme discutido por Frank Pasquale em seu livro "The Black Box Society" (2015).

Segundo Pasquale, os modelos são os instrumentos por meio dos quais esses dados pessoais são processados, transformando-os em resultados que podem ser utilizados para uma vasta gama de finalidades. Tais modelos, que inicialmente foram concebidos para aperfeiçoar estratégias econômicas existentes, como *marketing* personalizado e perfilização, têm o potencial de remodelar completamente os cenários econômico, político e social.

No entanto, é importante observar que os algoritmos não se limitam ao processamento de dados objetivos e ao fornecimento de resultados claros e quantificáveis. Cada vez mais, os algoritmos são empregados para tomar decisões subjetivas e realizar análises complexas e valorativas. Eles são capazes de avaliar características, personalidade, inclinações e até a orientação sexual de uma pessoa. Além disso, podem identificar estados emocionais, intenções, e até detectar mentiras.

Em cenários profissionais, os algoritmos são usados para avaliar a aptidão das pessoas à determinadas tarefas; quando falamos de segurança pública, eles podem ser usados para analisar a propensão à criminalidade; já no âmbito da saúde, tem o potencial de antecipar sinais de doenças, mesmo antes do surgimento de quaisquer sintomas. Portanto, à medida em que a digitalização do mundo se intensifica, é cada vez mais crucial entender, avaliar e monitorar a transparência e a equidade desses algoritmos.

Essa, porém, é uma tarefa desafiadora, sobretudo quando conjugada ao

dever de resguardar os segredos de negócio dos responsáveis pelo tratamento automatizado de dados, sobretudo porque, muitas vezes, aquilo que se costuma chamar ordinariamente de “caixas-pretas da sociedade da informação” são o próprio segredo de negócio (PASQUALE, 2015).

Existem defensores da ideia de que as organizações deveriam tornar públicos os seus códigos-fonte, a fim de explicitar os critérios usados para alcançar seus resultados. Isso daria à sociedade um meio de verificar ou até mesmo estabelecer limites na implementação de certos desvios. No contexto do direito trabalhista, recentemente, o Tribunal Regional do Trabalho da 1ª Região (TRT1) decidiu manter uma decisão de primeiro grau que permite a realização de perícia nos algoritmos armazenados no código-fonte do aplicativo Uber, a fim de aferir a existência de vínculo de trabalho. Na decisão, o tribunal destaca que, no caso específico, as prerrogativas conferidas pela Lei Trabalhista pesam em favor da manutenção da decisão exarada pelo juiz primevo (BRASIL, 2021).

Essa, porém, é uma posição controversa e a solução para esse dilema não é simples, como confirma uma análise da LGPD: a lei prevê princípios de transparência e responsabilidade, mas, ao mesmo tempo, garante a proteção dos segredos de negócios em vários dispositivos. Esse é um dos mais difíceis e importantes equilíbrios a serem alcançados pela LGPD e a dificuldade para encontrar o equilíbrio é acentuada porque, pela forma como a lei trata do tema, o princípio da transparência é diretamente moldado pela preservação dos segredos de negócio.

De fato, ao mesmo tempo em que a LGPD o define o princípio como uma garantia de informações claras, precisas e facilmente acessíveis sobre o tratamento de dados e seus respectivos agentes, ela menciona a necessidade de proteger os segredos de negócio em diversas ocasiões, inclusive ao tratar das competências da ANPD, deixando claro que as ações da autoridade também devem primar pela observância desses segredos (art. 55-J, II, e § 5º[50]).

De toda forma, a LGPD é adepta da ideia de que decisões automatizadas que afetem terceiros precisam ser explicáveis, de modo que o segredo de negócio

[50] Art. 55-J. Compete à ANPD: [...] II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; [...] § 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei.

não pode ser usado para justificar a falta de explicações.

A fim de alicerçar a reflexão sobre como balancear esses estímulos a princípio contraditórios, é importante considerar a natureza e os limites dos segredos de negócio. Afinal, há várias discussões acerca da função social da propriedade, especialmente da propriedade intelectual, e situações nas quais há forte questionamento sobre a necessidade de flexibilização dos direitos dos detentores de segredos em face dos direitos dos titulares de dados.

No contexto de uma análise sobre os desafios que modelos cujo funcionamento é desconhecido podem representar para a justiça social, vale considerar o seguinte ponto: diversos mecanismos nos sistemas de propriedade intelectual estão estruturados para equilibrar os interesses do detentor com os da sociedade. Isso enfatiza que esses segredos não são direitos absolutos e, em situações nas quais influenciam diretamente a terceiros, é fundamental que exista um nível adequado de transparência (MOORE, 2017).

No caso brasileiro, vale a pena mencionar que a LPI permite a revelação do segredo de negócios em casos excepcionais, no contexto de disputas judiciais, desde que sob segredo de justiça (art. 206[51]).

É necessário, então, estabelecer critérios para a explicação, de maneira que se possa avançar na análise dos métodos de auditoria, avaliando em que medida proporcionam um adequado nível de proteção aos segredos industriais ao mesmo tempo em que asseguram a transparência preconizada pela LGPD.

3.2 Interpretabilidade de modelos

Interpretar as decisões tomadas com base em tratamento automatizado de dados é um desafio complexo, que envolve a compreensão das decisões resultantes de processos intricados, especialmente quando são utilizadas técnicas de aprendizado de máquina e redes neurais. Essa complexidade acrescenta ainda mais dificuldade à manutenção de níveis adequados de transparência em operações que envolvem tratamento automatizado de dados, pois a linguagem matemática utilizada muitas vezes não é compreensível àqueles que não estão familiarizados

[51] Art. 206. Na hipótese de serem reveladas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, sejam segredo de indústria ou de comércio, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades.

com aspectos técnicos.

Em função disso, é comum a percepção de que a imensa complexidade dos modelos os torna tecnicamente inescrutáveis para a sociedade, incluindo a leitura individual de milhões de linhas de código que fazem referência a outros pacotes, módulos e bases de dados.

De fato, em razão do volume de cálculos e da quantidade de dados necessária para a concepção de um modelo de *deep learning*, até mesmo os desenvolvedores enfrentam dificuldades em compreender o processo exato pelo qual o modelo chega a suas predições ou decisões. Essa falta de transparência pode gerar desconfiança e suposições sobre a confiabilidade do modelo, o que pode exigir a intervenção humana para sua implementação prática (REIS, 2021).

Essa conjuntura faz com que seja necessário analisar o conceito interpretabilidade, um termo usado por alguns autores de forma intercambiável com explicabilidade (GILPIN et al., 2019) e que se refere à capacidade de um modelo de tornar compreensíveis para os humanos os fatores que influenciaram seus resultados. Isso não se limita apenas ao funcionamento interno do modelo, mas também pode levar em conta conhecimento prévio sobre o problema em questão (CHAKRABORTY et al., 2017).

Outrossim, à medida em que as soluções usadas para o tratamento de dados pessoais são cada vez mais aplicadas em diferentes campos, a demanda por explicações cresce, fato que tem impulsionado as pesquisas em Inteligência Artificial Explicável (XAI) e interpretabilidade.

Modelos que trabalham com aprendizado de máquina se destacam em relação à dificuldade de interpretar a maneira como alcançaram determinados resultados. Tais soluções, apesar de serem ferramentas eficazes para solucionar uma vasta gama de problemas, ainda carecem de representatividade perfeita do mundo real. Isso pode ser atribuído em grande parte à otimização de funções matemáticas durante o treinamento do modelo, um processo que pode negligenciar aspectos como ética e justiça, os quais não são facilmente quantificados.

A seleção de técnicas de aprendizado de máquina envolve um equilíbrio entre a precisão e a transparência. Modelos mais simples, como regressão linear e árvores de decisão, são considerados "caixa-branca" e são mais fáceis de interpretar.

Em sentido similar, existem algumas técnicas auto-explicativas, sendo aplicáveis principalmente em problemas de visão computacional e processamento de séries temporais longas. Modelos que usam “Attention” contêm um conjunto extra de pesos e neurônios que indicam a influência dos parâmetros de entrada na geração de cada parâmetro de saída (GILPIN et al., 2019).

A interpretabilidade, nesses casos, passa pela maneira como o modelo é estruturado. Isto é, os desenvolvedores inserem mecanismos que assegurem a possibilidade de quantificar os critérios usados pelo modelo para alcançar determinados resultados.

Essas soluções, porém, tem aplicação limitada. Em problemas mais complexos, onde um número maior de parâmetros está envolvido, outros métodos, como *deep learning*, podem ser necessários para alcançar uma alta acurácia, embora sejam considerados "caixa-preta" e não forneçam meios nativos de interpretabilidade (DOSHI-VELEZ et al. 2017).

Para os modelos caixa-preta, existem as chamadas abordagens *post-hoc*, que buscam fornecer meios compreensíveis de explicar as respostas dos modelos. Técnicas notáveis incluem LIME (RIBEIRO et al., 2016), que cria um modelo caixa-branca para facilitar a compreensão, e SHAP (LUNDBERG et al., 2017), que distribui a influência de cada parâmetro de maneira justa, usando a teoria dos jogos cooperativos.

Essas abordagens são importantes pois, conforme Doshi-Velez e Kim (2017) apontam, a interpretabilidade é essencial para a garantia de várias propriedades desejáveis em um projeto de aprendizado de máquina, incluindo justiça, privacidade, robustez, causalidade e confiança. Assim, a interpretabilidade se torna um elemento crucial para assegurar que as decisões do modelo estejam alinhadas com essas considerações abstratas (LIPTON, 2018).

Vários atributos estão associados à interpretabilidade, incluindo explicabilidade e causalidade. A explicabilidade, por exemplo, é o quão completa é uma explicação fornecida, considerando o público-alvo (GILPIN et al., 2019; MURDOCH et al., 2019). A causalidade, por outro lado, descreve a capacidade de identificar relações e interações entre parâmetros (LIPTON, 2018).

A transparência proporcionada pela interpretabilidade é crucial para gerar confiança nos modelos. No entanto, também existem desafios associados a ela,

como garantir a estabilidade, que se refere à robustez das interpretações sobre diferentes padrões de observação (MURDOCH et al., 2019).

Compreender um modelo de aprendizado de máquina normalmente envolve a análise das decisões gerais que o modelo toma com base nas variáveis do conjunto de dados. No entanto, às vezes, pode ser necessário entender os fatores que levaram a uma previsão específica.

Isso leva a uma divisão do escopo da interpretabilidade em global e local. Enquanto a análise local envolve a análise de uma observação específica, a análise global procura entender o comportamento geral do modelo.

A interpretação global é útil quando se busca compreender as relações de dados que influenciam a predição, sendo especialmente relevante em cenários onde é preciso obter informações sobre um problema ou identificar vieses adquiridos pelo modelo durante o treinamento (DOSHI-VELEZ, 2017). A partir de uma análise dessa natureza, seria possível explicar como um modelo toma decisões a partir do estabelecendo de regras seguidas pelo sistema, sem referência a uma decisão específica.

Por outro lado, a interpretação local é fundamental para justificar uma decisão específica do modelo, sendo uma prática comum em ambientes regulamentados. Nesses casos, o interesse gravita em torno das razões ou justificativas para esse resultado particular, em vez de uma descrição do processo de tomada de decisão em geral.

É importante frisar que não existe uma dicotomia absoluta entre as abordagens, porque entender a forma como um modelo opera pode auxiliar a compreender a forma como alcançou um resultado particular. O contrário também é verdade.

Naturalmente, conforme os modelos se tornam mais complexos, é cada vez mais desafiador interpretar o comportamento das soluções. Como resultado dessa crescente dificuldade, surgiu a necessidade de explicar as influências sobre a pontuação de um modelo treinado em vez de interpretá-las. Nesses casos, os métodos explicativos são utilizados após a saída do modelo, adicionando um nível de abstração à estrutura de interpretação. Esses métodos explicativos são categorizados em importância das variáveis, raciocínio baseado em casos e exploração do espaço latente.

A importância das variáveis classifica as variáveis com base em sua relevância para a predição. O raciocínio baseado em casos seleciona exemplos do conjunto de dados para explicar o comportamento do modelo, enquanto a exploração do espaço latente examina o impacto das mudanças nas entradas sobre a pontuação do modelo.

Os métodos explicativos permitem que a explicação seja independente do modelo usado, proporcionando uma representação padronizada da explicação e possibilitando a comparação entre diferentes modelos.

Dessa forma, existe arcabouço técnico para a implementação de soluções sofisticadas quando da realização de auditoria para averiguar a existência de aspectos discriminatórios em tratamento automatizado de dados. Porém, não se pode perder de vista que uma explicação deve fornecer conteúdo útil, que permita compreender o grau em que uma entrada específica foi determinante ou influente no resultado.

Diante disso, se faz necessário o estabelecimento de critérios para determinar o nível de explicabilidade de uma decisão tomada com base em tratamento automatizado de dados, a fim de obter uma métrica objetiva para avaliar o grau de transparência dessas soluções.

Nesse sentido, Doshi-Velez (2017) argumenta que é possível estipular três critérios-chave para aferir o nível de explicabilidade de uma decisão, são eles: quais os principais fatores envolvidos na tomada de decisão; se a alteração de um fator específico poderia ter conduzido a uma mudança na decisão; e se dois casos semelhantes poderiam resultar em decisões diferentes.

O primeiro critério, relacionado aos principais fatores que influenciaram a decisão, comunga da expressão mais comum de explicabilidade de decisões automatizadas. Nesse caso, em relação aos aspectos discriminatórios que a ANPD buscará investigar, o primeiro critério traduz uma noção bastante prática, pois indica que é preciso averiguar se informações pessoais como etnia, gênero e orientação sexual, por exemplo, foram consideradas para a tomada de decisão.

O segundo critério, por sua vez, se conecta com uma necessária comparação de resultados diante da alteração das entradas. Nesse caso, a busca não é por saber se um fator foi considerado, mas se foi determinante.

Por derradeiro, o terceiro critério trata da diferenciação de dois casos

paradigma, para compreender a causa pela qual receberam decisões diferentes. Esse critério resulta na determinação quanto à existência de um aspecto discriminatório relacionado ao tratamento de dados pessoais, a partir da descoberta de que, não fosse um traço característico do indivíduo a quem os dados se referem, os resultados teriam sido diferentes.

Com base nesses critérios, é possível instituir uma metodologia de auditoria capaz de atender satisfatoriamente a demanda da sociedade por transparência, buscando manter também um grau adequado de proteção aos segredos de negócio.

Tratando do âmbito de incidência da LGPD, é preciso atentar ao fato de que métodos muito sofisticados podem comprometer o respeito aos segredos de negócio do agente envolvido no tratamento de dados pessoais, uma vez que os técnicos responsáveis pela auditoria podem compreender melhor o funcionamento dos modelos e, potencialmente, replicá-los posteriormente. Isso levanta preocupações sobre a proteção do segredo de comércio, que é a fonte de ganhos do desenvolvedor do modelo.

É dizer, embora seja possível que o desenvolvedor do modelo compreenda e tenha capacidade para explicar o processo que levou a uma determinada decisão, expor esse caminho poderia comprometer o segredo comercial ou industrial que é a base de seus ganhos com o modelo (REIS, 2021).

Noutro giro, embora a análise da interpretabilidade seja crucial para garantir a precisão das conclusões da auditoria e facilitar a identificação de aspectos discriminatórios, na prática, explicar essas decisões aos titulares dos dados pode ser extremamente difícil, uma vez que eles normalmente não têm conhecimento dos aspectos técnicos do modelo.

Isso revela que a transparência possui diversas facetas que vão além do simples contexto individual, fornecer informações em excesso ou de forma pouco clara pode representar, na verdade, o não fornecimento das informações. Conforme salientado pela legislação, as informações devem ser transparentes e pertinentes, levando em conta o receptor da informação e o critério de compreensibilidade.

A compreensão das decisões algorítmicas e a explicação dos resultados de forma compreensível aos titulares dos dados são aspectos essenciais, porém, a proteção do segredo empresarial e a complexidade técnica envolvida podem

dificultar essa tarefa.

É fundamental encontrar um equilíbrio entre a transparência e a proteção dos segredos de negócio para garantir a confiança e a precisão na utilização dos algoritmos.

Diante dessa conjuntura, uma análise contrafactual mais simples pode representar uma solução adequada, que permita averiguar a existência de aspectos discriminatórios, explicar aos titulares, de jeito compreensível, como foi conduzida a investigação e, ao mesmo tempo, resguardar os segredos de negócio do agente envolvido no tratamento de dados.

3.2.1 Análise contrafactual

Conforme exposto no tópico anterior, a busca por esclarecimentos sobre os critérios aplicados na tomada de decisões automatizadas tem fomentado estudos no campo da inteligência artificial explicável, resultando em avanços significativos na criação de métodos para entender como um modelo chega a um determinado resultado.

Dentre as abordagens em desenvolvimento, o método proposto por Wachter (2018), que recorre a análises contrafactuais, se destaca para os propósitos deste estudo. Trata-se de uma metodologia voltada à busca por esclarecimentos acerca de como as entradas de um modelo necessitariam ser alteradas para gerar resultado específico.

Em suma, uma explicação contrafactual apresenta uma relação causal da seguinte maneira: “se X fosse Y, o resultado seria Z ao invés de W”, sendo X e Y entradas e W e Z resultados hipotéticos do processamento. Desse modo, análises contrafactuais envolvem a criação de uma realidade hipotética que contradiz os fatos observados.

Ao se tratar da tomada de decisões baseada em processamento automatizado de dados, explicações contrafactuais podem ser empregadas para elucidar previsões de casos individuais e, quando observadas sistematicamente, podem apontar a presença de vieses no modelo.

Tais explicações inspecionam o sistema para identificar as correlações entre entrada e saída, bem como para extrair os fatores predominantes da decisão, com a particularidade de avaliar como uma mudança em um fator específico impacta

a decisão. Isso pode ser usado, por exemplo, para avaliar a equidade de uma decisão com base em como cada fator dentro de uma entrada específica influencia a decisão (BRKAN et al., 2020).

Ademais, a adoção de explicações contrafactuais é considerada uma das formas de suprir a demanda por interpretabilidade, culminando no desenvolvimento de diversas estratégias para identificar tais explicações e em uma literatura crítica acerca do uso de abordagens contrafactuais.

Essa tendência deve-se, em parte, à facilidade de implementação do método, que é basicamente uma função de perda (com um ou vários objetivos) otimizável. Alguns detalhes adicionais precisam ser considerados, como restringir os valores das características a intervalos significativos.

Igualmente, a interpretação de explicações contrafactuais é bastante direta. Se os valores das características de uma instância são alterados conforme o contrafactual, a previsão se modifica para a previsão preestabelecida.

Estudos recentes a respeito das análises contrafactuais realçaram a relevância do entendimento causal. Em uma revisão sistemática, Chou et al. (2022) sustentam que o fornecimento de entendimento causal é de extrema importância e, portanto, que "abordagens causais deveriam ser enfatizadas" (CHOU et al., 2022, p. 78).

Contudo, os autores também apontam que "a literatura que estabelece relações causais à inteligência artificial explicável é escassa." (CHOU et al., 2022, p. 66). Uma consequência dessa lacuna é o questionamento acerca do nível de precisão proporcionado por análises contrafactuais em relação às causalidades operadas por um sistema.

Essa restrição implica que, embora as explicações contrafactuais estabeleçam uma relação causal e forneçam uma explicação compreensível aos usuários, elas não indicam como foram estipulados os critérios usados para a tomada de decisão original.

Existe, portanto, um nível reduzido de complexidade envolvido na realização de análises contrafactuais, que resulta, consequentemente, em um grau inferior de precisão e limita a interpretabilidade do modelo em face de uma eventual auditoria.

Tratando concretamente da auditoria prevista no art. 20, § 2º, da LGPD,

voltada à identificação de aspectos discriminatórios, é necessário que a equipe responsável por sua realização tenha acesso a uma interface que permita trabalhar com a inserção de entradas e a observação dos resultados obtidos a partir dessas entradas.

Vale destacar que a auditoria, como mencionado alhures, nos termos da lei, deve ocorrer diante de uma preocupação concreta, de jeito que a análise se inicia a partir da suspeita de que o modelo possui vieses discriminatórios.

Isso permite concluir que o trabalho de elaborar quais hipóteses devem ser testadas por meio da auditoria será simplificado, porquanto realizado a partir de uma situação concreta, que fornecerá informações quanto aos possíveis aspectos discriminatórios sob investigação e, por conseguinte, auxiliar no estabelecimento de parâmetros para a realização da auditoria.

No tocante à auditoria estipulada pelo art. 20, § 2º, da LGPD, cujo foco reside na identificação de aspectos discriminatórios, torna-se essencial, para a realização de uma análise contrafactual, que a equipe incumbida de sua execução tenha acesso a uma interface que habilite a manipulação de entradas de dados e a observação dos resultados gerados a partir dessas entradas.

A auditoria, conforme mencionado anteriormente e de acordo com a lei, é mobilizada por uma preocupação específica, iniciando-se pela suspeita de que o modelo em uso possa conter vieses discriminatórios. Tal circunstância leva à conclusão de que a tarefa de elaborar as hipóteses que serão testadas durante a auditoria será simplificada, pois será realizada com base em uma situação concreta. Essa situação fornecerá dados sobre os possíveis aspectos discriminatórios em análise, auxiliando assim na definição dos parâmetros para a condução da auditoria.

Sob a perspectiva de proteção do segredo de negócio, essa metodologia apresenta vantagens significativas, pois não requer a análise aprofundada de códigos-fonte. Sem esse tipo de análise, o entendimento dos auditores sobre como o modelo foi desenvolvido é consideravelmente limitado, o que dificulta a exposição de informações confidenciais relacionadas ao funcionamento do modelo.

Esse ponto é esclarecido por Christoph Molnar, que enfatiza o quão atraente esse método é para empresas auditadas por terceiros. Segundo ele:

> O método contrafactual não requer acesso aos dados ou ao modelo. Requer apenas acesso à função de previsão do modelo, que também funcionaria por meio de uma API da web, por exemplo. Isso é atrativo para empresas

> que são auditadas por terceiros ou que estão oferecendo explicações aos usuários sem divulgar o modelo ou os dados. Uma empresa tem interesse em proteger modelos e dados, por causa de segredos comerciais ou de proteção de dados. As explicações contrafactuais oferecem um equilíbrio entre explicar as previsões do modelo e proteger os interesses do proprietário do modelo. (MOLNAR, 2023, p. 243, tradução nossa)

Essa seleção criteriosa ajuda a preservar o segredo industrial, pois limita o acesso dos auditores aos códigos do modelo. Contudo, é importante salientar que, para a realização efetiva da auditoria, é imprescindível que a ANDP possua os meios adequados para verificar se o modelo sob investigação é realmente o que efetua as decisões.

Vale enfatizar que este é um dos principais aspectos a serem considerados quando do estabelecimento de uma metodologia de auditoria apropriada, já que a previsão normativa estabelece que o agente envolvido no tratamento, nesse contexto de auditoria, terá demonstrado preocupação em proteger informações confidenciais.

Assim, com uma atenção particular à preservação dos segredos de negócio, uma análise contrafactual se revela adequada, pois requer um nível de acesso mais restrito ao modelo para fornecer resultados satisfatórios.

Outro ponto relevante diz respeito à complexidade das explicações proporcionadas por análises desse tipo, tendo em vista que a LGPD inclui a transparência entre seus princípios. Nesse contexto, vale recordar que as informações fornecidas aos titulares de dados são facilmente acessíveis. Esse conceito é bem ilustrado por Ferrari e Becker, que destacam que o titular, ao questionar uma decisão, não busca entender as tecnicidades envolvidas, mas sim as razões pelas quais a decisão foi tomada:

> "[O titular] não deseja receber códigos-fonte, mas entender os critérios que foram utilizados, pois, para ele, como leigo, é irrelevante o número de linhas de programação utilizadas [...] para o titular dos dados, é fundamental receber informações consistentes e compreensíveis para que ele, querendo, possa contestar a decisão automatizada." (FERRARI et al., 2018).

Dessa forma, no que se refere à transparência e à acessibilidade das conclusões às quais a auditoria possa chegar, o método também se revela adequado.

Além disso, o método contrafactual, ao se alinhar com os critérios

propostos por Doshi-Velez (2017), explicados no tópico anterior, se apresenta como um mecanismo valioso e eficaz. Tais critérios incluem a identificação dos elementos principais que influenciam a tomada de decisão; a avaliação se a modificação de um elemento específico poderia ter resultado em uma decisão diferente; e a análise se duas situações semelhantes poderiam levar a decisões distintas.

O primeiro critério, que envolve a identificação dos elementos fundamentais que influenciaram a decisão, é o mais difícil de verificar ao realizar uma análise contrafactual. Isso acontece porque tal análise não permite estabelecer, de maneira definitiva, a importância de determinadas características na decisão. Contudo, através da criação de diversos cenários hipotéticos, é viável compreender se informações tais como etnia, gênero e orientação sexual, por exemplo, foram consideradas na decisão.

Em contraste, o segundo critério pode ser verificado com mais facilidade em análises contrafactuais. Isso se dá especialmente porque são construídos cenários hipotéticos com o objetivo específico de determinar o quanto a alteração de algumas entradas pode mudar o resultado fornecido pelo modelo. Nesse cenário, se torna possível, por meio da análise contrafactual, entender se um elemento específico teve papel decisivo.

Por fim, o terceiro critério enfoca a diferenciação entre casos diversos, com o intuito de entender por que foram alvo de decisões diferentes. Este critério também pode ser avaliado via análise contrafactual, especialmente quando há suspeita de que um elemento particular esteja exercendo influência significativa nos resultados.

Dessa forma, por meio das análises contrafactuais, e não de códigos intricados e linguagem computacional complexa, é possível fornecer ao titular uma série de observações sobre como a alteração de certas características de um perfil hipotético mudou os resultados do modelo. Assim, fica compreensível se uma ou mais características estão sendo avaliadas negativamente.

Portanto, explicações contrafactuais representam um primeiro passo rumo ao equilíbrio entre transparência, explicabilidade e responsabilidade com outros interesses, a exemplo de uma minimização da carga regulatória sobre os interesses comerciais, a privacidade, além de promover uma aceitação pública da decisão automatizada (WACHTER et al., 2018).

Com base na discussão apresentada, conclui-se que a análise contrafactual se estabelece como uma ferramenta poderosa e eficaz para a auditoria de modelos algorítmicos, conforme previsto no art. 20, § 2º, da LGPD.

Ao oferecer uma abordagem menos complexa em comparação com outros métodos, essa técnica facilita a implementação do processo de auditoria, tornando-o mais acessível e eficiente.

Ademais, a análise contrafactual possibilita a geração de respostas mais objetivas e de fácil compreensão para os titulares dos dados, fornecendo explicações claras sobre a função, o impacto e o valor de diferentes tipos de informações em uma decisão automatizada. Isso proporciona uma maior transparência no processo de tomada de decisão, permitindo que os indivíduos compreendam e, se necessário, contestem as decisões tomadas por algoritmos.

Ainda, é importante destacar que a análise contrafactual se harmoniza com a necessidade de preservar os segredos de negócio, um aspecto crucial em qualquer auditoria. Essa metodologia oferece um balanço adequado entre explicar as predições do modelo e proteger os interesses do proprietário do modelo.

Em conclusão, a análise contrafactual oferece uma via promissora e pragmática para a realização de auditorias em conformidade com a LGPD. Ela proporciona uma compreensão mais profunda das decisões automatizadas, ao mesmo tempo que assegura a transparência e a proteção dos segredos industriais. Portanto, é uma abordagem que merece séria consideração para a adoção em larga escala no contexto da auditoria de proteção de dados.

CONCLUSÃO

A presente pesquisa teve por objetivo discutir a articulação entre os direitos dos titulares de dados pessoais, sobretudo o direito à transparência, e a proteção dos segredos de negócio dos agentes envolvidos no tratamento de dados pessoais. Nesse intuito, foi apresentada a seguinte pergunta de partida: a análise contrafactual pode ser utilizada para fins da auditoria de que trata o art. 20, § 2º, da LGPD, com o fito de esclarecer a existência de aspectos discriminatórios em tratamento automatizado de dados pessoais e, ao mesmo tempo, preservar o segredo de negócio?

A hipótese aventada era no sentido de que a auditoria prevista no art. 20, § 2º da LGPD, poderia ser realizada por meio de análise contrafactual, a qual bastaria para auferir a existência de aspectos discriminatórios no tratamento de dados pessoais e garantir a transparência dos processos automatizados de tomada de decisão com base no processamento de dados, garantindo-se, ao mesmo tempo, a preservação do segredo de negócio.

Assim, a partir da metodologia empregada, chegou-se à conclusão de que, de fato, é viável utilizar a análise contrafactual para a auditoria prevista no art. 20, § 2º, da LGPD, buscando de identificar possíveis aspectos discriminatórios em processos automatizados de tratamento de dados pessoais.

O caminho percorrido para alcançar essa conclusão foi inicialmente traçado por meio de um mergulho nas origens e desenvolvimento das leis de proteção de dados pessoais, com uma atenção especial à legislação brasileira e suas peculiaridades. Ao longo desse mapeamento, uma descoberta emergiu: frequentemente, a proteção de dados pessoais pode encontrar-se em tensão com a necessidade de preservar segredos de negócio, especialmente quando colocados sob o prisma da transparência.

Aprofundando-se nessa discussão, o primeiro capítulo se propôs a estudar o conceito e a trajetória histórica de proteção ao segredo de negócio, culminando em uma análise específica do tratamento dado por nosso ordenamento jurídico.

Essa investigação trouxe à luz o fato de que, apesar de sua relevância, tal instituto ainda é incipientemente desenvolvido no Brasil, um cenário que se torna

mais complexo à luz dos avanços tecnológicos, especialmente com o surgimento e a popularização de soluções em inteligência artificial e aprendizado de máquina.

Tais soluções são reflexo dos anseios pela otimização nas operações de organizações de todos os tamanhos. Na era da informação, decidir com base em dados consolidados e bem analisados se tornou um diferencial competitivo crucial. Nesse contexto, a automação no tratamento de dados pessoais não é mais vista apenas como uma tendência, mas como uma necessidade.

Com vistas a esse cenário, torna-se evidente que o tratamento automatizado de dados ocupa uma posição central no ambiente tecnológico e socioeconômico da atualidade. Dessa maneira, foram analisadas as particularidades dessa modalidade de tratamento de dados.

Inicialmente, foram notados os grandes benefícios trazidos pelo tratamento automatizado de dados, que assegura maior precisão, velocidade e capacidade de processamento em face de métodos analógicos, que dependem fortemente da ação humana. Em suma, tais métodos trazem eficiência ao tratamento de dados pessoais e, por conseguinte, melhores resultados aos agentes envolvidos.

Contudo, a mudança acelerada no paradigma tecnológico traz consigo questões que ultrapassam as barreiras da tecnologia da informação e alcançam o Direito. O avanço tecnológico vertiginoso não apenas molda, mas também questiona e tensiona os limites da ciência jurídica. Dessa forma, foram avaliados também impactos negativos do tratamento automatizado de dados pessoais por um enfoque jurídico.

Dentre os principais riscos associados a essa modalidade de tratamento de dados pessoais, destaca-se a possibilidade de reiteração de padrões discriminatórios e a dificuldade de compreensão dos motivos que deram origem à decisão. Essa dificuldade remete à dualidade encontrada no primeiro capítulo, de equilibrar transparência e proteção aos segredos de negócio.

Uma das materializações da contraposição entre a transparência que a LGPD busca conferir às operações que envolvem tratamento de dados pessoais e a necessidade de proteção dos segredos de negócio é encontrada no art. 20 da lei. Esse dispositivo assegura aos titulares o direito de solicitar a revisão de decisões tomadas apenas com base em tratamento automatizado de dados pessoais e assegura o fornecimento de informações claras a respeito dos critérios e

procedimentos adotados.

Contudo, uma vez que esse grau de abertura poderia promover a divulgação de informações que caracterizam segredo de negócio, a lei assegura ao agente envolvido a oportunidade de negar seu fornecimento. Nesse caso, contudo, a ANPD pode promover auditoria para investigar a existência de aspectos discriminatórios no tratamento de dados.

A lei, todavia, não descreve como essa auditoria deve ser realizada. De maneira que é necessário buscar uma metodologia adequada, tanto ao fornecimento de informações que satisfaçam a demanda por transparência quanto a proteção dos segredos de negócio.

Nesse contexto, a análise contrafactual surge como uma alternativa. Para averiguar a adequação dessa metodologia, foi analisa a estrutura da ANPD e o conceito de interpretabilidade aplicado aos modelos que trabalham com tratamento automatizado de dados, buscando entender quais critérios devem ser adotados para determinar o grau de explicabilidade de uma decisão tomada por um modelo.

Essa análise demonstrou que a ANPD possui, em sua estrutura interna, a Coordenação-Geral de Fiscalização e a Coordenação Geral de Tecnologia e Pesquisa, dois setores que devem trabalhar em conjunto, para que a demanda por multidisciplinariedade averiguada na auditoria seja satisfatoriamente atendida.

O estudo também culminou na adoção de três critérios para investigar o grau de explicabilidade de uma decisão tomada por modelos que usam processamento automatizado de dados. Esses critérios compreendem: os principais fatores envolvidos na tomada de decisão; o impacto que a alteração de um desses fatores teria na decisão; e as possíveis diferenças averiguadas em casos semelhantes.

Então, foram pesquisados detalhes da metodologia contrafactual, que busca entender como o modelo se comportaria se lhe fossem fornecidos dados diferentes. Nessa análise, constatou-se que a metodologia contrafactual preenche os critérios de explicabilidade.

Da mesma maneira, concluiu-se que ela oferece uma abordagem mais simples em comparação com outros métodos e facilita a implementação do processo de auditoria, tornando-o mais acessível e eficiente. Gerando respostas mais objetivas e de fácil compreensão para os titulares dos dados, o que proporciona

maior transparência.

Outrossim, viu-se que a análise contrafactual está em linha com a necessidade de preservação dos segredos de negócio, pois não demanda um acesso amplo ao funcionamento do modelo.

Dessa maneira, em síntese, após uma análise aprofundada e abrangente, este estudo conclui que a análise contrafactual é uma metodologia adequada para a auditoria prevista no art. 20, § 2º, da LGPD, satisfazendo as demandas de transparência e de proteção dos segredos de negócio e sendo condizente com os princípios gerais da legislação brasileira.

REFERÊNCIAS

AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. **Máquinas Preditivas:** a simples economia da inteligência artificial. Rio de Janeiro: Alta Books, 2018.

ALEMANHA. Tribunal Constitucional Federal. BVerfGE 65, 1 (1983).

ALEXY, Robert. **Teoria dos Direitos Fundamentais.** 2. ed. São Paulo: Malheiros, 2011.

ALMADA, Marco. Revisão humana de decisões automatizadas. Pósdebate 2019-USP, São Paulo, p. 1-22, nov. 2019. Disponível em: < https://www.academia.edu/41483884/Revis%C3%A3o_humana_de_decis %C3%B5es_automatizadas>. Acesso em: 14 nov. 23.

ALMEIDA, Daniel Evangelista Vasconcelos. **Shadow profiles e a Privacidade na Internet:** a coleta de dados pessoais de usuários e não usuários das redes sociais. Porto Alegre: Editora Fi, 2019. E-book. Disponível em: <https://www.editorafi.org/541daniel>. Acesso em: 14 nov. 23.

AMERICAN LAW INSTITUTE. **Restatement (Second) of Torts.** Philadelphia: American Law Institute, 1965. Seção 757. Disponível em: <https:// www.lrdc.pitt.edu/ashley/restatem.htm>. Acesso em: 14 nov. 23.

ARAUJO, Thiago Volpi de; D'AVILA, Ana Vitória Germani; DA SILVA, Bruna Fabiane. **LGPD:** Muito Além da Lei. São Leopoldo: Gvtech Soluções em Tecnologia da Informação Ltda., 2021. E-book.

BARBOSA, Denis Borges. **Uma Introdução à Propriedade Intelectual.** 2. Ed. Rio de Janeiro: Lumen Juris, 2010.

BARLOW, John Perry. **Uma Declaração da Independência do Ciberespaço.** Tradução Rafael Augusto Arruda Merlo. Davos: 1996. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/4631592/mod_resource/content/1/John %20Perry%20Barlow%20-%201996%20-%20Uma%20Declara%C3%A7%C3%A3o %20da%20Independ%C3%AAncia%20do%20Ciberespa%C3%A7o.pdf>. Acesso em: 12 ago. 23.

BIONI. Bruno Ricardo. **Proteção de dados pessoais:** A função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019. E-book.

BRASIL, Ministério da Justiça. **A proteção dos dados pessoais nas relações de consumo:** para além da informação creditícia. Escola Nacional de Defesa do Consumidor; coord. Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/Anexos/manual -de-protecao-de-dados-pessoais.pdf>. Acesso em: 14 nov. 23.

_____. ANPD. Presidência da República. Portaria n. 1, de 8 de março de 2021. Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados -

ANPD. Diário Oficial da União, Brasília, DF, p. 3, 9 mar. 2021, Seção 1.

_____. Constituição Federal da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

_____. Decreto n. 24.507, de 29 de junho de 1934. Aprova o regulamento para a concessão de patentes de desenho ou modelo industrial, para o registro do nome comercial e do título de estabelecimentos e para a repressão á concorrência desleal, e dá outras providências. Diário Oficial da União. Rio de Janeiro, RJ, p. 15332. 26 jul. 1934, Seção 1.

_____. Decreto n. 75.572, de 8 de abril de 1975. Promulga a Convenção de Paris para a Proteção da Propriedade Industrial revisão de Estocolmo, 1967. Diário Oficial da União, Brasília, DF, p. 4114, 10 abr. 1975, Seção 1.

_____. Decreto n. 8.771, de 11 de maio de 2016. Regulamenta a Lei n. 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Diário Oficial da União - Edição Extra, Brasília, DF, p. 7, 11 mai. 2016, Seção 1.

_____. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União. Rio de Janeiro, RJ, p. 23911. 31 dez. 1940, Seção 1.

_____. Decreto-Lei n. 7.903, de 27 de agosto de 1945. Código da Propriedade Industrial. Diário Oficial da União. Rio de Janeiro, RJ, p. 15481. 29 set. 1945, Seção 1.

_____. Lei Complementar n. 166, de 8 de abril de 2019. Altera a Lei Complementar n. 105, de 10 de janeiro de 2001, e a Lei n. 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Diário Oficial da União, Brasília, DF, p. 1, 9 abr. 2019, Seção 1.

_____. Lei n. 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União, Brasília, DF, p. 2, 10 jun. 2011, Seção 1.

_____. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, p. 1, 24 abr. 2014, Seção 1.

_____. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, p. 59, 15 ago. 2018, Seção 1.

_____. Lei n. 13.853, de 8 de julho de 2019. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade

Nacional de Proteção de Dados; e dá outras providências. Diário Oficial da União, Brasília, DF, p. 1, 9 jul. 2019, Seção 1.

_____. Lei n. 14.460, de 25 de outubro de 2022Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Diário Oficial da União, Brasília, DF, p. 3, 26 out. 2022, Seção 1.

_____. Lei n. 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Diário Oficial da União - Suplemento, Brasília, DF, p. 1, 12 set. 1990, Seção 1.

_____. Medida Provisória n. 869, de 27 de dezembro de 2018. Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Diário Oficial da União, Brasília, DF, p. 8, 28 dez. 2018, Seção 1.

_____. Presidência da República. Mensagem n 451, de 14 de agosto de 2018. Brasília: Presidência da República, 2018. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em: 14 nov. 23.

_____. Senado Federal. Projeto de Lei n. 4.496, de 2019. Altera a Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), para definir a expressão “decisão automatizada”. Brasília: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/138136>. Acesso em: 14 nov. 23.

_____. Tribunal Regional do Trabalho da 1ª Região. Mandado de Segurança Cível n. 0103519-41.2020.5.01.0000, da Seção Especializada em Dissídios Individuais. Rio de Janeiro, RJ, 22 abr. 2021. Disponível em: <https://www.conjur.com.br/dl/0103519-4120205010000-pericia-algoritmo.pdf>. Acesso em: 14 nov. 23.

BRAYNE, Sarah. **Predic and Surveil:** Data, Discretion, and de Future of Policing. 1 ed. Oxford: Oxford University Press, 2020.

BRKAN, M.; BONNET, G. **Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions:** of Black Boxes, White Boxes and Fata Morganas. European Joumal of Risk Regulation, v. 11, n. 1, 2020. p. 49

CARLOTO, Selma. **Lei Geral de Proteção de Dados:** Enfoque nas relações de trabalho. São Paulo: LTR, 2020.

CARNEIRO, Giovana; MAGRANI; Eduardo; SOUZA, Carlos Affonso. **Lei Geral de Proteção de Dados Pessoais:** uma transformação na tutela dos dados pessoais.

In: MULHOLLAND, Caitlin (org.). A LGPD e o Novo Marco Normativo no Brasil. Porto Alegre: Arquipélago Editorial, 2020. E-book, pp. 77-118.

CASTELLS, Manuel. **Ruptura:** a crise da democracia liberal. Rio de Janeiro: Zahar, 2018.

_____. **A sociedade em rede.** Vol. I. Tradução de Roneide Venâncio Majer. 8 ed. São Paulo: Paz e Terra, 2005.

CHAKRABORTY, Supriyo; TOMSETT, Richard; RAGHAVENDRA, Ramya; HARBORNE, Daniel; ALZANTOT, Moustafa; CERUTTI, Federico; SRIVASTAVA, Mani; PREECE, Alun; JULIER, Simon; RAO, Raghuveer M.; KELLEY, Troy D.; BRAINES, Dave; SENSOY, Murat; WILLIS, Christopher J.; GURRAM, Prudhvi. **Interpretability of deep learning models:** A survey of results. In: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced. Disponível em: < https://ieeexplore.ieee.org/document/8397411/authors#authors>. Acesso em: 14 nov. 23.

CHOU, Yu-Liang; MOREIRA, Catarina; BRUZA, Peter; OUYANG, Chun; JORGE, Joaquim. **Counterfactuals and causability in explainable artifcial intelligence:** Theory, algorithms and applications. 2021. Disponível em: <https://arxiv.org/abs/2103.04244>. Acesso em: 14 nov. 23.

CLARKE, Roger. **Profiling:** A hidden challenge to the regulation of data surveillance. Journal of Law & Information Science, [s. l.], v. 4, p. 403, 1993. Disponível em: <http://classic.austlii.edu.au/au/journals/JlLawInfoSci/1993/26.html>. Acesso em: 14 nov. 23.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Editora Renovar, 2006.

DOSHI-VELEZ, Finale; KIM, Been. **Towards A Rigorous Science of Interpretable Machine Learning.** 2017. Disponível em: <http://arxiv.org/abs/1702.08608>. Acesso em: 14 nov. 23.

_____; KORTZ, Mason; BUDISH, Ryan; BAVITZ, Chris; GERSHMAN, Sam; O'BRIEN, David; SCHIEBER, Stuart; WALDO, James; WEINBERGER, David; WOOD, Alexandra. **Accountability of AI Under the Law:** the role of explanation. Cornell University, nov. 2017. Disponível em: <https://arxiv.org/abs/1711.01134v1>. Acesso em: 14 nov. 23.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 7/2015:** meeting the challenges of Big Data A call for transparency, user control, data protection by design and accountability. União Europeia: EDPS, 2015. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> Acesso: 14 nov. 23.

FEKETE, Elisabeth Edith G. Kasnar. **Deve ser dado tratamento especial às informações confidenciais nos processos licitatórios no direito brasileiro,**

diante da nova Lei de acesso à informação? *In:* FEKETE, Elisabeth Edith G. Kasnar. Estudos de Direito Intelectual em homenagem ao prof. Doutor José de Oliveira Ascenção. 50 anos de vida universitária. Coimbra: Almedina, 2015. p. 191-208.

_____. **O regime jurídico do segredo de indústria e comércio no direito brasileiro.** Rio de Janeiro: Forense 2003.

_____. **Segredo de Empresa.** *In:* CAMPILONGO, Celso F.; GONZAGA, Alvaro de A.; FREIRE, André L. (coords.). Enciclopédia Jurídica da PUCSP. Tomo Direito Comercial, 1 ed., jul. 2018. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa>. Acesso: 14 nov. 23.

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. 1/2018, 2018.

FRAZÃO, Ana. **Fundamentos dos dados pessoais:** Noções introdutórias para a compreensão da importação da Lei Geral de Proteção de Dados. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords). Lei Geral de Proteção de Dados e Suas Repercussões no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019. E-book, pp. 25-63.

_____. **Transparência de algoritmos x segredo de empresa.** Jota, 2021. Disponível em: <http://www.professoraanafrazao.com.br/files/publicacoes/2021-06-09-Transparencia_de_algoritmos_x_segredo_de_empresa_As_controversias_a_respeito_das_decisoes_judiciais_trabalhistas_que_determinam_a_realizacao_de_pericia_no_algoritmo_da_Uber.pdf> Acesso em: 11 ago. 23.

GARVIE, Clare; FRANKLE, Jonathan. **Facial-Recognition Software Might Have a Racial Bias problem:** Depending on how algorithms are trained, they could be significantly more accurate when identifying white faces than African American ones. *In:* THE ATLANTIC. The Atlantic, 6 abr. 2016. Disponível em: <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-syst ems/476991/>. Acesso em: 10 ago. 23.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro, volume 1:** Parte Geral. 10 ed. São Paulo: Saraiva, 2012.

GILPIN, L. H; BAU, David; YUAN, Bem Z.; BAJWA, Ayesha; SPECTER, Michael; KAGAL, Lalana. **Explaining explanations:** An overview of interpretability of machine learing. Proceedings - 2018 IEEE 5th International Conference on Data Science and Advanced Analytics, DSAA 2018, p. 80-89, 2019. Disponível em: <https://arxiv.org/abs/1806.00069>. Acesso em: 14 nov. 23.

GUNTHER, Luiz Eduardo; LIMA, Thomires E. P. B. de; SILVA, Aurélio Miguel B. da. **Proteção de dados sensíveis na contratação do empregado.** *In:* GUNTHER, Luiz

Eduardo; VILLATORE, Marco Antônio César (coords.). Direitos Digital: LGPD - Aplicabilidade e Questionamentos. Joinville: Maïtre Editora, 2022. E-book. pp. 136-166.

HARARI, Yuval Noah. **21 Lições Para o Século 21.** São Paulo: Companhia das Letras, 2018.

HILDEBRANDT, Mireille. **Privacy as Protection of the Incomputable Self:** from agnostic to agonistic machine learning. Theoretical Inquiries In Law, Tel Aviv, v. 20, n. 1, p. 83-121, jan. 2019. Disponível em: <https://www7.tau.ac.il/ojs/index.php/til/article/view/1622/1723. Acesso em: 14 nov. 23;

HITACHI-UTOKYO LABORATORY. **Society 5.0:** A people-centric super-smart society. Tokyo: Springer, 2018. E-book.

KANSAS. Supreme Court of Kansas. Mann v. Tatge Chemical Co., Inc., 201 Kan. 326, mai. 1968. Disponível em: <https://casetext.com/case/mann-v-tatge-chemical-co-inc>. Acesso em: 14 nov. 23.

KEARNS, Michael; ROTH, Aaron. **The Ethical Algorithm:** the science of socially aware algorithm design. Oxford: Oxford University Press, 2019. E-book.

LANCIERI, Filippo; SAKOWSKI, Patricia Morita. **Competition in Digital Markets:** A Review of Expert Reports. Stanford Journal of Law, Business & Finance. v. 26, p. 65-170, fev. 2021. Disponível em: <https://ssrn.com/abstract=3681322>. Acesso em: 14 nov. 23.

LEE, Kai-Fu. **Inteligência artificial:** Como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos. Tradução de Marcelo Barbão. 1 ed. Rio de Janeiro: Globo Livros, 2019.

LEMONJE, Julise. **Princípios da Lei Geral de Proteção de Dados Pessoais:** do núcleo comum aos desafios de concretização. *In:* BARZOTTO, Luciane C.; COSTA Ricardo H. de A. Martins (orgs.). Estudos sobre LGPD: doutrina e aplicabilidade no âmbito laboral. Porto Alegre: Diadorim Editora, 2022. pp. 181-190.

LEMOS, Ronaldo; LEITE, George Salomão. **Marco Civil da Internet.** São Paulo: Atlas, 2014.

LIPPOLDT, Douglas; SCHUTZ, Mark. **Uncovering Trade Secrets:** An Empirical Assessment of Economic Implications of Protection for Undisclosed Data. Paris: OECD Publising, 2014. p. 7. (OECD Trade Policy Papers, n. 167). Disponível em: <https://doi.org/10.1787/5jxzl5w3j3s6-en>. Acesso em: 14 nov. 23.

LIPTON, Zachary C. **The mythos of model interpretability.** 2018. Disponível em: <https://arxiv.org/abs/1606.03490>. Acesso em: 14 nov. 23.

LOPES, Ivana M. C. **Segredo de Negócio e as Transformações Advindas com a Diretiva 943/2016 UE.** Dissertação (Mestrado em Direito e Ciências Jurídicas) – Faculdade de Direito, Universidade de Lisboa. Lisboa, pp. 151, 2019.

LUNDBERG, Scott; LEE, Su-In. **A Unified Approach to Interpreting Model Predictions.** 2017. Disponível em: <https://arxiv.org/abs/1705.07874>. Acesso em: 14 nov. 23.

MAGALHÃES, Kátia Braga de. **Proteção Legal aos Segredos de Negócio.** Revista da EMERJ, v.3, n.12, 2000.

MAIA, Roberta M. M. **O Legítimo Interesse do Controlador e o Término do Tratamento de Dados Pessoais.** *In:* MULHOLLAND, Caitlin (org.). A LGPD e o Novo Marco Normativo no Brasil. Porto Alegre: Arquipélago Editorial, 2020. E-book, pp. 216-264.

MALDONADO, Viviane Nóbrega. **Dos direitos do titular.** *In:* NOBREGA, Viviane Maldonado; BLUM, Renato Ópice (coord.). LGPD: Lei Geral De Proteção De Dados comentada. São Paulo: Thomson Reuters Brasil. 2019.

MALGIERI, Luciano. **Trade secrets vs personal data:** a possible solution for balancing rights. International Data Privacy Law, v. 6, n. 2, maio 2016.

MASSACHUSETTS. Massachusetts Supreme Judicial Court. Peabody v Norfolk, Inc., 98 Mass. 452, jan. 1868. Disponível em: <https://cite.case.law/mass/98/452/>. Acesso em: 14 nov. 23.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data:** A Revolution That Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt, 2013.

_____; RAMGE, Thomas. **Reinventing Capitalism in the Age of Big Data.** New York: Basic Books, 2018.

_____. **“Generational Development of Data Protection in Europe”**. *In:* Technology and Privacy: The New Landscape. Massachusetts: The MIT Press, 2001.

MCAFEE, Andrew; BRYNJOLFSSON, Erik. **Big Data:** The Management Revolution. Harvard Business Review. Publicado em: out. 2012. Disponível em: <https://hbr,org/2012/10/big-data-the-management-revolution>

MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à Nova Lei de Proteção de Dados (Lei nº 13.709/2018):** O Novo Paradigma da Proteção de Dados. Revista de Direito do Consumidor, v. 120, nov./dez. 2018. p. 22

MINISTÉRIO PÚBLICO FEDERAL. Nota técnica - Veto Lei Geral de Proteção de Dados. Brasília, 2018. Disponível em: <http://www.mpf.mp.br/pgr/documentos/3ccr_nota_tecnica-veto-lei-geral-de-proteção-de-dados-2018.pdf/view>. Acesso em: 14 nov. 23.

MITCHELL, Tom M. **Machine Learning.** New York: McGraw Hill, 1997.

MOLNAR, Cristoph. 2020. **Interpretable Machine Learning:** A guide for making black box models explainable. [S.l.:s.n.], 2022.

MOORE, Taylor R. **Trade Secrets and Algorithms as Barriers to Social Justice.** Center for Democracy and Technolog, 2017. Disponível em: <https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-asBarriers-to-Social-Justice.pdf>. Acesso em: 14 nov. 23.

MULHOLLAND, Caitlin S. **Dados pessoais sensíveis e a tutela de direitos fundamentais:** uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). Revista Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, p. 167 set./dez. 2018. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf>. Acesso em: 14 nov. 23.

_____; FRAJHOF, Isabella Z**. Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais:** breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. *In:* MULHOLLAND, Caitlin, FRAZÃO, Ana (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MURDOCH, W. James; SINGH, Chandan; KUMBIER, Karl; ABBASI-ASL, Reza; YU, Bin. **Interpretable machine learning: definitions, methods, and applications.** 2019. Disponível em: <http://arxiv.org/abs/1901.04592>. Acesso em: 14 nov. 23.

MUSSA, Adriano. **Inteligência Artificial - Mitos e Verdades:** as reais oportunidades de criação de valor nos negócios e os impactos no futuro do trabalho. São Paulo: Saint Paul, 2020.

NYBO, Erick Fontenele. **O Poder dos Algoritmos.** São Paulo: Enlaw, 2019.

ORGANIZAÇÃO MUNDIAL DO COMÉRCIO. **Agreement on Trade-Related Aspects of Intellectual Property Rights.** Genebra: Organização Mundial do Comércio, 1994. Disponível em: https://www.wto.org/english/docs_e/legal_e/27-trips.pdf. Acesso em: 14 nov. 23.

PASQUALE, Frank. **The black box Society:** The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PEREIRA, Alexandre Libório Dias. **A Jurisdição na Internet segundo o Regulamento 44/2001 (e as alternativas extrajudiciais e tecnológicas).** 2001. Disponível em: <https://estudogeral.uc.pt/handle/10316/28775>. Acesso em: 12 ago. 23.

PESTANA, Marcio. **Os princípios no tratamento de dados na LGPD.** Revista Consultor Jurídico, 25 de maio de 2020. Disponível em:

<https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 14 nov. 23

REICHMAN, Jerome. **Universal Minimum Standards of Intellectual Property Protection under the TRIPS Component of the WTO Agreement.** The International Lawyer, Dallas, v. 29, n. 2, p. 347, jan. 1995.

REIS, Nazareno C. M. **Direito à Proteção de Dados e Decisões Automatizadas:** os direitos do titular à luz da LGPD. Dissertação (Mestrado em Direito Constitucional) – Instituto de Ensino Superior, Instituto Brasiliense de Direito Público. Teresina, pp. 203, 2021.

RIBEIRO, Marco. T.; GUESTRIN, Carlos; SINGH, Sameer. **Why Should I Trust You?** Expiaining the Predictions of Any Classifier. 2016. Disponível em: <https://arxiv.org/abs/1602.04938>. Acesso em: 14 nov. 23

SARLET, Gabrielle B. Sales; SARLET, Ingo Wolfgang. **Algumas notas sobre a relação entre Inteligência Artificial, Proteção de Dados Pessoais e os Direitos Fundamentais na Ordem Constitucional Brasileira.** In: DONEDA, Danilo; MENDES, Laura; SARLET, Ingo Wolfgang (coords). Inteligência Artificial, Proteção de Dados Pessoais e Responsabilidade na Era Digital. São Paulo: Expressa Jur, 2022. E-book, pp. 11-40.

SCHEMKEL, Rodrigo Zasso. **Violação do direito à privacidade pelos bancos de dados informatizados.** Disponível em: <http://www.egov.ufsc.br/portal/conteudo/viola%C3%A7%C3%A3o-do-direito-%C3%A0-privacidade-pelos-bancos-de-dados-informatizados>. Acesso em: 14 nov. 23.

SEJNOWSKI, Terrence J. **A revolução do aprendizado profundo.** Rio de Janeiro: Alta Books, 2019.

SILVA, Tarcízio. **Racismo algorítmico:** inteligência artificial e discriminação nas redes sociais. São Paulo: Edições Sesc, 2022. E-book.

SILVEIRA, Newton. **Propriedade Intelectual:** propriedade industrial, direito de autor, software, cultivares, nome empresarial, título de estabelecimento, abuso de patentes. 6. ed. Barueri: Manole, 2018. E-book.

SMYTH, S. M. **The Facebook Conundrum:** Is it Time to Usher in a New Era of Regulation for Big Tech? International Journal of Cyber Criminology, v. 13, n. 2, p. 578-595, jul./dez. 2019.

SOUZA, Carlos Afonso; PERRONE, Christian; MAGRANI, Eduardo. **O direito à explicação entre a experiência europeia e sua positivação na LGPD.** *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. E-book.

TALBOTT, Amy. **Privacy Laws:** How the US, EU and others protect IoT data (or don't). ZdNet, 2016. Disponível em: <https://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/>. Acesso em: 11 ago. 23.

TAVARES, Letícia Antunes; ALVAREZ, Bruna Costa. **Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil.** *In:* ONODERA, Marcus Vinicius Kiyoshi; FILIPPO, Thiago Baldani Gomes. (Coords.). Brasil e EUA: temas de direito comparado. São Paulo: Escola Paulista da Magistratura, 2017.

TEFFÉ, Chiara Spadaccini de. **Dados sensíveis de crianças e adolescentes:** aplicação do melhor interesse e tutela integral. *In:* LATERÇA, Priscilla Silva; Fernandes, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). 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. p. 365-420.

TEPEDINO, Gustavo; OLIVA, Milena Donato. **Tratamento de dados de crianças e adolescentes na LGPD e o sistema de incapacidades do Código Civil.** *In:* LATERÇA, Priscilla Silva; Fernandes, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). 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. p. 305-333.

UE. Comissão Europeia. 2000/520/CE: Decisão da Comissão, de 26 de julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02000D0520-20000825&from=EL>. Acesso em: 14 nov. 23.

UE. Comissão Europeia. **Ethics guidelines for trustworthy AI.** 8 abr. 2019, Disponível em: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>. Acesso em: 14 nov. 23.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. **Counterfactual explanations Without Opening the Black Box:** automated decisions and the GDPR. Harvard Journal of Law & Technology, Cambridge, v. 31, n. 2, p. 841-887, 2018. Disponível em: <https://arxiv.org/abs/1711.00399>. Acesso em: 14 nov. 23

WESTIN, Alan. F. **Privacy and Freedom.** New York: Atheneum, 1967.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira. Rio de Janeiro: Intrínseca, 2019.