UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO
CURSO DE DIREITO

THAIANE KOEHLER

SITUAÇÕES DISCRIMINATÓRIAS CAUSADAS PELO TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS: OS IMPACTOS DA AUSÊNCIA DE UMA REVISÃO HUMANA NO ARTIGO 20 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

FLORIANÓPOLIS
2023

Thaiane Koehler

Situações discriminatórias causadas pelo tratamento automatizado de dados pessoais: os impactos da ausência de uma revisão humana no artigo 20 da Lei Geral de Proteção de Dados Pessoais

Trabalho de Conclusão de Curso submetido ao curso de Direito do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Bacharela em Direito.

Orientadora: Prof.ª Liz Beatriz Sass, Dr.ª

Florianópolis

2023

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado "Situações discriminatórias causadas pelo tratamento automatizado de dados pessoais: os impactos da ausência de uma revisão humana no Art. 20 da Lei Geral de Proteção de Dados Pessoais", elaborado pelo(a) acadêmico(a) **Thaiane Koehler**, defendido em **16/06/2023** e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota 10,0 (dez), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, 16 de Novembro de 2023

Liz Beatriz Sass
Professor Orientador

Bruno Cassol da Silva
Membro de Banca

Rômulo Francisco Hendges dos Santos
Membro de Banca

Universidade Federal de Santa Catarina
Centro de Ciências Jurídicas
COORDENADORIA DO CURSO DE DIREITO

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E ORIENTAÇÃO IDEOLÓGICA

Aluno(a): Thaiane Koehler
RG: 6.513.645
CPF: 108.683.719-39
Matrícula: 18200056
Título do TCC: Situações discriminatórias causadas pelo tratamento automatizado de dados pessoais: os impactos da ausência de uma revisão humana no artigo 20 da Lei Geral da Proteção de Dados Pessoais.
Orientador(a): Liz Beatriz Sass

Eu, **Thaiane Koehler**, acima qualificado(a); venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 16 de junho de 2023.

gov.br Documento assinado digitalmente
THAIANE KOEHLER
Data: 23/06/2023 14:52:22-0300
Verifique em https://validar.iti.gov.br

Thaiane Koehler

Thaiane Koehler

Situações discriminatórias causadas pelo tratamento automatizado de dados pessoais: os impactos da ausência de uma revisão humana no artigo 20 da Lei Geral de Proteção de Dados Pessoais

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de Bacharela e aprovado em sua forma final pelo Curso de Direito.

Florianópolis, 16 de junho de 2023.

Prof. Francisco Quintanilha Veras Neto, Dr.
Coordenação do Curso

Banca examinadora

Prof.ª Liz Beatriz Sass, Dr.ª
Orientadora

Bruno Cassol da Silva
Programa de Pós-Graduação em Direito (PPGD/UFSC)

Rômulo Francisco Hendges dos Santos
Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação (PROFNIT)

Rafael Carvalho Bueno
Programa de Pós-Graduação em Direito (PPGD/UFSC)

Florianópolis, 2023.

Dedico esta monografia à minha família, em especial aos meus avós, por nunca terem experienciado as mesmas oportunidades que tive. Também à Luana, minha amada companheira, que há dois anos me incentiva e apoia na realização dos meus sonhos.

AGRADECIMENTOS

É chegado o momento de concluir uma das etapas mais desafiadoras e importantes para o meu desenvolvimento pessoal e profissional até aqui. Por isso, este Trabalho de Conclusão de Curso carrega consigo um significado para além do conteúdo e tema abordados.

Ele representa, também, uma vitória para aquela menina que enfrentou grandes desafios de adaptação à escola durante a infância e que jamais imaginou ser capaz de sair da casa dos pais aos dezoito anos para cursar Direito na Capital.

É verdade que para chegar até aqui, contei com o apoio, incentivo e me espelhei em muitas pessoas, as quais não seria capaz de agradecer nominalmente. Porém, aqueles que forem citados, certamente, representam também todos que, de alguma forma, contribuíram para esta conquista.

Em primeiro lugar, agradeço à minha mãe, Ana Regina. Obrigada por cada minuto de escuta, por cada palavra de conforto e carinho dita nos momentos em que me senti confusa ou pensei em desistir. Obrigada também por ter feito tanto pelo meu desenvolvimento. Você sempre fez o melhor que pôde com os recursos que tinha, desde os meus primeiros anos até os dias atuais, isso fez toda diferença e me tornou a pessoa que sou hoje. Você sempre será o meu grande exemplo de vida.

Ao meu pai, Antônio, sou eternamente grata por ter acreditado e confiado, desde sempre, nas minhas ideias. O seu suporte e segurança tornaram os caminhos mais fáceis. Obrigada por me amparar e por colocar a nossa família em primeiro lugar. Me inspiro muito na sua honestidade e trabalho árduo para conquistar o melhor para nós.

Às minhas irmãs, Thaise e Daniela, vocês são os meus dois grandes e primeiros exemplos de dedicação para alcançar cada objetivo. Foi com vocês que aprendi valores significativos e é em suas conquistas, tanto pessoais como profissionais, que me espelho. Obrigada por estarem ao meu lado me dando forças para seguir desde sempre. Amo muito vocês.

Ao meu cunhado, Fife, você é como um irmão, obrigada por estar conosco há tanto tempo e por sempre me apoiar.

Aos nossos pequenos, Laura e Afonso, obrigada por completarem a nossa família e por nos trazerem tantas alegrias. Espero, em alguma medida, abrir

caminhos para a jornada que vocês irão trilhar no futuro. Contem sempre com a Tia Ni.

Ao meu amor, Luana, obrigada por estar ao meu lado, por ouvir as minhas angústias, planos e por sonhar comigo. Ter você para compartilhar a vida torna tudo melhor.

Agradeço, também, a todos os professores que, desde a alfabetização até a graduação, contribuíram para a minha formação. Em especial, cito a Lila Krieger, responsável por plantar em mim a sementinha da vontade de estudar em uma Universidade Federal. Serei eternamente grata por, no ano de 2014, o universo ter cruzado os nossos caminhos e por teres me feito acreditar tanto no meu potencial.

Aos meus colegas da graduação, obrigada pelos momentos de descontração, por terem feito Floripa se tornar, também, o meu lar. A excelência de cada um, apesar de suas particularidades, me inspira a ser cada vez melhor. Embora nossos caminhos possam nos distanciar, guardarei com muito carinho as memórias construídas nestes anos com vocês.

Agradeço também ao DOT Digital Group, mais especificamente a Bruna e ao Gui, pessoas que, em 2021, me acolheram nesta incrível empresa e, desde então, confiam no meu trabalho. Serei eternamente grata pelas oportunidades diárias vividas junto de vocês.

Por fim, agradeço ao Universo por sempre colocar no meu caminho pessoas boas, com as quais pude aprender e ensinar. É nisso que tudo se resume. Espero ter ainda muita saúde e energia para continuar em busca de evolução pessoal, profissional e acadêmica para poder oferecer o meu melhor a quem eu encontrar pela vida.

RESUMO

A presente monografia, elaborada com base no método indutivo e em revisões bibliográficas, procura evidenciar como a privacidade e a proteção dos dados pessoais estão ligadas aos mecanismos tecnológicos, especialmente às decisões automatizadas tomadas por Sistemas de Inteligência Artificial. Nesse viés, concentrando-se mais especificamente no artigo 20 da Lei Geral de Proteção de Dados Pessoais, mostra-se como a atual redação deste artigo da Lei pode sujeitar o titular de dados pessoais que tenha se sentido lesado e, por isso, solicitado revisão desta decisão, à uma nova situação potencialmente discriminatória. Ou, ainda, corroborar para a falta de uma explicação clara sobre como determinada decisão foi tomada. Diante de tal cenário, objetiva-se evidenciar a emergente necessidade de retificação do artigo 20 da Lei Geral de Proteção de Dados Pessoais, bem como, demonstrar a importância da promulgação de uma Lei específica que regule a temática da Inteligência Artificial no Brasil, conforme já vem sido discutido no Senado Federal. Assim, o primeiro capítulo discorre sobre os aspectos gerais da privacidade e proteção de dados pessoais. O segundo, abrange os aspectos técnicos das tecnologias que tomam decisões de forma autônoma, evidenciando seus principais problemas. Por fim, o terceiro capítulo fornece um panorama geral sobre a regulação do tema no Brasil e no mundo, apresentando, também, a sugestão de mudança do atual artigo 20 da Lei Geral de Proteção de Dados Pessoais e a necessidade de promulgação de uma Lei específica para regular, em linhas gerais, os Sistemas de Inteligência Artificial no Brasil.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais. Discriminação. Dados Pessoais. Decisões Automatizadas. Algoritmos. Inteligência Artificial.

ABSTRACT

This monograph, developed based on the inductive method and on bibliographic reviews on the subject, wants to show how privacy and data protection are near to technologies, especially automatizated decisions made by Artificial Intelligent Sistems. In this way, specific considering the 20 article of the brazilian Lei Geral de Proteção de Dados Pessoais, the objective is to evidence how the current wording of this article of the Law can subject the holder of personal data who has felt aggrieved and, therefore, requested revision of this decision, to a new potentially discriminatory situation. Or even corroborate the lack of a clear explanation of how a particular decision was made. Faced with such a scenario, based on technical and factual evidence discussed throughout the chapters, the objective is to show the emerging need to rectify article 20 of the General Law for the Protection of Personal Data, as well as to demonstrate the importance of enacting of a specific Law that regulates the topic of Artificial Intelligence in Brazil, as has already been discussed. So, this search is based on three chapters. The first is about general aspects about data protection and privacy. The second chapter includes technical aspects of technologies that make decisions autonomously, bringing some of their problems, since they are created. The third and last chapter brings a general view about this subject in Brazil and other countries around the world, making a suggestion to change the currently 20 article of the Brazilian Lei Geral de Proteção de dados and the necessity of a specific law to regulate the subject of Artificial Intelligent in Brazil.

Keywords: General Data Protection Law. Discrimination. Personal Data. Automated Decision. Algorithms. Artificial Intelligent.

SUMÁRIO

1 INTRODUÇÃO

Quando se pensa sobre a internet, é comum a impressão de que ela está intimamente relacionada ao ser humano e vem funcionando como um componente essencial para a sua relação com a sociedade. Entretanto, sabemos que nem sempre foi assim.

Por volta dos anos 2000, parcela da população tinha acesso à conhecida Web 1.0, marcada pela conexão discada, a qual apresentava uma série de limitações e empecilhos técnicos. Por isso e por outras razões, o público que a utilizava mostrava-se bastante reduzido. Já com o advento da Web 2.0, responsável por viabilizar que mais pessoas pudessem acessar a internet, por apresentar para a sociedade os smartphones, bem como, a possibilidade de interação entre os usuários nos sites, teve início um novo cenário (ANDRADE, 2022).

Nos dias de hoje, vivemos na era da Web 3.0, momento no qual as máquinas e usuários estão convivendo de maneira extremamente próxima e constante. Nesta fase, a privacidade e inteligência artificial são palavras-chave, as quais estão revolucionando a maneira como o ser humano interage com a tecnologia (ANDRADE, 2022).

Portanto, diante dos consideráveis impactos econômicos e das significativas mudanças percebidas na vida das pessoas provocadas pela ascensão da Web 3.0, o Direito foi, mais incisivamente, convocado a agir. Nesse viés, legislações tiveram que ser criadas – e outras ainda devem surgir ou sofrer aprimoramento – para poder albergar e regular questões que, ao longo deste desenvolvimento tecnológico passaram a afetar, em alguns casos, negativamente, a vida das pessoas.

No Brasil, uma dessas intervenções do Direito culminou na Lei Geral de Proteção de Dados Pessoais, diploma legal voltado especificamente para regular como deve se dar o tratamento dos dados pessoais no Brasil, e responsável por incutir na sociedade questões fundamentais sobre a necessidade de preservação da privacidade das pessoas.

No artigo 20 da referida Lei, há menção sobre decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, evidenciando, assim, sua forte relação com a Web 3.0, tendo em vista que o tratamento automatizado a que se refere é viabilizado por Sistemas de Inteligência Artificial.

Desse modo, a problemática a ser trabalhada no presente estudo reside justamente no texto do artigo 20 da Lei Geral de Proteção de Dados Pessoais, o qual, da maneira como se apresenta hoje, não atende, efetivamente, às necessidades da sociedade. Isso porque sua atual redação permite às empresas designarem robôs para revisar decisões tomadas unicamente com base no tratamento automatizado dos dados pessoais – ou seja, permite que decisões potencialmente lesivas, originalmente tomadas por robôs, sejam também revisadas por robôs, em vez de assegurar que um ser humano se responsabilize por esta revisão.

Além disso, serão abordadas questões técnicas dos Sistemas de Inteligência Artificial, os quais apresentam alta capacidade de proporcionar relevantes ganhos de produtividade para a sociedade em geral, mas possuem características intrínsecas potencialmente lesivas aos usuários como, por exemplo, a perpetuação de preconceitos sociais já conhecidos.

Desse modo, o presente estudo visa, por meio de revisões bibliográficas, contextualizar pontos basilares sobre a privacidade, mostrando como se deu a construção da percepção da necessidade de proteção legal em relação ao tema ao longo das décadas, até chegar ao seu status atual.

Busca-se também, por meio de explicações a respeito das especificidades técnicas destes mecanismos, especialmente tratadas no segundo capítulo, proporcionar ao leitor a construção de uma visão crítica e questionadora sobre a captação e tratamento dos dados pessoais. Sendo assim, serão debatidos temas como a instauração de uma vigilância ininterrupta sobre os indivíduos, a defendida ideia de neutralidade dos algoritmos e os argumentos – proteção dos segredos comercial e industrial – que conferem proteção legal a estas tecnologias e, por vezes, inviabilizam que as empresas sejam pressionadas a resolver os problemas apresentados.

No último capítulo, serão trazidas considerações sobre o cenário atual do Brasil e do mundo a respeito da regulação legislativa relacionada aos Sistemas de Inteligência Artificial, os quais estão intimamente relacionados às decisões tomadas de maneira totalmente automatizada, objeto do presente estudo.

Por fim, far-se-á a proposição de uma mudança pontual no texto do artigo 20 da Lei Geral de Proteção de Dados Pessoais capaz de trazer significativos impactos positivos quando um titular de dados se sentir lesado e, por isso, solicitar a revisão

de uma decisão totalmente automatizada que, possivelmente, tenha lhe causado algum prejuízo. Além da defesa da ideia de continuidade dos esforços legislativos no país para que uma lei específica para regular os Sistemas de Inteligência Artificial seja promulgada.

2 HISTÓRICO E EVOLUÇÃO DA CAPTAÇÃO DE DADOS PESSOAIS

No primeiro capítulo do presente estudo serão tecidas considerações gerais sobre a privacidade, sua relação com os dados pessoais e sobre como eles se conectam à sociedade como um todo. Nesse sentido, a utilização de referências literárias nacionais e internacionais, as quais retratam a questão da privacidade em momentos e contextos sociais diversos, servirá como ponto de partida para o entendimento de que todas as pessoas, em maior ou menor grau, enfrentam tais dilemas ao longo de suas vidas.

A fim de evidenciar e enfatizar a importância que se atribui ao tema, será traçada a linha cronológica, com base nas quatro gerações de leis de proteção de dados pessoais, tornando possível, assim, uma melhor visualização sobre como a privacidade e a proteção dos dados pessoais passou a receber respaldo legal no decorrer das décadas. Por fim, o capítulo se encerra com a constatação e o apontamento das lacunas que ainda persistem em nosso ordenamento jurídico e podem ser prejudiciais ao titular de dados pessoais no Brasil.

2.1 PRIVACIDADE E DADOS PESSOAIS

Ao falar em privacidade, muitas são as obras literárias que, de um modo ou de outro, perpassam pelo tema. Sendo assim, optou-se por introduzir as primeiras linhas destinadas a tratar sobre a vida íntima das pessoas, trazendo para o debate a icônica obra brasileira *O Cortiço* (AZEVEDO, 2019), a qual transita pelo assunto de maneira singular.

Na obra em questão, as pessoas vivem sem os mínimos resquícios de privacidade. Como descrito em caráter até eufêmico – que abrandava o verdadeiro caos – desde o amanhecer, nas primeiras necessidades do dia, as pessoas estavam dividindo o mesmo espaço e a mesma água para lavar os rostos (AZEVEDO, 2019). Nessas estadias apertadas, viviam os menos favorecidos financeiramente e, para eles, a privacidade custaria um valor impossível de se pagar. Portanto, conseguir se instalar e viver de maneira privada no século XIX era um privilégio alcançado apenas pelos mais ricos.

No mesmo ano de lançamento da obra supracitada, nos Estados Unidos, Samuel Warren e Louis Brandeis publicaram o artigo *The Right to Privacy* na revista

Harvard Law Review. Diferentemente do livro brasileiro, a obra em questão possui caráter jurídico, não literário, e foi responsável por ensejar o reconhecimento formal do direito à privacidade no ordenamento jurídico americano. Tal artigo é, até os dias de hoje, considerado um marco sobre o tema da privacidade (WARREN; BRANDEIS, 1890).

Na obra americana, encontram-se considerações dos autores sobre como o direito se expande para comportar as necessidades de intervenção jurídica na vida das pessoas na medida em que ocorrem as mudanças nos âmbitos político, social e econômico da sociedade.

Nesse viés, as mudanças sociais ocorridas com o advento das tecnologias são trazidas pelos autores como ensejadoras da criação de novos direitos e, como pontuado no artigo, invenções e métodos recentes estavam chamando atenção para que um próximo passo fosse dado para a proteção das pessoas (WARREN; BRANDEIS, 1890).

Esse direito emergente, por assim dizer, seria o “direito de ser deixado a sós” e um dos principais episódios que motivou sua reivindicação foi a intrusão da mídia, munida das mais novas e tecnológicas máquinas fotográficas da época, na esfera privada das pessoas.

Os autores americanos tecem críticas severas em relação ao fato de que a invasão na vida íntima da população mais abastada e a posterior veiculação comercial das fotos capturadas, havia virado um negócio lucrativo. Para eles, a disseminação detalhada dos bastidores da vida das pessoas para satisfazer a curiosidade e servir de entretenimento para a massa estava criando uma necessidade cada vez maior de preservação da privacidade dos indivíduos (WARREN; BRANDEIS, 1890).

Portanto, ao comparar as duas referências acima citadas, ainda que sejam aparentemente opostas em seu conteúdo e estilo literário, observa-se o tema da privacidade trazido para o debate e figurando como assunto inerente aos mais diversos contextos sociais. Entretanto, na primeira obra, a mesma figura como um traço que apenas compõe o cotidiano da população sendo, inclusive, negligenciado. Já no artigo publicado na *Harvard Law Review*, considerando que o público diretamente afetado possuía influência e poderes na sociedade, a privacidade é tratada com centralidade, sendo a sua defesa reivindicada de maneira contundente ao longo do texto.

Nesse ponto, considerando o antagônico cenário social experienciado pelos habitantes dos cortiços no Rio de Janeiro daqueles vividos pelas pessoas que compunham a elite americana – ao passo que , no primeiro, a escassez fazia todos ocuparem o mesmo espaço e, no segundo, a vida das pessoas era suficientemente interessante para ser especulada disseminada em jornais e gerar lucros – faz-se pertinente mencionar a constatação trazida por Doneda (2021), na qual o referido autor defende que a tutela da privacidade só passa a ser percebida como fator relevante a partir do momento em que outras necessidades mais básicas inerentes ao ser humano já tenham sido satisfeitas (DONEDA, 2021, p. 45).

Não obstante, passado quase um século da veiculação das duas obras já mencionadas, Michel Foucault publica um de seus livros mais famosos, *Vigiar e punir* (FOUCAULT, 1987). Nele, uma das temáticas abordadas é, também, a privacidade, a qual será apresentada no presente trabalho sob um terceiro recorte.

Para Foucault, o ato de vigiar, responsável por suprimir a privacidade das pessoas, estaria relacionado diretamente ao grau de disciplina e controle que seria incutido nelas. Portanto, as mais diversas instituições, como escolas, fábricas e presídios, deveriam dispor de eficientes mecanismos de vigia para que conseguissem atingir níveis elevados de desempenho produtivo e disciplinar (FOUCAULT, 1987).

Para que fosse possível exercer o controle e monitoramento máximo sobre as pessoas, o referido autor descreve na obra uma estrutura que, pela maneira como é construída, possibilita o exercício da vigilância de maneira extremamente eficiente: “O Panóptico é uma máquina de dissociar o par ver-se visto: no anel periférico, se é totalmente visto, sem nunca ver; na torre central, vê-se tudo, sem nunca ser visto.” (FOUCAULT, 1987, p. 222).

Nesse sentido, podemos depreender que a centralidade do funcionamento de tal mecanismo seria justamente criar a possibilidade de supressão da privacidade das pessoas sem que elas pudessem perceber que estão sendo vistas, causando, assim, a constante dúvida sobre a possibilidade de se estar sendo acompanhado e, por isso, sempre agir da maneira que fosse esperada pela instituição na qual o indivíduo está inserido.

Conforme será exposto no segundo capítulo, o que se constata é a evidente proximidade entre o panóptico de Foucault e o contemporâneo ato de vigiar exercido a partir de dispositivos tecnológicos que pairam sobre todos os indivíduos

conectados à rede mundial de internet. Hoje, nesse exato momento, as grandes empresas de tecnologia sabem, com precisão, os lugares pelos quais nos deslocamos e outras importantes informações sobre a vida privada das pessoas. Tudo isso sem que nós, necessariamente, tenhamos consciência de que “alguém” nos acompanha.

Além disso, ainda traçando um paralelo entre a obra de Foucault e a temática da privacidade, observa-se que atualmente a privacidade passou a se estruturar de uma maneira na qual está diretamente ligada ao controle das pessoas, em vez de se manter relacionada aos segredos, como era comum anteriormente (DONEDA, 2021).

A partir da explanação das três referências acima elencadas acerca da privacidade, cada qual em um contexto geográfico, social e temporário particular, podemos concluir que a questão concernente à temática é uma constante nas relações humanas. Sendo assim, procurar-se-á associar o tema à principal maneira de supressão da privacidade que encontramos hoje: os dados pessoais e a sua capacidade de criar rastros precisos sobre os seus titulares.

Nessa toada, ao encontro da realidade acima delineada, surge a ideia de dimensão coletiva da privacidade, a qual é explanada e relacionada aos dados pessoais de maneira acurada por Doneda (2021):

> Dessa dimensão coletiva surge, enfim, a conotação contemporânea da proteção da privacidade, que manifesta-se sobretudo (porém não somente) através da proteção de dados pessoais; e que deixa de dar vazão somente a um imperativo de ordem individualista, mas passa a ser frente onde irão confluir vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana, fazendo com que na disciplina da privacidade passe a se definir todo um estatuto que englobe as relações da própria personalidade com o mundo exterior. (DONEDA, 2021, p. 47).

Assim, para que seja possível uma compreensão ampla e contextualizada sobre o que seriam os dados pessoais e o que eles representam no nosso cotidiano, faz-se pertinente uma breve contextualização histórica, bem como, aderir a abordagem que permita compreender as mais diversas facetas apresentadas em diferentes circunstâncias e utilizações.

Nesse viés, o ato de sermos representados pelos nossos dados, guardadas as devidas peculiaridades de cada época, não é uma realidade exclusivamente contemporânea, ainda que na atualidade eles sejam, potencialmente, o mais

poderoso instrumento apto a dizer para a sociedade quem nós somos (DONEDA, 2021).

Nesse sentido, sabe-se que os registros civis, por exemplo, são práticas milenares presentes em diversas civilizações ao redor do globo. Essas escrituras seculares demonstram como o tratamento de dados pessoais pelo poder governamental foi importante para manter o conhecimento sobre a própria população devidamente organizado:

> Durante o governo dos Antônimos em Roma, o registro de nascimentos dentro de um prazo de 30 dias, no templo de Saturno, era obrigatório para toda a população livre. Um outro sistema antigo, com um certo grau de eficácia, era o registro civil do Império Inca. Em 1532, a Inglaterra estabeleceu a obrigatoriedade do registro de óbitos, através dos famosos Bills of Mortality, que deram origem a um dos primeiros estudos sistemáticos da mortalidade (Graunt, 1962). Em 1538, uma lei civil obrigou a Igreja Anglicana a manter registros semanais de casamentos, batismos e enterros. (HAKKERT, 1996, p. 32).

A coleta primitiva dos dados pessoais elencada acima é o que hoje se denomina "*raw-data*", ou seja, aqueles dados tratados antes do advento da internet e sem qualquer tipo de automatização envolvida (LINDOSO, 2021). Porém, atualmente, após revoluções tecnológicas, os dados compreendem um universo muito mais expandido:

> Hoje, os dados são considerados aqueles conteúdos que informam o nome, a data de nascimento, o gênero e a raça do usuário, mas que também informam o tempo de permanência em uma determinada página de rede social, a aquisição feita, a quantidade de interações pela internet, a busca realizada na página do Google, entre tantas outras informações. Tantas quanto possíveis, são as informações que se podem extrair da rede e que são considerados dados pessoais por relacionarem algum comportamento ou característica a uma pessoa específica. (LINDOSO, 2021, p. 33-34).

Assim, para que seja possível albergar a trajetória dos dados pessoais e o seu deságue no atual cenário com a Lei Geral de Proteção de Dados Pessoais, torna-se imprescindível a compreensão sobre as gerações de leis relacionadas aos dados pessoais que tivemos até o momento, em contexto mundial, e sobre como a tratamento jurídico relativo ao assunto evoluiu, no Brasil.

2.2 EVOLUÇÃO DO TRATAMENTO JURÍDICO SOBRE OS DADOS PESSOAIS NO BRASIL

Antes de adentrar especificamente nos aspectos nacionais relacionados à legislação em torno dos dados pessoais, será necessário, primeiramente, tecer os comentários pertinentes a respeito das gerações de leis de proteção de dados pessoais no cenário mundial que, ao total, são quatro.

A primeira geração de leis de proteção de dados pessoais teve início em 1970, no contexto em que o Estado figurava como detentor de vultosos bancos de dados utilizados, prioritariamente, mas não de maneira exclusiva, por órgãos da administração pública. Nesse momento, pairavam grandes incertezas acerca da utilização da tecnologia e as possíveis consequências de sua aplicação nesses grandes bancos. Por isso, o que se observa nessas legislações são princípios de proteção muito amplos, com foco específico na atividade do processamento de dados.

No primeiro momento, ficava evidente que, nesse contexto, se considerava a aplicação da tecnologia como um perigo e, por esse motivo, as leis eram direcionadas mais para os bancos de dados do que para a privacidade em si. Diante da multiplicação desses bancos e da dificuldade encontrada para instituir um acompanhamento constante e efetivo, a primeira geração de leis começou a declinar (DONEDA, 2021).

A segunda geração dessas leis, por sua vez, data da segunda metade da mesma década, e está inserida no contexto em que os bancos de dados já haviam se enraizado por vários lugares diferentes, fator responsável por dificultar de maneira considerável a capacidade de controle que poderia ser exercida sobre eles.

Assim, em relação à geração anterior:

> A característica básica que diferencia tais leis é sua estrutura, não mais em torno do fenômeno computacional em si, mas baseada na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa a ser exercida pelo próprio cidadão. (DONEDA, 2021, p. 181).

Aqui, apesar dessa primeira mudança de paradigma, alguns problemas ainda se faziam presentes como, por exemplo, a vasta abrangência das consequências

que seriam geradas a partir do consentimento dos cidadãos sobre o uso de seus dados pessoais (DONEDA, 2021).

Na década de 1980, observou-se o advento da terceira geração legislativa. Nesse momento, surge a preocupação em, para além da liberdade de conceder ou negar o uso dos próprios dados, assegurar a efetividade do exercício de tal liberdade pelos titulares.

Como trazido por Doneda (2021), o ponto relacionado a essa geração que merece destaque é a consideração de que os dados pessoais estão diretamente ligados à participação da pessoa na sociedade e, portanto, se torna fundamental que os titulares estejam protegidos dos possíveis fatores que prejudiquem seu direito de decidir livremente.

Foi no mesmo período que a autodeterminação informativa passou a ser defendida. Portanto, não bastava o consentimento do titular em relação ao uso de seus dados pessoais, mas deveria ser possível, ainda, que ele soubesse e pudesse acompanhar o que seria feito posteriormente com os dados ora cedidos. Entretanto, como bem elucidado por Doneda (2021), a necessidade de participação ativa das pessoas fez com que a adesão ao exercício de tal prerrogativa se limitasse a uma camada bastante restrita da sociedade.

A quarta geração de dados, por sua vez, compreende as leis contemporâneas sobre a temática. Como característica, pode-se citar o reconhecimento do desequilíbrio de poder existente entre os titulares de dados e as entidades que os coletam e promovem tratamento. Além disso, tendo em vista que as meras decisões individuais, por vezes, não são suficientes para assegurar a proteção integral da pessoa, observou-se a necessidade de uma proteção legal mais sofisticada, o que será elucidado à frente com base na Lei Geral de Proteção de Dados Pessoais. Dentro dessas leis, vê-se o surgimento de autoridades independentes atuantes na fiscalização e aplicação das sanções previstas nas leis, como é o caso da Autoridade Nacional de Proteção de Dados, no Brasil (DONEDA, 2021).

Como visto, a Lei Geral de Proteção de Dados está inserida no contexto da quarta geração. Tal dispositivo legal entrou em vigor em setembro de 2021 e passou a ditar as regras relacionadas à proteção de dados pessoais em todo o território brasileiro. Entretanto, é importante a compreensão de que a referida lei não inaugurou o respaldo jurídico relacionado aos dados pessoais no país.

Mesmo antes do advento da Lei Geral de Proteção de Dados Pessoais, existiam legislações esparsas que tratavam sobre o assunto de maneira descentralizada em nosso ordenamento como, por exemplo, a própria Constituição Federal, o Código de Defesa do Consumidor e o Marco Civil da Internet. É sobre essas previsões precedentes e descentralizadas que se ocuparão os próximos parágrafos do presente trabalho.

Como um primeiro ponto, cabe analisar que a própria Carta Magna brasileira traz, em seu artigo 5º, no rol de direitos fundamentais, dois incisos que abarcam a temática dos dados:

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

No inciso XII, observa-se a menção ao sigilo relacionado a dados. Entretanto, nesse momento, ainda não se falava propriamente nos dados pessoais, fator que aumentava consideravelmente o espectro abordado. Não obstante, a quebra do sigilo estava relacionada diretamente ao âmbito de ações criminais, não sendo possível tal aplicação na esfera civil.

Já no inciso LXXII do mesmo artigo, observa-se um remédio constitucional denominado habeas data. Tal previsão constitucional, remonta o período em que o país esteve sob a ditadura militar e, por isso, o Estado detinha informações sobre as pessoas e as mantinha sob sigilo, a fim de viabilizar o aparato de repressão ditatorial. Com a redemocratização, foi concedido o direito a cada cidadão de saber o que há sobre ele em bancos de dados governamentais ou de caráter público, instituindo-se, portanto, o habeas data.

Entretanto, um ponto que merece atenção sobre o Habeas Data é sua restrição relacionada às empresas e entidades que, nesse caso, devem obrigatoriamente ter caráter público. Isso se difere do que está previsto na Lei Geral de Proteção de Dados Pessoais, uma vez que, atualmente, tanto os órgãos públicos, quanto empresas privadas, estão sob os comandos legais. Importante também

constatar que nesse inciso, há menção direta às “informações relativas à pessoa”, ou seja, havia referência propriamente aos dados pessoais.

Passados dois anos da promulgação da Constituição Federal, o Código de Defesa do Consumidor (BRASIL, 1990), no artigo 43, também trouxe pertinentes disposições acerca da temática que merecem destaque:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. (BRASIL, 1990).

Como elencado no parágrafo primeiro do artigo mencionado supra, são trazidos pressupostos como veracidade, objetividade, limite temporal e comunicação prévia para que seja observada a licitude do tratamento dos dados. Além disso, os bancos de dados e cadastros de consumidores aos quais se refere a lei em comento, não mais se restringem aos órgãos públicos, como no caso do habeas data.

Como um terceiro ponto relevante acerca da temática que precedeu a Lei Geral de Proteção de Dados Pessoais e que colaborou para amadurecer a questão em torno do debate mais apurado sobre o tema, cabe citar a Lei n° 12.965 (BRASIL, 2014), conhecida como Marco Civil da Internet. Apesar de trazer em seu conteúdo diretrizes gerais sobre o uso da internet, o Marco Civil elencou, em seu artigo sétimo, alguns direitos dos usuários relacionados aos dados pessoais, como, por exemplo:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> [...]
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais [...] (BRASIL, 2014).

Como visto, o Marco Civil da internet trouxe, no ano de 2014, pressupostos como a vedação de compartilhamento dos dados pessoais com terceiros sem autorização, necessidade de exatidão e clareza sobre os dados, limitação das finalidades para sua utilização e a figura do consentimento, os quais ocupam lugar de destaque na atual Lei Geral de Proteção de Dados.

Após todo o trajeto legislativo percorrido e a presença dos artigos supracitados, que tratavam sobre os dados pessoais de maneira descentralizada, dentro de leis direcionadas a assuntos mais abrangentes, no ano de 2018 foi sancionada a Lei Geral de Proteção de Dados no Brasil.

As origens do referido diploma legal datam do ano de 2010, quando as primeiras tramitações foram iniciadas, mas a lei passou a viger e surtir seus efeitos apenas em setembro do ano de 2021.

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais inaugurou no cenário nacional um novo momento relacionado aos aspectos legislativos e culturais voltados aos dados pessoais no país. Como expressão desse novo cenário, pode-se citar, por exemplo, a definição de conceitos chave no bojo da lei – e aqui ganha destaque a definição dos dados sensíveis, ligados também ao combate à discriminação, como será abordado adiante, e a consolidação do direito de proteção de dados como um direito fundamental, o que se traduziu na emenda constitucional de número 115, promulgada no dia 11 de fevereiro de 2022.

Desse modo, conforme destacado por Lindoso (2020), a Lei Geral de Proteção de Dados Pessoais ensejou:

> A consolidação de um novo arcabouço principiológico que deverá orientar todo o tratamento de dados pessoais. Foram estabelecidas diretrizes importantes relacionadas à boa-fé, a não discriminação e à necessidade de transparência já dispersas em outros diplomas. Além da enumeração dos princípios, a própria definição de conceitos-chave para a dinâmica do tratamento de dados ressaltou a preocupação do legislador com essas diretrizes essenciais. (LINDOSO, 2020, p. 44).

Para além da definição de conceitos-chave, como visto, a referida lei está assentada sobre princípios fundamentais que norteiam toda a discussão sobre a qual se propõe. Esses dez princípios norteadores estão elencados no rol do artigo 6º, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Nesse viés, tendo em vista que o cerne do presente trabalho reside na discussão específica a respeito das situações discriminatórias causadas pelo tratamento automatizado de dados pessoais, faz-se pertinente, aqui, um estudo mais acurado sobre o princípio da não discriminação e sobre como ele se liga ao tratamento automatizado de dados pessoais.

Na Lei Geral de Proteção de Dados Pessoais, encontra-se o princípio da não discriminação no Art. 6º, inciso IX "[...] não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos [...]" (BRASIL, 2018). Além disso, cabe perceber que o referido princípio, além de encontrar abrigo na Lei Geral de Proteção de Dados, está cravado também na Constituição da República em seu Art. 3º, inciso IV, no qual consta: "[...] promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação [...]" (BRASIL, [Constituição, 1988]). E, para coroar sua relevância, documentos internacionais como a Declaração Universal dos Direitos Humanos, também preveem que a discriminação deve ser combatida em todo e qualquer tipo de relação e ambiente.

Um ponto importante a ser ressaltado, como defendido por Leonardo Roscoe Bessa[1] nessa discussão é a constatação de que o que se pretender inibir é a discriminação injusta, abusiva, com finalidade lesiva ou ilícita. Desse modo, doravante no presente trabalho, quando se falar em discriminação, deve-se sempre entender o conceito em seu sentido discriminatório injusto e não no sentido de mera distinção de diferenças, sem necessariamente ser prejudicial, que o termo também abarca quando suscitado em outros contextos.

[1] No curso de extensão "Lei de Proteção de Dados (LGPD) do Brasil", promovido pela Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) (PUCRS ONLINE, [202-]).

Nesse viés, dada a relevância que circunda o princípio da não discriminação, ele não poderia deixar de se fazer presente nas legislações destinadas a regular as decisões tomadas com base em dados pessoais no ambiente virtual.

Entretanto, apesar de sua presença para balizar as discussões jurídicas, o que se vê é que a lei ainda enfrenta dificuldades relacionadas tanto aos aspectos técnicos das tecnologias que aplicam decisões automatizadas por Inteligência Artificial e se mostram demasiadamente rebuscadas, quanto ao seu próprio texto que, por vezes, abre margem para perpetuar as situações de injusta discriminação, conforme será abordado no próximo tópico.

2.3 DECISÕES AUTOMATIZADAS NA LEI GERAL DE PROTEÇÃO DE DADOS DE ACORDO COM O ARTIGO 20 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Dos conceitos chave definidos pela Lei Geral de Proteção de Dados Pessoais, especialmente as definições de dado pessoal e de banco de dados merecem destaque, tendo em vista que ambas se relacionam diretamente com a viabilidade das decisões automatizadas, objeto do artigo 20 da lei e do presente trabalho. Tais definições estão elencadas em seu artigo quinto:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> [...]
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico [...] (BRASIL, 2018).

Desse modo, a letra da lei nos conta, a partir do termo “identificável” do inciso I, que para ser considerado como dado pessoal, não há necessidade de que ele promova a identificação direta da pessoa. Ou seja, o fato de determinada informação, ainda que isolada, poder ensejar a caracterização de seu titular, já torna essa informação um dado pessoal.

Como exemplo, podemos citar o endereço de e-mail. Esse endereço, por si só, pode não identificar a pessoa, mas quando cruzado com outras informações disponíveis, contribui para uma identificação completa e detalhada a respeito de quem o detém.

Em relação ao inciso IV, o que se depreende é que as disposições do diploma legal se estendem tanto aos bancos de dados físicos, não informatizados, quanto aos eletrônicos. Porém, tendo em vista que a discussão aqui proposta gira em torno de decisões automatizadas realizadas por inteligência artificial, não há que se falar, no presente trabalho, em bancos de dados físicos, apenas nos informatizados. A partir dessas duas conceituações, percebe-se que os bancos de dados, para existirem, dependem de uma matéria prima essencial: os dados pessoais. Assim, o que se observa é a relação estreita entre ambos os conceitos. Nesse viés, antes de prosseguir, faz-se pertinente compreender os motivos pelos quais os bancos de dados informatizados passaram a ocupar espaço relevante na discussão:

> O banco de dados informatizado, produto da tecnologia aplicada ao tratamento de informações pessoais, possui potencial antes inimaginável: é capaz de armazenar um grande volume de informações, de processá-las rapidamente, agregá-las e combiná-las dos mais diversos modos. em tempo irrisório se comparado com um tratamento manual - que muitas vezes sequer possível seria - funcionando como um elemento catalisador de um novo perfil de utilização de informação relevante a ponto de fazer com que grande parte das normas e procedimentos que foram produzidos sobre a matéria de dados logo acabasse por fazer referência direta ou até mesmo exclusiva aos bancos de dados como objeto a ser regulado. (DONEDA, 2021, p. 145).

Como visto, a partir da informatização dos bancos de dados, ações que antes jamais seriam viáveis se tornaram concretas. Nesse sentir, ao passo que tal tecnologia promoveu o avanço de processos responsáveis por ganhos exponenciais em certas atividades, inegavelmente, um lado danoso e que pode ser utilizado para maquinar ações mal-intencionadas – aqui se inclui a injusta discriminação – também passou a existir.

Assim, para uma melhor compreensão sobre como os bancos de dados informatizados podem funcionar impulsionando práticas lesivas às pessoas, faz-se necessário assimilar que, a partir da referida informatização, as informações antes dispersas e desconexas se tornaram informações organizadas, aptas a direcionar ações para o fim almejado por quem as detém (DONEDA, 2021).

Desse modo, levando em consideração a capacidade de organização e direcionamento que os bancos de dados automatizados possibilitam, os fins visados podem se traduzir em segregação por cor, raça, gênero e geolocalização por determinada empresa que pretenda alocar em determinado cargo apenas homens brancos que residam em bairros nobres, por exemplo. Desse modo, traçar o perfil

exato dos candidatos que pretende contratar se torna uma tarefa muito menos escancarada e árdua do que se a mesma seleção tivesse que ser feita a partir de bancos de dados não informatizados.

A partir da possibilidade técnica desses tipos de práticas e da verificação delas em casos reais, coube a lei garantir o amparo capaz de intervir e de atenuar esses possíveis tratamentos prejudiciais aos titulares dos dados pessoais.

Na Lei Geral de Proteção de Dados Pessoais, a atuação para redimir a incidência desses casos se traduziu no artigo 20 do texto legal, o qual prevê o seguinte:

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

Em sua grafia original, o texto do artigo 20 da lei previa que a revisão das decisões tomadas unicamente de maneira automatizada seria feita por uma pessoa natural. Entretanto, tal previsão foi vetada pelo presidente da república e substituída pelo texto vigente que, atualmente, assegura ao titular o direito de revisão, mas não prevê a obrigatoriedade de que ela seja feita por um humano. Desse modo, a necessidade de aprimoramento do referido artigo será apresentada no último capítulo do presente estudo.

Em que pese o espelhamento da lei brasileira na General Data Protection (EUROPEAN UNION, 2016), a qual dispõe de previsão sobre o tema no seu artigo de número 22:

> O titular dos dados tem o direito de não ficar sujeito a uma decisão baseada apenas no tratamento automatizado, incluindo a definição de perfis, que produza efeitos jurídicos sobre ele ou que o afete significativamente (EUROPEAN UNION, 2016, tradução nossa).

Denota-se, assim que o artigo 20 da nossa lei ainda se mostra frágil para combater satisfatoriamente situações de injusta discriminação passíveis de ocorrer no Brasil e se tornarem objeto de ajuizamento de ações judiciais, tendo em vista que, da maneira como se apresenta atualmente, apenas assegura uma revisão, sem se aprofundar sobre como a mesma deve ocorrer.

Nesse viés, os próximos tópicos se ocuparão de uma breve comparação entre o que está disposto na lei europeia e o que se definiu na lei brasileira sobre o tema. A partir de então, será possível conhecer as lacunas da Lei Geral de Proteção de Dados Pessoais que dificultam o combate às situações discriminatórias causadas pelo tratamento automatizado de dados pessoais e as consequências que tais ausências podem provocar na vida dos titulares de dados.

Assim, o primeiro ponto dissonante, e principal, entre as leis é que na General Data Protection o que se observa, é a consideração como premissa geral de que as decisões tomadas de maneira totalmente automatizada podem ocorrer apenas nas hipóteses previstas pela lei. Tal requisito legal europeu opõe-se diametralmente ao que se observa na Lei Geral de Proteção de Dados Pessoais, na qual não há menção sobre as ocasiões nas quais é permitida a aplicação de decisões totalmente automatizadas, mas apenas a garantia do direito do pedido de revisão pelo titular que se sentir lesado.

Não obstante, o considerando de número 71 da legislação europeia prevê que:

> Em todo o caso, esse tratamento deve estar sujeito a salvaguardas adequadas, que devem incluir informação específica ao titular dos dados e o direito de obter intervenção humana, para expressar o seu ponto de vista, para obter uma explicação sobre a decisão tomada após essa avaliação e contestar a decisão. (EUROPEAN UNION, 2016, tradução nossa).

Desse modo, o que se observa é a previsão clara, no referido considerando da General Data Protection Regulation, do direito dos titulares de solicitar uma revisão humana quando se sentirem lesados pelas decisões tomadas de maneira totalmente automatizada.

Ainda, no mesmo considerando da General Data Protection Regulation, fica previsto que os dados sensíveis, citados como “categorias especiais”, só podem ser objetos de decisões totalmente automatizadas em ocasiões específicas. E, como um terceiro ponto, consta a vedação expressa determinando a impossibilidade da tomada de decisão de maneira totalmente automatizada em relação aos dados pessoais de crianças na lei europeia.

O que se observa, portanto, é que a legislação europeia promoveu um detalhamento enriquecedor em seu diploma legal a fim de proteger os titulares de dados das nefastas consequências a que estão sujeitos os titulares quando da

atuação dos controladores e operadores munidos das tecnologias que possibilitam a aplicação de decisões totalmente automatizadas.

Essa proteção, por sua vez, se traduziu objetivamente na limitação das decisões totalmente automatizadas às hipóteses previstas na lei, na garantia de uma revisão humana a quem se sentir lesado e nas limitações impostas à aplicação de decisões totalmente automatizadas quando elas dizem a respeito de dados sensíveis ou de crianças.

A partir dessa sucinta análise a respeito das previsões garantidas pela Lei Europeia, fica evidente que, em relação ao tratamento unicamente automatizado de dados pessoais, a lei brasileira ainda se mostra pouco profunda e, portanto, atualmente, não se impõe como suficientemente capaz de proteger integralmente os titulares quando do tratamento de dados que se manifestam nas decisões tomadas de maneira totalmente automatizada.

Desse modo, apesar de a Lei Geral de Proteção de Dados Pessoais ter inaugurado uma nova fase no cenário nacional a respeito do respaldo legal sobre a proteção de dados pessoais, o que culminou na criação de uma lei específica para o tema, com definição de termos e fortes bases em princípios bem definidos, muito ainda precisa ser conquistado.

Nesse viés, um dos caminhos que cabe à lei percorrer, como já debatido, diz respeito às decisões automatizadas, objeto do artigo 20 da lei, o qual, por si só, abre as portas para um novo universo que compreende os algoritmos, a Inteligência Artificial, o Aprendizado de Máquina entre outros tantos conceitos e mecanismos utilizados na informática e que usam como insumo essencial os dados pessoais.

Portanto, o primeiro capítulo do presente trabalho se ocupou de tratar, de maneira breve, sobre as origens da privacidade e suas nuances ao longo da história, até ganhar relevância e se tornar um direito fundamental positivado, conforme pode ser observado na Constituição Federal Brasileira. Análises sucintas sobre as gerações de leis de proteção de dados pessoais em cenário mundial também foram trazidas, bem como, feitas ligeiras considerações a respeito das legislações esparsas no ordenamento jurídico brasileiro que, antes da Lei Geral de Proteção de Dados Pessoais, asseguravam alguns direitos aos titulares de dados pessoais.

A partir da compreensão do panorama histórico e contextualizador trazido no primeiro capítulo, forma-se a base para que seja possível compreender o cenário amplo no qual está situada a problemática que gira em torno dos aspectos técnicos

das tecnologias, a exemplo dos algoritmos, Inteligência Artificial e Aprendizado de Máquina.

Além disso, caberá ao segundo capítulo do presente trabalho mostrar como funciona a operacionalização dessas tecnologias e como sua presença constante no dia a dia dos indivíduos, por muitas vezes, acaba por violar os direitos dos usuários que, no caso brasileiro, dispõem de mecanismos legislativos ainda insuficientes para reivindicá-los. Por fim, serão discutidos casos de discriminação algorítmica ocorridos em empresas reconhecidas internacionalmente.

3 DECISÕES AUTOMATIZADAS, DISCRIMINAÇÃO ALGORÍTMICA E POTENCIAIS LESÕES AOS TITULARES DE DADOS

Neste capítulo, serão abordados os aspectos técnicos dos instrumentos tecnológicos que coletam constantemente os dados pessoais de seus usuários e aos quais a maior parte dos indivíduos se sujeita. Será possível compreender também como os algoritmos se tornam um valioso ativo das empresas que os detém e, por isso, são protegidos a todo custo. Além disso, os vieses pessoais incutidos na criação destes instrumentos, bem como, os argumentos que sustentam a desconstrução na crença da neutralidade das decisões tomadas por robôs serão trazidos para debate.

Por fim, serão analisados dois casos reais nos quais decisões totalmente automatizadas, tomadas com base em dados pessoais dos usuários, foram responsáveis por situações injustamente discriminatórias e, portanto, servem como base para alertar a necessidade de ações que coíbam a repetição de acontecimentos semelhantes no futuro.

3.1 HIPERCONECTIVIDADE

Na língua portuguesa, existem os prefixos de intensidade. Como exemplo, tem-se o prefixo Hiper, que, por transferência semântica, atribui o sentido figurado de alto grau a uma palavra posterior (SANDMANN, 1988). Sendo assim, quando se fala em hiperconectividade, estamos falando de conexão em demasia, com gradação aumentativa. Ainda, cabe destacar que doravante, no presente estudo, a conexão a qual nos referimos é aquela entre seres humanos e dispositivos eletrônicos, normalmente móveis e conectados à internet que, cada vez mais, compõem o dia a dia das pessoas.

Nesse viés, seis em cada dez norte-americanos assumem checar seus telefones a cada hora, e quase 10% deles acessam o aparelho a cada cinco minutos. Esses dispositivos acompanham seus proprietários no banheiro, na academia e, até mesmo, na cama (GOODMAN, 2018). Tais resultados demonstram, por si só, o quanto as tecnologias, principalmente os telefones móveis, fazem parte indissociável da vida de cada um e o quanto as pessoas estão hiper conectadas a esses dispositivos eletrônicos.

Assim, considerando a realidade delineada pelo autor do referido livro, tais evidências demonstram como se traduz, na prática, o significado do conceito “always on”, o qual pode ser entendido como o permanente acesso mantido entre indivíduo e dispositivo (MAGRANI, 2019).

Diante disso, você pode se questionar sobre qual seria a relação existente entre a hiperconectividade, o uso constante de smartphones e os dados pessoais, objeto do presente artigo. A resposta reside no fato de que os smartphones – e não apenas eles, como será visto adiante – representam um dos mais poderosos e constantes meios de captação de dados pessoais, o que é viabilizado, principalmente, por meio do uso dos aplicativos que fazem parte da rotina dos usuários, os quais estão sempre conectados.

Nesse viés, a coleta ininterrupta de dados por estes dispositivos, por sua vez, liga-se ao conceito “always recording”, termo utilizado para indicar o constante armazenamento dos dados que são produzidos durante o uso das aplicações (MAGRANI, 2019). Nesse sentido, cabe nos determos em uma das reflexões propostas por Gustavo Xavier de Camargo, o qual explica:

> A todo momento, em nossa vida diária, realizamos transações envolvendo dados pessoais. Ao utilizar uma aplicação de mapas, implicitamente vendemos nossos dados de localização; vendemos informações com nossos interesses imediatos quanto utilizamos um mecanismo de busca; vendemos nossa teia de relacionamentos, nossa imagem nas fotos, nossos interesses e nosso estado emocional quando utilizamos uma rede social. (CAMARGO, 2021, p. 101).

Desse modo, o que se observa é que tais aplicações são acessadas pelos usuários para atingir uma finalidade específica, mas, a partir de então, muitos outros desdobramentos ocorrem.

Como exemplo cotidiano, pode-se citar o ato de alguém que aciona um carro de aplicativo com o intuito de se deslocar ao local de trabalho ou para se locomover para os demais lugares que costuma frequentar diariamente. Para além de oferecer o serviço de transporte e satisfazer a necessidade momentânea do usuário, muitas vezes, as empresas mantém gravados os dados gerados por aquele usuário e, a partir de métricas, regras algorítmicas e cruzamentos tornam-se capazes de descobrir com precisão – utilizando para os mais diversos fins – não apenas o local de trabalho do usuário, mas também sua residência, círculo social, lojas e festas mais frequentadas por determinada pessoa, por exemplo.

A conduta de coletar dados e armazená-los para posterior tratamento, habitualmente encontra-se prevista nos termos de uso e políticas de privacidade dos aplicativos. Tais documentos, por sua vez, raramente são lidos ou compreendidos pelos usuários, quer seja pela própria falta de capacidade de compreensão acerca dos termos técnicos, pela extensão do conteúdo ou pela ânsia de fazer uso imediato do serviço oferecido.

Assim, desprovidas de qualquer análise crítica, milhões de pessoas diariamente aceitam longas páginas de conteúdo nas quais concedem poderes significativos em relação aos seus dados pessoais para que grandes empresas façam o uso que julgarem mais conveniente.

Para elucidar tal questão, podemos observar no pequeno trecho extraído da Política de Privacidade da rede social profissional denominada LinkedIn, a amplitude do poder concedido às empresas quando do aceite dos seus termos:

> Quando você visita ou deixa os nossos Serviços (incluindo alguns plugins e nossos cookies ou tecnologias semelhantes em sites de terceiros), recebemos a URL do site de onde você veio e a que visitará e a hora de sua visita. Também obtemos informações sobre sua rede e dispositivo (ex., endereço de IP, servidor proxy, sistema operacional, navegador e complementos, recursos e identificador de dispositivo, identificadores de cookies e/ou provedor de Internet ou operadora de celular). Ao usar nossos Serviços a partir de um dispositivo móvel, ele nos enviará informações sobre a sua localidade com base nas configurações do seu dispositivos. Pediremos que você habilite esse recurso antes de utilizarmos o GPS ou outras ferramentas para identificar precisamente a sua localidade (LINKEDIN, 2020).

Analisando o breve excerto destacado acima, torna-se evidente que, a partir do aceite do usuário aos termos dos aplicativos, as empresas interessadas passam a construir um vasto e valioso conhecimento gerado pela coleta ininterrupta e pelo posterior tratamento dos dados que foram coletados.

Com o passar do tempo, esse conhecimento se torna altamente ramificado, tendo em vista que, a depender dos casos, se estende para a página visitada antes e aquela vista depois pelo seu titular que, sem ter consciência plena sobre o que aceitou, continua sendo acompanhado de perto mesmo quando já esteja fazendo uso de outra aplicação.

3.2 ALGORITMOS, APRENDIZADO DE MÁQUINA E O VALOR DOS DADOS PESSOAIS

Considerando os conceitos e as práticas relacionadas aos dados pessoais debatidas no tópico anterior, torna-se indispensável compreender o funcionamento básico dos algoritmos, os quais se tornaram os verdadeiros responsáveis por tornar a mera coleta e armazenamento de dados algo expressivamente valioso.

Sendo assim, de maneira simplificada, os algoritmos podem ser explicados como a sequência lógica responsável por fornecer as instruções que devem ser tomadas visando a realização de determinada tarefa (MAGRANI, 2019). Desse modo, torna-se possível o aprendizado de máquina e, consequentemente, as empresas conseguem vislumbrar uma alternativa viável para a automatização dos processos de entregas de resultados cada vez mais satisfatória e ágil aos seus usuários.

Nesse viés, cabe esclarecer que uma razão importante que fez o buscador da Google ter um sucesso consideravelmente maior que o Yahoo, por exemplo, é a qualidade dos algoritmos desenvolvidos pela primeira empresa.

Ao considerarmos que, para os buscadores, cada clique que os usuários deixam de dar em determinada página pode significar uma oportunidade de venda perdida por aquele anunciante – o qual paga pelo espaço para promover a sua marca, um algoritmo altamente eficiente é fator fundamental para determinar o sucesso, ou não, de empresas como a Google, que vendem os espaços de anúncio para promover as marcas e produtos (DOMINGOS, 2017).

A partir de então, observa-se que, na maioria das vezes, os algoritmos acabam por se tornar extremamente valiosos e, quase sempre, passam a constituir o grande diferencial da empresa, a qual seria incapaz de exercer suas funções da mesma forma caso perdesse ou, por algum motivo, ficasse desprovida do algoritmo que utiliza. Por isso, conforme será melhor abordado ainda no presente capítulo, consideráveis são os esforços aplicados pelas corporações para mantê-los em segredo e distantes de quaisquer ameaças externas.

Como já mencionado anteriormente, cabe frisar que não são apenas os Smartphones os responsáveis por viabilizar a hiperconectividade contemporânea. Segundo Magrani (2019), para que a hiperconexão continue em expansão, faz-se

necessário o aumento do número de dispositivos diversos capazes de receber e enviar informações de maneira contínua.

Por isso, ao encontro de tal necessidade sugerida por Magrani (2019), atualmente observam-se altos investimentos direcionados aos dispositivos conhecidos como Internet das Coisas, por exemplo. Com a sua popularidade em alta, esses objetos vão desde os dispositivos vestíveis como os relógios inteligentes, passando pelo setor agrícola, solucionando problemas relacionados ao clima e, até mesmo, tornando realidade que uma pessoa possa esquentar o jantar, ligar as luzes e ajustar a temperatura de sua casa enquanto ainda está percorrendo o trajeto do trabalho para casa (MAGRANI, 2019). Tudo isso, possibilita que a base de dados dessas empresas se torne cada dia mais robustas e especializadas.

Até aqui, todo o desenvolvimento tecnológico construído ao longo das últimas décadas e que agora faz parte da vida diária das pessoas pode não parecer ofensivo. É comum o entendimento de que a coleta e armazenamento dos nossos dados tem como finalidade única e exclusiva o aperfeiçoamento dos serviços prestados pelas grandes empresas, as quais prometem entregar, cada vez mais, um tratamento personalizado aos seus usuários e a possibilidade de se usufruir de uma vida mais confortável.

Entretanto, faz-se imperiosa uma análise mais crítica a respeito do que nos é prometido e o que, de fato, acontece para além dos nossos olhos:

> Esses inúmeros dispositivos conectados, cada vez mais inteligentes e autônomos que nos acompanharão diária e constantemente em nossas rotinas, irão coletar, transmitir, armazenar e compartilhar uma quantidade enorme de dados, muitos deles estritamente particulares e mesmo íntimos. Com o aumento exponencial de utilização destes dispositivos, devemos estar atentos aos riscos que podem trazer para a privacidade e a segurança dos usuários. (MAGRANI, 2019, p. 25).

Torna-se evidente, então, que o ponto crucial colocado em risco diariamente é a privacidade dos indivíduos em seus aspectos mais particulares e sensíveis:

> Sempre que interagimos com um computador – seja o smartphone ou um servidor a milhares de quilômetros de distância – o fazemos em dois níveis. O primeiro é obter o que queremos: uma resposta, um produto para comprar, um novo cartão de crédito. O segundo nível, que em longo prazo é o mais importante, é ensinar ao computador quem somos. Quanto mais o ensinarmos, melhor ele poderá nos servir – ou nos manipular. (DOMINGOS, 2017, p. 187).

Entretanto, mesmo diante das evidências que alertam para o potencial manipulador e invasivo dessas tecnologias que coletam nossos dados pessoais constantemente, o que se vê, são os direitos, a muito custo conquistados ao longo das décadas, gradativamente sendo abdicados ou, o que é ainda pior, entregues por quem os detém sem que antes reflitam sobre a relevância desses dados tão valiosos.

Tal irrelevância atribuída aos dados pessoais pela grande maioria de seus titulares pode ser explicada, entre outros fatores, pelo fato de que o mercado de dados funciona como um monopsônio. Ou seja, ao contrário do monopólio ou oligopólio, no qual um ou poucos detém as vendas dos produtos que muitos almejam comprar, no monopsônio poucos são aqueles que pretendem comprar o que muitos têm disponível para oferecer (CAMARGO, 2021).

Desse modo, em se tratando especificamente dos dados pessoais, os principais interessados na sua aquisição são as grandes empresas de tecnologia mundiais como a Google e a Meta. Essas companhias detém o conhecimento e a estrutura necessários para armazenar e tratar dados pessoais na casa dos bilhões todos os dias, convertendo tal expertise em ganhos de performance que, posteriormente, são vendidos para outras empresas, proporcionando, então, exponenciais ganhos financeiros para o mundo corporativo como um todo.

Nesse ponto, é importante frisar que, na prática, os titulares não vendem, de fato, seus dados pessoais, como ocorreria em um monopsônio. Mas, no atual contexto, devido a falsa sensação coletiva de que os dados pessoais não possuem valor, as pessoas acabam por cedê-los sem qualquer contrapartida financeira.

Diante disso, as grandes empresas interessadas na obtenção dos dados, por sua vez, limitam-se ao oferecimento de entretenimento e de facilidades aos usuários, como é o caso das redes sociais Facebook, Instagram, LinkedIn, entre outras. Tais aplicações funcionam, por um lado, como a contrapartida pela cessão dos dados pessoais possibilitando que possamos nos entreter e buscar informações rapidamente, e, por outro lado, como um mecanismo que possibilita a permanente captação dos dados e mapeamento constante dos hábitos desenvolvidos pelos usuários que sequer tem consciência disso.

Considerando o breve panorama supracitado, fica evidente a falta de consciência a respeito do valor atribuído aos dados pessoais e sobre o que a sua disponibilidade de maneira inconsequente pode gerar. Portanto, convém mencionar,

nesse contexto, o pensamento de Edward Snowden, o qual sintetiza, em poucas linhas, uma analogia pertinente sobre a necessidade da devida compreensão e atribuição da relevância que o assunto merece:

> Argumentar que você não se importa com o direito à privacidade porque não tem nada a esconder não é diferente de falar que você não se importa com a liberdade de expressão porque não tem nada a dizer. (MAGRANI, 2019 apud SNOWDEN, 2019, p. 55).

O que se evidencia, então, é o estado coletivo de alienação ensejado pela falta de conhecimento sobre como, de fato, funciona o lucrativo negócio dos dados pessoais – viabilizado principalmente pelos algoritmos e pelo aprendizado de máquina – e como cada um de nós torna-se parte disso.

Assim, diante desse cenário, o que se observa é a necessidade de, gradativamente, se desconstruir a fiel crença das pessoas apenas no aspecto positivo das tecnologias. Atualmente, a narrativa repassada à massa é responsável por nutrir uma ânsia cada vez maior pela aquisição de aparelhos de última geração conectados à internet, os quais, quase sempre, fazem os consumidores enxergarem apenas a promessa da inserção de maior praticidade e conforto em sua vida cotidiana, tirando-lhes a capacidade de reflexão sobre o real impacto que tais dispositivos podem causar em suas vidas.

Para que seja possível seguir no caminho de combate à tal alienação, torna-se necessário o fomento da cultura em torno da temática da proteção de dados e, para ser efetiva, essa cultura deve a) ser promovida por estudos teóricos como o viabilizado pelo presente trabalho, possibilitando um maior entendimento a respeito de como se estruturam esses mecanismos e quais as suas reais intenções, a fim de que as pessoas consigam perceber e evitar as situações diárias que as colocam em riscos e b) possuir bases sólidas em leis bem construídas, as quais sejam capazes de suprimir as lacunas como a que se vê atualmente no artigo 20 da Lei Geral de Proteção de Dados Pessoais, objeto do presente estudo.

3.3 OS ALGORITMOS PODEM DISCRIMINAR INJUSTAMENTE?

Conforme abordado, a hiperconectividade está atrelada à constante sensação incutida nas pessoas de que é no ambiente virtual que a vida acontece. De certo

modo, de fato, hoje estamos reféns dos dispositivos móveis conectados à internet nas mais diversas situações do dia a dia. Como exemplo, pode-se citar os restaurantes nos quais o cardápio disponível é acessado unicamente por meio de QR Code, os eventos que vendem seus ingressos apenas em plataformas virtuais ou, ainda, os bancos que operam exclusivamente no meio digital.

Fato é, a necessidade prática aliada ao aspecto psicológico das pessoas, altamente voltado para a aderência massiva aos eletrônicos, constitui um caminho praticamente impossível de ser revertido. Diante disso e dos inegáveis ganhos em produtividade, praticidade e aproximação que as tecnologias proporcionam, urge a necessidade de reconhecimento e separação dos aspectos potencialmente danosos, daqueles que, de fato, agregam positivamente na vida dos usuários. A partir dessa identificação, torna-se possível traçar estratégias capazes de amenizar os impactos prejudiciais causados.

Nesse viés, um dos aspectos potencialmente danosos da tecnologia deriva, justamente, dos mecanismos de reprodução da inteligência humana por máquinas, área da ciência da computação conhecida como Inteligência Artificial. Portanto, faz-se pertinente conhecê-la desde a sua raiz, a partir da elucidação de seu conceito básico, traçando sua relação com os algoritmos já mencionados e, posteriormente, no terceiro capítulo, analisando seu deságue no esforço pela regulação legislativa dela no Brasil.

A Inteligência Artificial, apesar de invocada com maior frequência atualmente, tem suas raízes no século passado e, embora já tivesse passado por experimentos anteriores, foi no ano de 1955 que John McCarthy oficialmente cunhou o termo do referido campo de pesquisa (MCCARTHY, *et al.* 2006).

A partir de então, muitos foram os investimentos destinados à área e os adeptos que passaram a aplicar seus estudos para que as máquinas pudessem simular por conta própria a inteligência humana. Atualmente, a Inteligência Artificial pode ser compreendida como um campo amplo que engloba, entre outros, os Sistemas de Rede Neural Artificial, Inteligência de Enxame e o Aprendizado de Máquina. É em relação ao último campo, desenvolvido pela primeira vez em 1959, que nos deteremos doravante no presente estudo (DOMINGOS, 2017).

Conhecido como aprendizado de máquina, tal campo da Inteligência Artificial consiste na aptidão dos computadores para resolver uma tarefa proposta sem que tenham sido programados de maneira objetiva para tal. É por meio desse ramo da

inteligência artificial que opera a quase totalidade das decisões automatizadas baseadas em tratamento de dados pessoais. Isso porque, o aprendizado de máquina surge como a melhor alternativa diante da impossibilidade de se atender todos os usuários de maneira personalizada com a devida qualidade que as grandes empresas almejam atingir (DOMINGOS, 2017).

Portanto, diante da inviabilidade técnica de se redigir cada linha dos softwares incumbidos de conhecer o perfil dos clientes e entregar a eles boas sugestões alinhadas ao seu perfil, as empresas adotam a postura de acumular os dados ao máximo para, posteriormente, aplicar a esses bancos os algoritmos de aprendizado e, assim, deixar com que as decisões sejam tomadas e aperfeiçoadas de maneira autônoma (DOMINGOS, 2017).

Nesse viés, a alavanca fundamental do Aprendizado de Máquina está nos algoritmos, já tratados brevemente no tópico anterior, o qual podem ser definidos como:

> Uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa, ou seja, uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa. (MAGRANI, 2019, p. 19).

Uma vez compreendida a relação existente entre a Inteligência Artificial e os Algoritmos, é imperiosa a constatação de que, na última década, a popularidade desses mecanismos começou a ser difundida de maneira ainda mais contundente. Anos antes, todas as ações geradas por meio desses instrumentos matemáticos rapidamente foram aceitas pelas pessoas que ficavam entusiasmadas e veneravam o poder dos robôs, exaltando suas funcionalidades e, principalmente, julgando as decisões tomadas pelas máquinas essencialmente imparciais:

> Um programa de computador poderia vasculhar milhares de currículos ou pedidos de empréstimo em um segundo ou dois e ordená-los em listas impecáveis, com os candidatos mais promissores no topo. Isso não apenas economizava tempo, mas também era vendido como algo imparcial e objetivo. Afinal, não envolvia humanos preconceituosos cavoucando resmas de papel, apenas máquinas processando números frios. Por volta de 2010, a matemática impunha-se como nunca nas questões humanas, e o público amplamente a saudava (O'NEIL, 2021, p. 6).

Nesse viés, torna-se evidente que o uso dos algoritmos como instrumentos que potencializam o tratamento de milhões de dados pessoais de maneira

automatizada, possibilitando sua manipulação ordenada, foi um grande responsável pelo significativo valor comercial incorporado ao armazenamento e tratamento de dados.

Diante disso, “surgiram empresas que se especializaram em coletar e decifrar, de forma detalhada, a atividade dos usuários através da leitura de dados pessoais que eram coletados pela internet” (LINDOSO, 2021). Tais empresas visavam principalmente se valer da vantagem competitiva que o conhecimento sobre o público-alvo pode representar nos mais variados tipos de negócios.

Entretanto, não se pode olvidar que tais regras algorítmicas foram e continuam sendo definidas por seres humanos voltadas para a satisfação dos desejos de outros seres humanos – normalmente disfarçados pelas empresas ou instituições que representam. Assim, ao contrário da concepção tradicional de que as máquinas não reproduzem vieses ideológicos ou sustentam preferências baseadas em preconceitos, fica evidente que elas decidem com base no que lhes foi proposto pelos programadores. Tais proposições, por sua vez, podem, sim, conter os mais diversos vieses ideológicos.

Nesse sentido, torna-se imprescindível compreender que os vieses pessoais começam a ser incorporados aos instrumentos matemáticos que, posteriormente, passarão a decidir por si mesmos quando são definidos os dados de entrada dos algoritmos, ou seja, aquilo que é informado para ser interpretado e gerar uma resposta (O’NEIL, 2021).

Desse modo, como exemplo, pode-se considerar que, para elaboração de um algoritmo de análise de históricos para concessão de crédito, seria claramente injusto e potencialmente discriminatório utilizar como dado de entrada a raça das pessoas (O’NEIL, 2021).

A utilização de tal elemento como entrada na construção de um algoritmo poderia, no futuro, ocasionar decisões que bloqueassem crédito para pessoas a depender de sua cor, potencializando a crença de que tal elemento influencia na quitação de empréstimos no prazo previsto, e, portanto, pela cor, seria possível distinguir as pessoas honradas daquelas que não cumprem com os seus compromissos.

Quando nos debruçamos sobre o papel desempenhado pelos dados utilizados como entradas nos softwares, somos capazes de contestar a concepção de neutralidade dos instrumentos de decisão automática, pois há elementos claros

capazes de demonstrar que os algoritmos não são fruto de combinações puramente matemáticas e objetivas.

A parcialidade desses instrumentos emerge ainda mais fortemente quando eles passam a ser conectados aos robustos bancos de dados que lhes darão vida (JURNO; DALBEN, 2018). Isso se explica, pois os bancos de dados são previamente lapidados visando alguma finalidade – escolhe-se com quais tipos de dados se deseja trabalhar em uma seleção de colaboradores, por exemplo – e constituem elementos decisivos para a construção dos multifacetados vieses que integram as decisões automatizadas:

> Ao se trabalhar com algoritmos é preciso sempre ter em mente que eles são o resultado de complexas redes sociotécnicas, formadas por diversos atores humanos e não humanos, e que influenciam e participam da construção de sentidos dos usuários das plataformas em que eles trabalham (JURNO; DALBEN, 2018, p. 25).

Portanto, considerando que os desenvolvedores desses instrumentos podem ser orientados por concepções pré-estabelecidas e preconceitos mais ou menos enraizados, muitos são os episódios nos quais as máquinas decidem com base em critérios injustamente discriminatórios, tendo em vista que foram previamente direcionadas para tal. É por isso que a autora Cathy O'Neil costuma chamá-los de Algoritmos de Destruição em Massa (O'NEIL, 2021).

Não por coincidência, a discriminação promovida por essas máquinas atinge em maior grau os grupos historicamente minoritários como mulheres, homossexuais, pessoas negras e de baixa renda, justamente replicando os entraves já conhecidos pela sociedade e as ideias discriminatórias incutidas nas pessoas há séculos. Esse ponto será especificamente abordado nas subseções "Caso Decolar" e "Caso Google Fotos" do presente capítulo, nos quais serão tratados casos reais envolvendo o assunto.

Com efeito, outro ponto importante é a proporção e os impactos significativos que as tomadas de decisões automáticas feitas por algoritmos, baseadas nos dados de milhões de pessoas, podem gerar. Nesse viés, esses algoritmos amplamente difundidos acabam por desempenhar um poder próximo ao poder de lei (O'NEIL, 2021).

Isso significa dizer que, devido à massiva adesão pelas grandes instituições e empresas à aplicação de decisões automatizadas para liberação de crédito, seleção

de colaboradores e muitas outras aplicações que influenciam diretamente na vida das pessoas, todos estamos sujeitos às possíveis injustiças, sem que algo realmente efetivo possa ser feito para reverter a situação diante de uma negativa de crédito ou da não convocação para uma entrevista de emprego, por exemplo. Portanto, o rápido ganho de escala observado conserva incomensurável potencial de dano, tornando os algoritmos plenamente capazes de definir o destino da vida de uma pessoa (O'NEIL, 2021).

Além disso, a opacidade dos algoritmos é outro ponto que se coaduna com a perpetuação de decisões injustas. Como visto, os responsáveis pela elaboração das regras matemáticas são os únicos capazes de compreendê-las e editá-las. Ou ainda, nem mesmo seus criadores conseguem compreendê-los depois de um determinado estágio atingido. Aos usuários, por sua vez, jamais foi permitido identificar sob quais julgamentos estão sendo postos ou o peso que será atribuído às suas respostas em um formulário, por exemplo. Sendo assim, o candidato a uma vaga de emprego não saberá se, ao informar o bairro em que reside, pontuará positivamente, negativamente ou de maneira neutra naquela seleção.

> Quando os algoritmos ficam complicados demais para nossos pobres cérebros humanos entenderem, quando as interações entre as diferentes partes do algoritmo se dão em número muito grande e são muito complexas, erros começam a surgir, não conseguimos encontrá-los e corrigi-los e o algoritmo não faz o que queremos (DOMINGOS, 2017, p. 28).

Portanto, depreende-se que todos os algoritmos possuem elementos básicos em comum que, a depender de cada caso, são observados com maior ou menor intensidade nestes instrumentos decisórios. Tais elementos, por sua vez, são conhecidos como Dano, Escala e Opacidade, ambos sinteticamente discorridos acima (O'NEIL, 2021).

3.4 É POSSÍVEL AUDITAR OS ALGORITMOS?

Em relação aos três elementos característicos dessas tecnologias, principalmente a opacidade, um comum questionamento gira em torno de que, se os algoritmos apresentam todos esses riscos, em caso de denúncias, quais seriam os motivos pelos quais não se pode abrir seus códigos, investigá-los e obrigar seus

proprietários a corrigi-los – em caso de os vícios realmente se mostrarem presentes e lesivos?

A resposta encontra abrigo na defesa da propriedade intelectual e dos segredos de negócio. Na própria Lei Geral de Proteção de Dados, há previsão da necessidade de proteção do segredo comercial e industrial:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> [...]
> VI - transparência: 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).

Desse modo, tais previsões legais são poderosos argumentos comumente utilizados para defender empresas, especialmente as que dominam o mercado nacional e internacional, quando elas são acusadas de estarem reproduzindo situações de injusta discriminação por meio de decisões automatizadas:

> Muitas empresas se esforçam para esconder os resultados de seus modelos ou mesmo a existência deles. Uma justificativa comum é de que o algoritmo constitui um “molho secreto” crucial ao negócio. É propriedade intelectual, e deve ser defendida, caso necessário, com legiões de advogados e lobistas. No caso de gigantes da web como Google, Amazon e Facebook, esses algoritmos precisamente talhados valem sozinhos centenas de bilhões de dólares. As ADMs são, por projeto, caixas-pretas impenetráveis. Isso torna mais difícil ainda responder a segunda pergunta: o modelo funciona contra os interesses do sujeito? Em resumo, é injusto? Ele danifica ou destrói vidas? (O’NEIL, 2021, p. 29).

Diante da confidencialidade, por vezes exacerbada e má intencionada, depositada nesses instrumentos tecnológicos e defendida a todo custo pelas empresas que os possuem, o que se observa é a insuficiência da lei e dos agentes reguladores para penetrar e conhecer o que, de fato, existe por trás dos códigos.

Assim, conforme defendido por Lindoso, tendo em vista o atual cenário no qual somos cada vez mais controlados pelos que constroem conhecimento a partir dos dados pessoais, o viés emancipatório defendido pelos idealizadores das tecnologias sofre severos boicotes que contrariam a finalidade libertária inicialmente defendida por muitos (LINDOSO, 2021).

Um dos exemplos desse boicote que se choca com o ideal libertário foi a manipulação das eleições para a presidência dos Estados Unidos, promovida pela

Cambridge Analytica, no ano de 2016. Na ocasião, ficou comprovado que a referida empresa, por meio da coleta de dados pessoais de maneira ilícita, fazia a categorização de indivíduos e, a partir de então, trabalhava direcionando conteúdos – muitas vezes falsos – nas redes sociais com o objetivo de mudar a opinião dos eleitores, incentivando-os a votar em um ou em outro partido, conforme a intenção desejada por quem articulava a ferramenta (FORNASIER, 2020).

O que se vê, portanto, é que para além do controle de mercado, tais empresas passam, até mesmo, a exercer algo muito próximo de um poder político. A partir dessa constatação, observa-se, então, o significativo aumento na dificuldade de as legislações conseguirem controlar, de maneira efetiva, a exploração má intencionada dos dados pessoais promovidas pelas big techs, tendo em vista que tais empresas, na maioria das vezes, o fazem de modo parcial e injusto, unicamente visando satisfazer os desejos de quem as financia, sejam para finalidades éticas ou não.

Sendo assim, o que se observa é a urgente necessidade da criação de mecanismos legislativos que consigam, para além de garantir a preservação da propriedade intelectual das empresas, também proteger os usuários expostos às decisões automatizadas potencialmente lesivas as quais são submetidos diariamente.

Adiante, serão analisados dois casos específicos, Decolar.com e Google Fotos, respectivamente, nos quais o tratamento automatizado de dados pessoais da maneira e para a finalidade que foi utilizado, tornou-se responsável por gerar sérios danos aos titulares de dados usuários das aplicações mencionadas.

3.4.1 Caso Decolar

O primeiro dos casos sobre o qual trataremos se deu no âmbito do comércio eletrônico, segmento que, com o advento da pandemia de covid-19 teve, em 10 semanas, o mesmo percentual de crescimento que levou para atingir entre os anos de 2009 e 2019 (ATLÂNTICO, 2020).

No caso em questão, em 15 de agosto de 2016, a Agência de viagens Decolar.com, foi acusada e condenada pela prática de Geoblocking e o Geopricing em seu site de vendas. Tal atividade, foi responsável por desfavorecer, tanto pela impossibilidade de compra, quanto pelo aumento dos preços, milhares de

consumidores brasileiros, beneficiando aqueles que tentavam realizar as mesmas aquisições em outros países.

Desse modo, para que seja possível compreender no que consistem as referidas práticas, é imprescindível, primeiramente, assimilar como funcionam os mecanismos ora adotados pela empresa. Nesse sentido, o Geoblocking consiste em, por meio da análise de dados – localização espacial – e uso de algoritmos desenvolvidos para tal, bloquear anúncios de ofertas para pessoas que estejam em regiões pré-definidas pela companhia. Portanto, os que se encontram geograficamente localizados nos pontos determinados, sequer são capazes de visualizar as ofertas.

O Geopricing, por sua vez, consiste na prática de, por meio do conhecimento sobre a geolocalização do consumidor – viabilizado pelo tratamento de dados pessoais – atribuir preços distintos aos mesmos produtos oferecidos (FRAZÃO, 2018).

Diante dos fenômenos conhecidos como Geoblocking e Geopricing, torna-se evidente como, na prática, os mais variados dados pessoais se traduzem em informações com significativo valor de mercado, constituindo verdadeiros insumos viabilizadores do posicionamento estratégico das empresas em detrimento de alguns consumidores.

Ainda, outro elo que pode ser traçado a partir do caso em debate, é o de que, uma vez existindo potencial econômico a ser explorado, a alegada neutralidade algorítmica também perde suas bases, tendo em vista que, em tal contexto, as empresas privadas passam a ser guiadas pelos seus próprios interesses, os quais se sobrepõem aos princípios sociais pautados na justiça e nos preceitos éticos (LINDOSO, 2021). Assim, a nítida busca inconsequente pelo atingimento de interesses econômicos das grandes corporações deve, obrigatoriamente, ser moderada por legislações como a Lei Geral de Proteção de Dados Pessoais, a qual, por inexistir na época dos fatos, não pode ser invocada para apurar o caso e punir os responsáveis pelo acontecido.

Regressando ao caso em análise, as práticas adotadas pela Decolar.com evidenciaram que a diferenciação de preços e o impedimento da visualização das viagens ofertadas não se pautava em razões econômicas legítimas que justificassem tal discrepância – como seria o caso de custos logísticos adicionais para entrega do produto, por exemplo. Diante disso, a referida empresa foi multada

pelo Departamento de Proteção e Defesa do Consumidor em R$7,5 milhões, ficando obrigada a interromper imediatamente o funcionamento desses mecanismos sob pena de ter suas atividades suspensas e seu site retirado do ar (FRAZÃO, 2018). Posteriormente, a Secretaria Nacional do Consumidor reduziu a multa inicialmente aplicada para o valor de R$2,5 milhões de reais, o qual foi destinado ao Fundo de Defesa de Direitos Difusos (DECOLAR.COM..., 2022).

Na ocasião, tendo em vista que a Lei Geral de Proteção de Dados Pessoais ainda não se encontrava vigente, os principais dispositivos legais que embasaram a referida decisão foram o artigo 6º do Código de Defesa ao Consumidor, principalmente no ponto em que o mesmo prevê proteção contra métodos comerciais coercitivos ou desleais, bem como, o Artigo 39, inciso II do mesmo código, o qual veda a recusa do fornecedor ao atendimento à demanda do consumidor na medida de seus estoques – fato camuflado pelas práticas mantidas pela Decolar.com.

Considerando que a decisão em comento foi proferida antes da entrada em vigor da Lei Geral de Proteção de Dados Pessoais no Brasil, uma análise atual do caso requer, imprescindivelmente, o exercício de aplicação do caso em comento à lei de proteção de dados que dispomos atualmente a fim constatarmos se ela seria ou não eficiente para albergar satisfatoriamente a questão.

Em uma primeira análise sobre a Lei 13.709/2018, nota-se que os princípios da finalidade, prevenção e, principalmente, não discriminação poderia ser invocados em favor dos consumidores lesados pelo ocorrido:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> [...]
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> [...]
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos [...] (BRASIL, 2018).

Entretanto, tendo em vista que o presente caso se articulou essencialmente a partir do uso de mecanismos de inteligência artificial e decisões automatizadas, torna-se indispensável invocar o artigo 20 da atual Lei Geral de Proteção de Dados,

destinado a tratar objetivamente sobre o assunto e sobre o qual se debruça o presente estudo.

Nesse viés, a legislação atual assegura aos titulares de dados o direito de solicitar a revisão das decisões automatizadas baseadas em seus dados pessoais – como é o caso do Geoblocking e do Geopricing – executadas pelos algoritmos das companhias, quando o titular de dados se sentir lesado. Entretanto, a redação atual da lei não delimita de que modo tal revisão será realizada.

Portanto, baseadas na Lei Geral de Proteção de Dados Pessoais, empresas como a Decolar.com, ao serem contatadas pelos consumidores que entendem estar sendo prejudicados pelo tratamento automatizado de seus dados pessoais, podem, de acordo com o seu melhor entendimento e dada a falta de delimitação do artigo 20 da Lei Geral de Proteção de Dados Pessoais, designar tanto um robô, quanto uma pessoa natural, para fazer a revisão das decisões lesivas alegadas.

Nesse contexto, tendo em vista a convencionalidade prática e econômica de se designar um novo robô para realizar tal atividade, torna-se evidente o método que será preferencialmente adotado para atender os pedidos dos titulares direcionados às grandes companhias.

Sendo assim, no cenário em que um robô já realizou o tratamento de dados pessoais de forma lesiva, recorrer a outra máquina para executar a revisão de tal decisão coloca os titulares de dados pessoais em uma dupla sujeição ao erro, bem como, corrobora para a morosidade na resolução do caso e a perpetuação de práticas como as já ocorridas.

Portanto, embora os princípios e finalidades que legitimam o tratamento de dados pessoais sejam bem delimitados na Lei Geral de Proteção de Dados Pessoais, o que se constata é que a atual redação do artigo 20 da Lei, no ponto em que se omite em delimitar com clareza a necessidade de uma revisão das decisões automatizadas por pessoa natural, mostra-se falha e insuficiente para coibir práticas lesivas como as ocorridas, deixando o titular de dados à mercê de situações injustamente discriminatórias.

Não obstante, a atual redação do referido artigo contribui para a manutenção de ambientes discriminatórios de duas maneiras. Por um lado, faz com que a resolução das práticas discriminatórias já ocorridas se tornem, no mínimo, significativamente mais morosas e, por outro, como fator ainda mais grave, contribui para que outras novas situações de injusta discriminação surjam, tornando-se

responsável por possíveis novos danos causados a milhares de pessoas simultaneamente a cada dia.

3.4.2 Caso Google Fotos

O segundo caso em comento ocorreu no ano de 2015 e, portanto, também antes da promulgação da Lei Geral de Proteção de Dados no Brasil. Na oportunidade, a Google, gigante da tecnologia e a mesma empresa já citada durante o presente estudo mundialmente reconhecida pela robustez e qualidade de seus algoritmos, foi responsável por um perverso episódio racista ocasionado pelo tratamento automatizado de dados pessoais, o qual atingiu especificamente dois de seus usuários da aplicação Google Fotos.

O referido episódio teve como base a tecnologia do reconhecimento facial, a qual utiliza-se do Aprendizado de Máquina, já tratado no presente trabalho, para distinguir rostos em imagens e vídeos, agrupando-os em categorias como comidas, animais, familiares e similares em geral.

Na ocasião, após armazenar fotos suas e de sua companheira no referido sistema de armazenamento de fotos da Google, o usuário, Jacky Alciné, observou que elas haviam sido automaticamente direcionadas pela aplicação para uma pasta denominada “Gorilas”. Tanto Alciné, quanto sua companheira são pessoas negras. Após a constatação, o usuário se manifestou na rede social Twitter e, em poucos minutos, foi respondido pelo chefe de arquitetura social da Google, o qual desculpou em nome da companhia e evidenciou publicamente o comprometimento da empresa para resolver o problema (HARADA, 2015).

Entretanto, mais de dois anos após o ocorrido, para coibir a ocorrência de episódios similares, a empresa apenas tomou a ação de bloqueio em relação à palavra “Gorila” e outras potencialmente lesivas na referida aplicação. Não houve, no entanto, um trabalho direcionado da organização visando a correção dos vícios para tornar a ferramenta efetivamente prudente e confiável em relação ao tratamento e classificação de dados pessoais que realiza e, desse modo, segura para todos os seus usuários (WHEN..., 2018).

Atualmente, mais de sete anos após o lamentável episódio, a aplicação Google Fotos continua com o seu buscador desativado para a palavra “Gorila”. Tal atitude da Google perante a situação reforça a ideia defendida por Cathy O’Neil a

respeito da postura displicente, que normalmente as empresas adotam diante de casos de tal natureza:

> Sim, caso fique claro que sistemas automatizados estão errando de modo vergonhoso e sistemático, os programadores irão voltar atrás e ajustar os algoritmos. Mas na maior parte das vezes os programas entregam sentenças inflexíveis, e os seres humanos os utilizando dão de ombros como se dissessem, “bem, fazer o quê?”. (O’NEIL, 2021, p. 14).

Nesse viés, como já mencionado, o referido caso também ocorreu antes da vigência da Lei Geral de Proteção de Dados Pessoais, em um momento no qual o debate sobre a proteção de dados pessoais, principalmente no Brasil, não conservava o enfoque observado atualmente.

Por isso, seguindo o exemplo da primeira análise, nos deteremos em um exame a respeito das possíveis consequências e enquadramentos que o episódio teria dentro da legislação de proteção de dados atualmente vigente no país, bem como, analisaremos as disposições da própria Constituição Federal de 1988 sobre o assunto.

Nesse viés, diante do lamentável episódio ocorrido, sob a luz da Lei Geral de Proteção de Dados Pessoais, o primeiro ponto que deve ser destacado é o fato de tal episódio ter derivado do tratamento de dados pessoais sensíveis. Em seu artigo 5º, a Lei Geral de Proteção de Dados reserva espaço para discorrer sobre o significado do termo:

> 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 [...] (BRASIL, 2018).

Desse modo, constata-se que o reconhecimento facial que ensejou o ocorrido classifica-se como dado biométrico fazendo, portanto, parte do rol de dados pessoais sensíveis, sobre os quais o artigo 11 da Lei Geral de Proteção de Dados Pessoais se debruça e delimita as hipóteses de tratamento. A partir desse reconhecimento facial pela biometria, constatou-se, no caso em comento, sua classificação discriminatória com base na origem racial do titular dos dados.

Assim, tal episódio possibilita compreender que os dados pessoais sensíveis são classificados de tal maneira por conservarem potencial discriminatório intrínseco à sua própria natureza e, portanto, estão diretamente conectados ao princípio da não-discriminação, previsto no artigo 6º IX da Lei Geral de Proteção de Dados Pessoais, o qual baliza todo o diploma legal em torno da proteção de dados pessoais (LINDOSO, 2021).

Nesse viés, constata-se que, no caso em comento, o tratamento de dados pessoais sensíveis deu causa a um reprovável episódio racista e, quando comparado às lesões ocorridas no caso Decolar.com, por exemplo, o torna consideravelmente mais invasivo ao titular, ferindo direitos para além de seu aspecto patrimonial.

Sendo assim, se o ocorrido tivesse se dado no Brasil em plena vigência da Lei Geral de Proteção de Dados Pessoais, ficaria constatada a clara violação do princípio da não discriminação previsto na Lei Geral de Proteção de Dados Pessoais. Para além, seria constatada a quebra do direito fundamental posto no artigo 5º, inciso X, da Constituição Federal, o qual prevê a inviolabilidade da intimidade, da vida privada, da honra e imagem das pessoas, assegurando-lhes o direito a indenização em caso de violação.

Não obstante, no caso em comento, seria possível o enquadramento do ocorrido na hipótese prevista no atual artigo 20 da Lei Geral de Proteção de Dados Pessoais, sobre o qual se debruça o presente estudo, tendo em vista que a classificação por similares viabilizada pelo aplicativo da Google ocorre essencialmente baseada no tratamento automatizado de dados pessoais por Inteligência Artificial.

Nesse caso, tendo em vista que a falha relatada ocasionou constrangimento de ordem moral ao usuário, seria imprescindível, mais uma vez, que o titular de dados lesado pelo ocorrido estivesse amparado pela lei no sentido de poder contar com uma revisão feita por pessoa natural para revisar e buscar resolver o caso de maneira mais célere e digna.

Diante das questões de ordem técnica trazidas para debate no presente capítulo, torna-se possível compreender, a partir de uma visão macro, como cada cidadão que faz uso de dispositivos conectados à internet estão, em maior ou menor grau, sujeitos as adversidades que as decisões automatizadas com base em dados pessoais podem ocasionar na vida das pessoas. Além disso, os dois casos reais

supracitados, corroboram para evidenciar o potencial de dano conservado por tais instrumentos tecnológicos que se utilizam de decisões automatizadas baseadas em Inteligência Artificial.

Considerando tal cenário, o próximo capítulo se ocupará de elucidar os esforços de alguns países ao redor do globo, incluindo o Brasil, para tentar, com maior ou menor rigorosidade, instituir leis ou estruturar mecanismos para balizar a questão.

Conforme será visto, admitidas algumas exceções, na maioria dos casos, a alternativa encontrada para tal regulação reside na elaboração de cartilhas, relatórios, incentivo de pesquisas e estudos que estabeleçam princípios gerais para regular os desenvolvimentos dessas novas tecnologias as quais, diariamente, se integram na vida de milhões de novos usuários e podem impactá-los diretamente, muitas vezes de maneira severa.

4 O ATUAL CENÁRIO SOBRE A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL E PROPOSTA DE REFORMULAÇÃO DO ARTIGO 20 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Conforme abordado no primeiro e segundo capítulos do presente trabalho, a massiva coleta e armazenamento de dados pessoais está intrinsecamente conectada e tornou-se necessária para possibilitar os demais avanços da tecnologia. Nesse contexto, os mais diversos instrumentos tecnológicos tornam-se interdependentes e, para que sejam capazes de gerar resultados capazes de impactar, de alguma forma, no dia a dia das pessoas, eles se encaixam como peças de um quebra cabeça.

É por isso que leis como a Lei Geral de Proteção de Dados Pessoais trazem disposições a exemplo do seu artigo 20, não considerando os dados pessoais apenas de maneira isolada, como um fim em si mesmos, mas também levando em consideração o tratamento desses dados quando realizado por sistemas de Inteligência Artificial, em decisões automatizadas.

Nesse viés, conforme já elucidado anteriormente, a Inteligência Artificial, pode ser considerada a grande viabilizadora das decisões automatizadas justamente por conservar incomensurável potencial de criar uma vastidão de soluções baseadas em dados, as quais, não poderiam ser executadas com a devida personalização, rapidez e alcance exigidos no mundo contemporâneo, se não fosse pelas soluções de Inteligência Artificial. Sendo assim, ainda que a nossa atual Lei Geral de Proteção de Dados Pessoais abarque, em suas passagens, a hipótese de tratamento por Inteligência Artificial, o que se vê é, cada vez mais, a necessidade de diplomas legais específicos para tratar do tema com a profundidade que lhe é necessária. Por isso, muitas são as reflexões e esforços legislativos ao redor do mundo que giram em torno de regulação específicas sobre a Inteligência Artificial.

O objetivo principal desses movimentos regulatórios é traçar princípios e diretrizes gerais que imponham limites e sejam capazes de preservar os direitos humanos diante dos relevantes fatores de risco e impactos reais que podem ser observados pelo expressivo avanço tecnológico que, muitas vezes, nos dias de hoje, segue sem os devidos cuidados necessários.

Desse modo, a primeira parte do presente capítulo apresenta o cenário internacional sobre a regulação da Inteligência Artificial – discorrendo sobre os

principais apontamentos da Declaração de Montreal Pelo Desenvolvimento Responsável Da Inteligência Artificial, e do relatório desenvolvido pela Evidências Express – o qual apresenta o status do tema tratado em diversos países do mundo. Em relação a este último, serão analisados, especialmente, o cenário na União Europeia, Reino Unido, Estados Unidos e Japão. Após, será traçado um panorama sobre os projetos de lei referentes ao tema da regulação da Inteligência Artificial que tramitam no Senado brasileiro, bem como, breves serão feitos comentários a respeito da progressão do referido debate no país.

Por fim, serão tecidas considerações sobre como o texto do artigo 20 da Lei Geral de Proteção de Dados Pessoais deve ser ajustado para atender apropriadamente os titulares de dados, bem como, será considerada, e justificada, a necessidade da promulgação de uma lei específica para a regulação da Inteligência Artificial no país.

4.1 ESFORÇOS PARA A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO MUNDO

Nesse viés, em se tratando da Declaração de Montreal (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018) pela IA responsável, o documento foi desenvolvido em 2018 e possui forte base na opinião de especialistas com conhecimentos multidisciplinares e demais atores interessados no desenvolvimento das discussões a respeito do tema.

Ao longo de seu texto, é enfatizada a intenção de se estabelecer orientações mais amplas, as quais se traduziram em 10 princípios gerais. Em última análise, o objetivo do documento é fixar os limites éticos, visando mitigar os possíveis riscos para a sociedade e para o meio ambiente que podem vir a ocorrer na hipótese de os sistemas que se utilizam de Inteligência Artificial se desenvolverem sem qualquer base regulatória (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018).

Portanto, nos deteremos, pelas próximas linhas, na análise de cada um dos princípios trazidos no bojo da referida Declaração, elucidando o seu principal objetivo e, quando aplicável, apontando como cada um se relaciona mais diretamente ao conteúdo objeto do presente estudo, especialmente no que tange às situações discriminatórias e decisões automatizadas.

O primeiro deles, intitulado como Princípio do Bem-estar, destaca a necessidade de que os Sistemas de Inteligência Artificial não se tornem causadores de danos aos demais seres sencientes – não se limitando, portanto, apenas aos seres humanos, bem como, proíbe que tais instrumentos sejam utilizados como verdadeiros assediadores das pessoas no ambiente digital (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 8).

O Respeito à Autonomia é trazido no segundo princípio. Sua principal intenção é a de manter os seres humanos no controle de sua vida e do meio ambiente, sem que ele seja repassado aos Sistemas de Inteligência Artificial. Outro ponto relevante abarcado pelo princípio é a essencialidade de que as pessoas sejam devidamente capacitadas sobre as tecnologias digitais para que possam sempre exercitar o pensamento crítico nesse sentido (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 9).

O terceiro princípio visa a Proteção da Intimidade e da Vida Privada. Nesse sentido, determina-se que os Sistemas de Inteligência Artificial não podem ser projetados para violar a intimidade das pessoas, principalmente na intenção de criar rótulos ou proferir julgamentos morais com base naquilo que foi captado. Além disso, aborda-se a questão do pleno controle sobre os dados pessoais pelos seus titulares e a proibição de que, para serem utilizados, os SIA incitem a renúncia do titular aos direitos de propriedade sobre seus dados ou que criem perfis de preferências individuais para influenciar o comportamento do usuário (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 10).

No quarto princípio, nomeado como Princípio da Solidariedade, pode-se observar um importante elo com a questão central debatida ao longo presente trabalho, qual seja: a possibilidade de se direcionar as revisões solicitadas pelos titulares de dados que se sentiram lesados, prevista no artigo 20 da Lei Geral de Proteção de Dados Pessoais para serem executadas por novos robôs. Nesse sentido, o referido princípio menciona com clareza a necessidade de que os Sistemas de Inteligência Artificial não devem ser utilizados para substituir pessoas em tarefas que exigem relacionamento humano de qualidade (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 11).

O quinto princípio, intitulado de Princípio da Participação Democrática, aborda outro tema relevante e já debatido no presente estudo: a opacidade dos algoritmos. Fica claro, no documento, que os SIA responsáveis por proferir decisões que

impactam a vida das pessoas devem ser inteligíveis pelos desenvolvedores. Não obstante, quando solicitado, as máquinas devem ser capazes de oferecer justificativas semelhantes às que seriam fornecidas por um ser humano relacionadas ao que foi questionado (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 12).

O sexto princípio, nomeado como Princípio da Equidade, também aborda diretamente o cerne do presente estudo, visando proibir que as SIA reproduzam quaisquer tipos de discriminação, sejam sociais, sexuais, étnicas, culturais e religiosas ou outras (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 13).

O sétimo, intitulado como Princípio da Diversidade, determina que a manutenção da diversidade social, em seus mais amplos aspectos, não seja cerceada, nem que os Sistemas de Inteligência Artificial viabilizem a redução do espectro das escolhas oferecidas às pessoas (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 14).

O Princípio da Prudência, por sua vez, determina que qualquer Sistema de Inteligência Artificial deve apresentar alta confiabilidade, segurança e integridade sem colocar a segurança e qualidade de vida das pessoas em risco, devendo, portanto, serem realizados testes prévios à sua ampla disponibilização. Por fim, o princípio traz o dever de dar ampla publicidade aos erros e vulnerabilidades que sejam encontrados nos referidos sistemas (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 15).

O Princípio da Responsabilidade visa, como o próprio nome sugere, não eximir da responsabilidade aquelas pessoas que sejam responsáveis pelas decisões tomadas pelas máquinas (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p. 16).

O último princípio elencado na Declaração, conhecido como Princípio do Desenvolvimento Sustentável, traz, em linhas gerais, a necessidade de que os SIA avancem de maneira regulada, a fim de não prejudicar o meio ambiente (UNIVERSITÉ DE MONTRÉAL ET DU MONDE, 2018, p.17).

Não obstante, visando proporcionar uma visão mais ampla sobre como o tema vem sendo desenvolvido ao redor do globo, cabe trazer para o debate os resultados mostrados no relatório da Evidências Express, uma iniciativa da Diretoria de Altos Estudos da Escola Nacional de Administração Pública em parceria com a Universidade Federal de Brasília.

Trataremos, com base nas informações do referido documento, sobre como a questão vem sendo debatida na União Europeia, nos Estados Unidos e no Japão, de maneira a elucidar como tais países têm direcionado seus esforços no sentido de desenvolver suas legislações sobre o assunto (ENAP; EVIDÊNCIA EXPRESS, 2022).

De acordo com o referido relatório, na União Europeia, no ano de 2018, foi criada uma comissão para atuar na criação de estratégias para regulação e desenvolvimento da Inteligência Artificial, o que teve como resultado o Plano Coordenado para a Inteligência Artificial. Assim, para além das já recorrentes recomendações, como a proibição de seu uso com fins discriminatórios injustos, garantia de privacidade e proteção dos dados dos titulares, a comissão divulgou, no ano de 2020, os primeiros esboços de uma legislação propriamente ditam para regular a temática na União Europeia (ENAP; EVIDÊNCIA EXPRESS, 2022, p. 9).

Cabe destacar, aqui, que tal legislação se baseia, essencialmente, em três diferentes níveis de risco – risco inaceitável, risco elevado e risco baixo ou mínimo – com atribuição de sanções aplicáveis quando do infringimento de suas diretrizes, a depender do enquadramento em cada risco.

Nesse sentido, tendo em vista que, no presente estudo, nos detemos nas implicações geradas pelas decisões automatizadas pelas IA, merece destaque, por exemplo, o que é previsto para as soluções de gestão de trabalhadores – uso de software para triagem de currículos para processos de recrutamento.

Tais soluções foram classificadas, pela regulação Europeia proposta, na categoria de Alto Risco (ENAP; EVIDÊNCIA EXPRESS, 2022, p. 9). Ainda, aos fornecedores de soluções baseadas em IA que se enquadrem no nível “Alto Risco”, como é o caso das soluções de gestão de trabalhadores, serão impostas, entre outras, obrigações horizontais que devem, impreterivelmente, ser obedecidas: (i) Elaborar a documentação técnica do sistema de IA de risco elevado e (ii) Adotar as medidas corretivas necessárias, se o sistema de IA de risco elevado não estiverem em conformidade com os requisitos estabelecidos;

Portanto, de acordo com o breve panorama traçado, na União Europeia, os primeiros passos para a estruturação de uma lei específica, com obrigações horizontais aliadas às multas que serão previstas na legislação, irão configurar como medida importante para ensejar a lisura dos sistemas que se utilizam da Inteligência

Artificial, incentivando que eles sejam eficientes na mitigação dos riscos que apresentam.

Em se tratando do desenvolvimento do assunto na América, mais especificamente nos Estados Unidos, até meados de abril de 2023 o país possuía como principal norteador do assunto um guia geral para firmar os princípios que devem guiar o desenvolvimento da Inteligência Artificial. Tal documento não possuía força de lei e não objetivava se tornar uma, porém, estabelecia princípios gerais, dos quais dois deles merecem destaque, pois se coadunam com o tema aqui trabalhado: (i) Os usuários devem saber por que e como um sistema de IA fez sua determinação; (ii) As pessoas devem ter a opção de optar por não tomar decisões de IA e recorrer a um ser humano se o sistema apresentar um erro, falhar ou se elas quiserem contestar a decisão (ENAP; EVIDÊNCIA EXPRESS, 2022).

Nesse viés, considerando que os desenvolvimentos no campo da Inteligência Artificial, em sua maior parte, estão sob a direção do setor privado, consideráveis foram os esforços no sentido de se limitar qualquer regulação rigorosa que possa se tornar excessiva e prejudicar a posição dos EUA como vanguardista nos processos de inovação que se utilizam da Inteligência Artificial (ENAP; EVIDÊNCIA EXPRESS, 2022).

Entretanto, com o advento e rápida popularização do ChatGPT, Sistema de Inteligência Artificial rapidamente aclamado pelos usuários, o Senado dos EUA apresentou recentemente, em abril de 2023, movimentos voltados para o possível estabelecimento de regulações mais fortes relacionadas à questão. Nesse viés, conforme apontado por Chuck Schumer, líder do Senado, a intenção é conseguir evitar possíveis danos graves, por meio de medidas mais rígidas como, por exemplo, a prévia revisão dessas novas tecnologias por especialistas independentes, antes de serem lançadas no mercado (SHEPARDSON, 2023).

No Japão, país amplamente reconhecido pelo massivo uso de robôs, principalmente para automatização de seus processos industriais, a regulação da temática se dá, também, por meio de regulamentos e recomendações esparsas, as quais funcionam mais como orientações do que imposições legislativas e se diferem, em muito, da linha adotada pela União Europeia (ENAP; EVIDÊNCIA EXPRESS, 2022).

A intenção do governo japonês de regular a temática por meio de regulações menos rígidas pode ser entendida como uma medida para (i) não afetar, ou colocar

em risco, os investimentos aplicados no desenvolvimento das tecnologias em seu território e, assim, não cercear as iniciativas inovadoras, bem como, (ii) uma maneira relativamente eficiente de não eximir completamente país do debate regulatório.

Nesse sentido, cabe destacar que o Ministério Japonês da Economia, Comércio e Indústria publicou, em 2018, um documento no qual cita uma das principais questões debatidas no presente estudo: a necessidade de identificação do responsável legal quando do acontecimento de incidentes em sistemas de Inteligência Artificial (ENAP; EVIDÊNCIA EXPRESS, 2022).

Mais recentemente, no ano de 2021, o país desenvolveu a ideia de que que se deve, imprescindivelmente, sopesar os possíveis prejuízos causados e os inúmeros benefícios comprovadamente observados pelo desenvolvimento das soluções baseadas em Inteligência Artificial (ENAP; EVIDÊNCIA EXPRESS, 2022).

O referido documento aponta para a importância de, também, considerar as chances de gradativa diminuição dos riscos de falhas na medida em que as tecnologias se desenvolvem. Portanto, entendeu-se que travar o desenvolvimento por meio de regulações rígidas não se torna uma boa opção, tendo em vista que se torna capaz de prejudicar até mesmo o próprio aprimoramento das tecnologias.

Por fim, em sua conclusão, o relatório menciona que, a depender do setor, especialmente quando se tratar daqueles mais sensíveis, quando impactos severos nas vidas dos cidadãos poderão ser observados, as regulações devem estar sob o escopo das áreas responsáveis pelas leis de cada área.

4.2 ESFORÇOS PARA A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL

Em contexto nacional, torna-se importante considerar o papel não vanguardista do Brasil no desenvolvimento de soluções tecnológicas baseadas em Inteligência Artificial, quando comparado a países como os EUA, Japão e do continente europeu, já citados acima. Entretanto, embora não ocupe posição de destaque no desenvolvimento de tais tecnologias, na seara legislativa o país iniciou a discussão sobre o assunto ainda no ano de 2019.

Desse modo, há cerca de quatro anos, tramitam no senado brasileiro projetos de lei que visam instaurar a devida regulamentação legal sobre a temática com o intuito de instituir as balizas para orientar o enquadramento das referidas soluções

nos requisitos éticos, que respeitem, em primeiro lugar, os direitos humanos. Atualmente, são três os projetos de lei, 5051/2019, 872-2021 e 21-2020, ambos em tramitação que, em 16 de fevereiro de 2023 aguardavam despacho no Plenário do Senado Federal.

Portanto, no presente tópico, far-se-á uma análise sobre cada um destes projetos de lei citados, buscando enaltecer seus pontos de destaque, os quais podem corroborar para a efetivação dos avanços sobre a matéria. Além disso, se observada tal necessidade, serão tecidas críticas e sugestões de melhorias nos referidos textos.

A justificação de ambos os projetos prevê os sistemas de Inteligência Artificial como verdadeiros catalisadores dos avanços de produtividade e capazes de viabilizar ganhos financeiros expressivos na economia futura. Entretanto, todos eles também ponderam que diante das significativas mudanças já sentidas, as quais tendem a se intensificar com o passar do tempo, há grande necessidade de instauração de limites legais capazes de mitigar os impactos negativos aos quais os seres humanos poderão estar sujeitos.

Assim, o Projeto de Lei 5051/2019 (BRASIL; SENADO FEDERAL, 2019), de autoria do Senador Styvenson Valentim, em que pese seja breve e careça de maiores detalhamentos para que, de fato, venha a se tornar uma lei eficientemente aplicável, traz, em seu artigo segundo, duas disposições de extrema relevância para o tema, sendo que ambas conversam diretamente com a problemática trazida no presente estudo:

> Art. 2º A disciplina do uso da Inteligência Artificial no Brasil tem como fundamento o reconhecimento de que se trata de tecnologia desenvolvida para servir as pessoas com a finalidade de melhorar o bem-estar humano em geral, bem como:
> [...]
> IV – a transparência, a confiabilidade e a possibilidade de auditoria dos sistemas;
> V – a supervisão humana. (BRASIL; SENADO FEDERAL, 2019).

No artigo quarto do mesmo projeto, há outra disposição relevante, que dialoga com o artigo supracitado e merece comento:

> Art. 4º Os sistemas decisórios baseados em Inteligência Artificial serão, sempre, auxiliares à tomada de decisão humana.

> § 1º A forma de supervisão humana exigida será compatível com o tipo, a gravidade e as implicações da decisão submetida aos sistemas de Inteligência Artificial.
> § 2º A responsabilidade civil por danos decorrentes da utilização de sistemas de Inteligência Artificial será de seu supervisor. (BRASIL; SENADO FEDERAL, 2019).

Conforme apontado no primeiro parágrafo do referido artigo, alinhar os graus de supervisão humana com base no nível de gravidade das implicações passíveis de serem geradas pelos sistemas de Inteligência Artificial, mostra-se uma medida prudente para, de maneira justa e coerente, conferir maior ou menor necessidade da supervisão humana a tais instrumentos.

Além disso, conforme apontado no parágrafo segundo, atribuir a responsabilidade civil ao ser humano responsável pelo sistema que causou danos, constitui uma possível alternativa viável para que, finalmente, a indiferença das empresas que lucram com base em tais sistemas seja confrontada.

Isso porque, muitos são os casos em que, pela falta de clareza a respeito de quem seria responsabilizado pelos danos causados, tais organizações não dedicam os esforços que deveriam para evitar os problemas ou, se já ocorridos, buscar resolvê-los de maneira efetiva. Tal cenário, muito provavelmente mudaria se, conforme proposto pelo Projeto de Lei (BRASIL; SENADO FEDERAL, 2019) em comento, para cada Sistema de Inteligência Artificial, tivéssemos um ser humano responsável pelos erros dessas máquinas (O'NEIL, 2021).

Sobre o Projeto de Lei número 872/2021 (BRASIL; SENADO FEDERAL, 2021), de autoria do Senador Veneziano Vital do Rêgo, embora também seja sucinto e, ao nosso olhar, careça de maiores detalhamentos para regular a questão com propriedade, cabe destacar dois itens de seu artigo 4º que dialogam com o cerne da discussão do presente artigo:

> Art. 4º As soluções de Inteligência Artificial devem:
> [...]
> V – conter ferramentas de segurança e proteção que permitam a intervenção humana;
> VI – prover decisões rastreáveis e sem viés discriminatório ou preconceituoso [...] (BRASIL; SENADO FEDERAL, 2021).

Em se tratando do Projeto de Lei número 21/2020 (BRASIL; SENADO FEDERAL, 2020), nota-se, de início, a maior profundidade que ele carrega em seu conteúdo. Sendo assim, no segundo artigo encontra-se a definição sobre o que, nos

termos da lei, seria considerado um sistema de inteligência artificial, e o que estaria fora de tal classificação.

> Art. 2º Para os fins desta Lei, considera-se sistema de inteligência artificial o sistema baseado em processo computacional que, a partir de um conjunto de objetivos definidos por humanos, pode, por meio do processamento de dados e de informações, aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, fazendo predições, recomendações, classificações ou decisões, e que utiliza, sem a elas se limitar, técnicas como:
> I – sistemas de aprendizagem de máquina (machine learning), incluída aprendizagem supervisionada, não supervisionada e por reforço;
> II – sistemas baseados em conhecimento ou em lógica;
> III – abordagens estatísticas, inferência bayesiana, métodos de pesquisa e de otimização. (BRASIL; SENADO FEDERAL, 2020).

Mais adiante, em seu artigo terceiro, o referido projeto também deixa claro o objetivo de se promover a harmonização entre a futura lei de Regulação da Inteligência Artificial com diplomas legais já instituídos como, por exemplo, a Lei Geral de Proteção de Dados Pessoais, o Código de Defesa do Consumidor, Lei de defesa da Concorrência e Lei da Liberdade Econômica. Este ponto de necessária intersecção entre as leis será, justamente, debatido com centralidade no item 3.3 do presente artigo.

> Art. 3º A aplicação de inteligência artificial no Brasil tem por objetivo o desenvolvimento científico e tecnológico, bem como:
> [...]
> XV – a harmonização com as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), 12.965, de 23 de abril de 2014, 12.529, de 30 de novembro de 2011, 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e 12.527 de 18 de novembro de 2011. (BRASIL; SENADO FEDERAL, 2020).

Embora o Projeto de Lei número 21/2020 (BRASIL; SENADO FEDERAL, 2020), em muitos aspectos, se mostre capaz de abarcar pontos pertinentes para regulamentar a temática, cabe trazer para debate três dos apontamentos feitos por Bruno Bioni em sua participação Audiência Pública da Câmara dos Deputados sobre a Regulação do uso de inteligência artificial no Brasil, realizada em 30 de agosto de 2021.

Conforme apontado pelo especialista, um aprimoramento para o referido projeto seria a inserção, no rol de princípios já elencados no artigo 6º, dos princípios da prevenção e precaução. Além disso, a definição sobre quais seriam os requisitos

necessários para se definir tais tecnologias como de médio, alto e baixo risco, mostra-se essencial para um texto legal mais adequado (CIÊNCIA..., 2021).

Como último ponto de destaque, o apontamento de Bioni no sentido de se destinar, no bojo da lei, todo um capítulo relacionado ao poder público mostra-se indispensável. Isso porque, para além dos meros ditames legais, existe a necessidade de instauração de verdadeiras políticas públicas, com efetiva participação do Estado, a fim de que seja possível a aplicação e cumprimento efetivo de seus preceitos pela sociedade (CIÊNCIA..., 2021).

4.3 PROPOSTA DE REFORMULAÇÃO DO ARTIGO 20 DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Hoje estamos diante de um paradoxo no qual, de um lado, observa-se grande dificuldade de se compreender quais são, de fato, as implicações das novas tecnologias na vida cotidiana, e, de outro, a constatação de que apenas o saber pode não ser de grande ajuda, tendo em vista a escassez de meios para controlá-las dentro de uma perspectiva regulatória tradicional (DONEDA, 2021).

Sendo assim, diante de todo o exposto sobre o funcionamento dos algoritmos, especialmente tratados no segundo capítulo, considerando desde a coleta dos dados pessoais pelas organizações interessadas, a modelação dos bancos de dados formados para o atingimento de determinados fins, e, principalmente, os pesos atribuídos a cada resposta fornecida pelos titulares que, de alguma forma, pretendem obter resultados a partir do fornecimento de seus dados pessoais, torna-se fundamental alcançar o equilíbrio entre conhecimento e os mecanismos legais suficientes capazes de combater, na prática, as possíveis situações que exigem intervenção.

Desse modo, como uma das necessidades mais latentes para tornar os referidos instrumentos suficientemente seguros e respeitosos para com os direitos fundamentais das pessoas, consideramos indispensável o apoio subsidiário de um ser humano aos sistemas de Inteligência Artificial. Este apoio, por sua vez, para que seja efetivo e acarrete mudanças práticas na postura das empresas, fornecendo maior amparo aos titulares de dados, deve estar positivado na Lei Geral de Proteção de Dados Pessoais.

O papel principal desses seres humanos designados seria o de supervisionar a conformidade do trabalho dos robôs e, quando solicitado, revisar determinada escolha feita pelos sistemas, garantindo, então, que as decisões proferidas automaticamente, quando questionadas por quem se sentiu lesado, sejam minuciosamente revisadas.

Assim, em última análise, estaríamos diante de um mecanismo capaz de trazer mais segurança e conformidade com os direitos humanos para as decisões que hoje são tomadas com base no tratamento automatizado de milhões de dados pessoais diariamente, nos mais diversos setores.

Na Lei Geral de Proteção de Dados, para que tal mudança seja efetiva, ela deve ocorrer, especificamente, no artigo 20 da Lei Geral de Proteção de Dados Pessoais, o qual, de acordo com nossa sugestão, passaria a ter a seguinte redação:

> Art. 20. O titular dos dados tem direito a solicitar a revisão [por pessoa natural] 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).

Uma vez instaurada tal mudança no artigo supracitado, as empresas estariam impedidas de, conforme seu melhor entendimento, designar outros robôs para atender o direito de revisão das decisões automatizadas que se configurarem lesivas ao seu titular. Assim, embora singela, a modificação em apenas um artigo da lei seria capaz de trazer maior conformidade com o próprio parágrafo primeiro do mesmo artigo, o qual menciona:

> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. (BRASIL, 2018).

Entende-se, portanto, que o fornecimento de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, não pode ser confundido com o mero fornecimento de explicações – conforme aponta a atual redação do artigo 20, as quais podem se mostrar superficiais e incapazes de atender a pretensão do titular interessado, se forem executadas por outros Sistemas de Inteligência Artificial, por exemplo.

Outro ponto indiretamente combatido pelo aprimoramento do texto legal seria o da opacidade dos algoritmos. Isso porque, se considerarmos a obrigatoriedade do oferecimento de explicações elaboradas por um ser humano, necessariamente, tais decisões precisarão ser compreendidas pelas pessoas. Consequentemente, conforme disposto por O'Neil, as empresas não poderão mais dar de ombros dizendo "bem, fazer o quê?" diante da incompreensão sobre suas próprias criações (O'NEIL, 2021).

4.4 A NECESSIDADE DE PROMULGAÇÃO DE LEI ESPECÍFICA PARA SISTEMAS DE INTELIGÊNCIA ARTIFICIAL NO BRASIL

Diante do exposto a respeito da coleta ininterrupta de dados pessoais e seu posterior tratamento automatizado por meio de Sistemas de Inteligência Artificial, considerando que tais sistemas são previamente construídos e direcionados para o atingimentos de finalidades pré-definidas por quem os detém, entende-se que o pequeno ajuste no atual artigo 20 da Lei Geral de Proteção de Dados Pessoais proposto no item 3.3, inegavelmente, possibilitará maior amparo ao titular de dados que se sentir lesado pelas decisões tomadas de maneira totalmente automatizada.

Entretanto, não se pode deixar de considerar o amplo desenvolvimento dos Sistemas de Inteligência Artificial e a sua ramificação para os mais diversos setores da sociedade. Como exemplo de tal ramificação, temos os dispositivos vestíveis, os instrumentos utilizados na predição de dados pelo setor agrícola, soluções voltadas aos problemas relacionados ao clima e, até mesmo, a possibilidade de permitir que uma pessoa possa esquentar o jantar, ligar as luzes e ajustar a temperatura de sua casa enquanto ainda está percorrendo o trajeto do trabalho para casa, conforme está detalhado no segundo capítulo do presente estudo.

Neste caso, constata-se que o mero aprimoramento de um artigo de uma lei voltada especificamente para regular a questão dos dados pessoais, não se mostra plenamente capaz de suprir outras eventuais lacunas que podem surgir diante de tamanha revolução tecnológica proporcionada por sistemas que apresentam especificidades técnicas muito próprias.

Sendo assim, considerando o que já foi tratado no item Esforços para a regulação da Inteligência Artificial no mundo e Esforços para a regulação da Inteligência Artificial no Brasil do presente estudo, nos quais foram abordados os

esforços de países ao redor do mundo e do Brasil, no sentido de regular a Inteligência Artificial por meio de legislação específica, torna-se imperiosa a defesa de esforços contínuos para que, de fato, os projetos de lei em tramitação no Senado avancem rapidamente.

Assim, para que tal avanço seja possível, propõe-se a participação ativa dos parlamentares brasileiros em debates mundiais sobre o desenvolvimento ético da Inteligência Artificial, visando o aprimoramento dos projetos de lei que atualmente tramitam no Senado para que seja possível, finalmente, a promulgação de uma lei específica sobre o tem inspirada em posturas como as adotadas pela União Europeia, a qual já foi debatida no item 3.1 do presente estudo.

Além disso, tal diploma legal deve, baseado em uma das principais características da quarta geração de leis de proteção de dados pessoais, conforme já detalhado no primeiro capítulo deste trabalho, trazer a criação de uma autoridade independente para atuar na fiscalização e orientação sobre os padrões mínimos a serem observados pelos sistemas de Inteligência Artificial.

Deste modo, será possível assegurar uma proteção mais ampla e efetiva aos titulares de dados pessoais e usuários em geral que, diariamente, fazem uso desses inovadores e disruptivos sistemas.

Assim, uma vez alcançado tal estágio, teremos dado passos largos na direção de um futuro que não refute as tecnologias, nem impeça seu desenvolvimento, mas busque, ao máximo, contornar suas possíveis consequências negativas para a população.

5 CONSIDERAÇÕES FINAIS

Diante do exposto no estudo desenvolvido, foi possível compreender como a Lei Geral de Proteção de Dados Pessoais se entrelaça com as ascendentes novidades tecnológicas que se apresentam e são inseridas na sociedade a cada dia.

O tema mostrou-se socialmente relevante e atual, principalmente pelo fato de que, atualmente, conforme já elucidado, vivemos em uma espécie de Cyber panóptico. Tal analogia está fundada na constatação de um monitoramento em tempo real da vida cotidiana dos cidadãos e o posterior armazenamento eletrônico das informações depreendidas para viabilização de futuras análises robotizadas desses seres humanos, considerando-os como meros números inseridos em estatísticas, para o atingimento de um fim pretendido (LINDOSO, 2021).

Assim, debruçando-se sobre o recorte do artigo 20 da Lei Geral de Proteção de Dados Pessoais, o qual se destina a tratar das decisões automatizadas, tornou-se evidente sua íntima relação com os Sistemas de Inteligência Artificial, área relevante da tecnologia e especialmente abordada ao longo do segundo capítulo deste trabalho.

Deste modo, ao longo da pesquisa desenvolvida a respeito da proteção de dados pessoais sob o viés de decisões totalmente automatizadas tomadas por Sistemas de Inteligência Artificial, tornou-se evidente que o artigo 20 da Lei Geral de Proteção de Dados Pessoais, da maneira em que se encontra atualmente escrito no bojo da lei, sem delimitar com clareza que a revisão, quando solicitada, seja realizada por um ser humano, é responsável por sujeitar o titular de dados que tenha se sentido lesado e, por isso, solicitado revisão desta decisão, à uma nova situação potencialmente discriminatória. Além disso, com base na característica intrínseca dos sistemas de Inteligência Artificial, conhecida como Opacidade e detalhada ao longo do segundo capítulo, constatou-se que sua atual redação corrobora, também, para a falta de uma explicação clara sobre como determinada decisão foi tomada.

Diante de tal cenário, com base nas evidências de ordem técnica sobre a criação e funcionamento destas tecnologias, bem como, nos relatos de dois casos reais nos quais houve injusta discriminação advindas do tratamento automatizado de dados pessoais, evidenciou-se a emergente necessidade de retificação do artigo 20 da Lei Geral de Proteção de Dados Pessoais como medida que se impõe para que o problema levantado possa ser combatido.

Por fim, para que a Lei Geral de Proteção de Dados esteja amparada por uma lei mais robusta sobre o tema, quando a mesma for invocada para regular questões relacionadas ao tratamento de dados pessoais de forma totalmente automatizada, constatou-se que a promulgação de uma Lei específica para regular a temática da Inteligência Artificial no Brasil, seguindo o exemplo da União Europeia, e conforme já vem sido discutido no Senado Federal Brasileiro, é outra medida que se impõe para o atingimento de uma proteção integral dos indivíduos acerca deste tema.

Assim, a partir da implantação efetiva das medidas acima propostas, será possível, garantir um amparo mais efetivo da lei aos cidadãos que, diante das possíveis consequências danosas desses novos sistemas de Inteligência Artificial, a cada dia, se estão mais profundamente inseridos em um mundo dominado por Sistemas que, por vezes, têm o poder de tomar decisões capazes de impactar significativamente suas vidas.

REFERÊNCIAS

ANDRADE, Léo. Conexão bem-sucedida: Web 3.0 traz privacidade e inteligência artificial. **Exame**. [*S. l.*], 20 jun. 2022. Disponível em: https://exame.com/bussola/conexao-bem-sucedida-web-3-0-traz-privacidade-e-inteligencia-artificial/. Acesso em: 23 março 2023.

ATLÂNTICO. **Relatório de Transformação Digital na América Latina 2020**. [*S. l.*], 20 out. 2020. Disponível em: https://www.atlantico.vc/latin-america-digital-transformation-report-pt-2020. Acesso em: 5 maio 2023.

AZEVEDO, Aluísio. **O Cortiço**. 38. ed. São Paulo: Ática, 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 4 maio 2023.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 4 maio 2023.

BRASIL. **Lei nº 12.529, de 30 de novembro de 2011**. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica; altera a Lei nº 8.137, de 27 de dezembro de 1990, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e a Lei nº 7.347, de 24 de julho de 1985; revoga dispositivos da Lei nº 8.884, de 11 de junho de 1994, e a Lei nº 9.781, de 19 de janeiro de 1999; e dá outras providências. Brasília: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm. Acesso em: 4 maio 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 5 maio 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 maio 2023.

BRASIL. **Lei nº 13.874, de 20 de setembro de 2019**. Institui a Declaração de Direitos de Liberdade Econômica; estabelece garantias de livre mercado; altera as Leis nos 10.406, de 10 de janeiro de 2002 (Código Civil), 6.404, de 15 de dezembro de 1976, 11.598, de 3 de dezembro de 2007, 12.682, de 9 de julho de 2012, 6.015,

de 31 de dezembro de 1973, 10.522, de 19 de julho de 2002, 8.934, de 18 de novembro 1994, o Decreto-Lei nº 9.760, de 5 de setembro de 1946 e a Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943; revoga a Lei Delegada nº 4, de 26 de setembro de 1962, a Lei nº 11.887, de 24 de dezembro de 2008, e dispositivos do Decreto-Lei nº 73, de 21 de novembro de 1966; e dá outras providências. Brasília: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm. Acesso em: 4 maio 2023.

BRASIL. Senado Federal. **Projeto de Lei n° 21, de 2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Senado Federal, 2020. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9063365&ts=1677521675384&disposition=inline. Acesso em: 19 março 2023.

BRASIL. Senado Federal. **Projeto de Lei n° 872, de 2021**. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2021. Disponível em: https://legis.senado.leg.br/diarios/ver/106230?sequencia=44. Acesso em: 19 março 2023.

BRASIL. Senado Federal. **Projeto de Lei n° 5051, de 2019**. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília, câmara dos Deputados, 2019. Brasília: Senado Federal, 2019. Disponível em: https://legis.senado.leg.br/diarios/ver/101901?sequencia=142. Acesso em: 19 março 2023.

CAMARGO, Gustavo Xavier de. **Dados Pessoais, Vigilância e Controle**: Como proteger Direitos Fundamentais em um mundo dominado por plataformas digitais? Rio de Janeiro: Lumen Juris, 2021. *E-book.*

CIÊNCIA e Tecnologia - Regulação do uso de inteligência artificial (PL 21/20) - Bruno Bioni. Publicado pelo canal Data Privacy Brasil. [*S. l.*: *s. n.*], 2021. 1 vídeo (12 min). Disponível em: https://www.youtube.com/watch?v=lYRpo2D7XWI. Acesso em: 9 maio 2023.

DECOLAR.COM é multada em R$ 2,5 milhões por diferentes preços de mesmo produto. **Valor Investe**. São Paulo, 23 jun. 2022. Disponível em: https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2022/06/23/decolarcom-e-multada-em-r-25-milhoes-por-diferentes-precos-de-mesmo-produto.ghtml. Acesso em 07 de maio de 2023.

DOMINGOS, Pedro. **O algoritmo mestre**: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. São Paulo: Novatec, 2017. *E-book.*

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 2021.

ENAP. EVIDÊNCIA EXPRESS. **Regulação da Inteligência Artificial**: benchmarking de países selecionados. [*S. l.*]: Enap; Evidência Express, 2022. Disponível em: https://repositorio.enap.gov.br/bitstream/1/7419/1/2022.12.08%20-%20Regula%C3%

A7%C3%A3o%20da%20Intelig%C3%AAncia%20Artificial.pdf. Acesso em: 7 maio 2023.

FOUCALT, Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: Escândalo, Legado e Possíveis Futuros para a Democracia. **Revista Direito em Debate**, v. 29, n. 53, p. 182-195, 2020. DOI: https://doi.org/10.21527/2176-6622.2020.53.182-195. Disponível em: https://doi.org/10.21527/2176-6622.2020.53.182-195. Acesso em: 7 maio 2023.

FRAZÃO, Ana. Geopricing e geoblocking: as novas formas de discriminação de consumidores. **JOTA**. [*S. l.*], 15 ago. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/geopricing-e-geoblocking-as-novas-formas-de-discriminacao-de-consumidores-15082018. Acesso em: 7 maio 2023.

GOODMAN, Marc. **Future Crimes**: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. São Paulo: HSM, 2018.

HARADA, Eduardo. Fail épico: sistema do Google Fotos identifica pessoas negras como gorilas. **TecMundo**. [*S. l.*], 1 jul. 2015. Disponível em: https://www.tecmundo.com.br/google-fotos/82458-polemica-sistema-google-fotos-identifica-pessoas-negras-gorilas.htm. Acesso em: 25 mar. 2023.

HAKKERT, Ralph. **Fontes e dados demográficos**. Belo Horizonte: Associação Brasileira de Estudos Populacionais, 1996. Disponível em: http://www.abep.org.br/publicacoes/index.php/textos/article/view/2987. Acesso em: 8 maio 2023.

JURNO, Amanda Chevtchouk; DALBEN, Sílvia. Questões e apontamentos para o estudo de algoritmos. **Revista Parágrafo**, São Paulo, v. 6, n. 1, p. 17-29, jan./abr. 2018. Disponível em: https://revistaseletronicas.fiamfaam.br/index.php/recicofi/article/view/709. Acesso em: 8 maio 2023.

LINDOSO, Maria Cristine Branco. **Discriminação de gênero no tratamento automatizado de dados pessoais**: como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021.

LINKEDIN. **Política de Privacidade do LinkedIn**. [*S. l.*], 11 ago. 2020. Disponível em: https://br.linkedin.com/legal/privacy-policy. Acesso em: 7 maio 2023.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago, 2019.

MCCARTHY, John *et al.* A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. **AI Magazine**, v. 27, n. 4, p. 12-14, 2006. DOI: https://doi.org/10.1609/aimag.v27i4.1904. Disponível em:

https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904. Acesso em: 7 maio 2023.

O'NEIL, Cathy. **Algoritmos de Destruição em Massa**. Santo André: Rua do Sabão, 2021. *E-book*.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. [*S. l.*], 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 4 maio 2023.

PUCRS ONLINE. **Lei de Proteção de Dados (LGPD) do Brasil**. [*S. l.*], [202-]. Disponível em: https://online.pucrs.br/enm/lei-de-protecao-de-dados-lgpd-do-brasil. Acesso em: 29 nov. 2021.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Union: Official Journal of the European Union, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 7 maio 2023.

SANDMANN, Antônio José. **Formação de palavras no Português Brasileiro Contemporâneo**. Curitiba: Scientia et Labor; Ícone, 1988.

SHEPARDSON, David. Líder do Senado dos EUA pede regras para IA. **ISTOÉ**. [*S. l.*], 13 abr. 2023. Disponível em: https://www.istoedinheiro.com.br/lider-do-senado-dos/. Acesso em: 7 maio 2023.

UNIVERSITÉ DE MONTRÉAL ET DU MONDE. **Declaração de Montreal pelo desenvolvimento responsável da Inteligência Artificial**. [*S. l.*]: Université de Montréal et du monde, 2018. Disponível em: https://www.sbmac.org.br/wp-content/uploads/2021/02/Portugue%CC%82s-UdeM_Decl-IA-Resp_LA-Declaration_vf.pdf. Acesso em: 8 maio 2023.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, 1890. DOI: https://doi.org/10.2307/1321160. Disponível em: https://www.jstor.org/stable/1321160?seq=1. Acesso em 20 de março de 2023.

WHEN It Comes to Gorillas, Google Photos Remains Blind. **WIRED**. [*S. l.*], 11 jan. 2018. Disponível em: https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/. Acesso em: 7 maio 2023.