CENTRO UNIVERSITÁRIO DAS FACULDADES METROPOLITANAS UNIDAS

PROGRAMA DE MESTRADO EM DIREITO DA SOCIEDADE DA INFORMAÇÃO

DANIEL CESAR

# PRIVACIDADE E PROTEÇÃO DE DADOS: RISCOS IMPOSTOS PELO RECONHECIMENTO FACIAL E A DISCRIMINAÇÃO ALGORÍTMICA

SÃO PAULO

2022

DANIEL CESAR

# PRIVACIDADE E PROTEÇÃO DE DADOS: RISCOS IMPOSTOS PELO RECONHECIMENTO FACIAL E A DISCRIMINAÇÃO ALGORÍTMICA

Dissertação apresentada à Banca Examinadora do Centro Universitário das Faculdades Metropolitanas Unidas – FMU, como exigência parcial para obtenção do título de Mestre, sob orientação Professor Doutor Irineu Francisco Barreto Junior.

Área de Concentração: Teoria da relação jurídica na Sociedade da Informação

São Paulo

2022

DANIEL CESAR

# PRIVACIDADE E PROTEÇÃO DE DADOS: RISCOS IMPOSTOS PELO RECONHECIMENTO FACIAL E A DISCRIMINAÇÃO ALGORÍTMICA

Linha de pesquisa 1: Teoria da Relação Jurídica na Sociedade da Informação

Aprovado em: _____ de_____ de _____.

BANCA EXAMINADORA

_____

Prof. Dr. Irineu Francisco Barreto Junior

Centro Universitário das Faculdades Metropolitanas Unidas – FMU

_____

Prof. (a) Dr. (a)

_____

Prof. (a) Dr. (a)

## DEDICATÓRIA

Dedico esta pesquisa às minhas filhas, Helena e Luísa e à minha esposa Camila, razões para continuar nos momentos difíceis, sonhar e buscar por dias melhores, em um mundo melhor.

Para todos aqueles que sofreram e sofrem na pele, na carne e na mente o racismo, horrenda invenção humana que já deveria ter sido extirpada da face da terra.

## AGRADECIMENTOS

Agradeço a Deus, o autor da vida, que me trouxe com Sua graça, mesmo sem eu merecer, até aqui.

Aos meus pais, minha irmã, vocês são parte importante no que sou.

Às minhas filhas, Helena e Luísa, as razões da minha vida, não sei como passei tantos anos sem ter vocês, é um sentimento indescritível.

À minha esposa Camila, um anjo na minha vida, um exemplo, um porto seguro, de uma inteligência e de uma bondade que me inspiram.

Ao meu orientador, Professor Doutor Irineu Francisco Barreto Junior, um exemplo de docente, que tanto me ajudou e ajuda na caminhada acadêmica. Espero um dia ser um professor que inspire e que faça a diferença como o senhor tem feito na jornada de tantos de nós, seus alunos.

Ao programa de Mestrado em Direito da Sociedade da Informação do Centro Universitário das Faculdades Metropolitanas Unidas na figura do coordenador deste programa de mestrado, Professor Doutor Ricardo Libel Waldman, um programa excepcional o qual tive o privilégio de cursar e que transformou minha forma de ver este mundo tão conectado, com créditos e discussões essenciais sobre a Sociedade da Informação.

E a todos aqueles e aquelas que contribuíram na minha jornada de alguma forma.

Muito obrigado!

**RESUMO:** Esta dissertação foi redigida no âmbito da Linha de Pesquisa 1: Teoria da Relação Jurídica na Sociedade da Informação, do Programa de Mestrado em Direito da Sociedade da Informação do Centro Universitário das Faculdades Metropolitanas Unidas – SP. Situa-se no contexto das transformações sociais no qual dados possuem um valor alto, gerando serviços que conectam bilhões de pessoas ao redor do mundo, a chamada Sociedade da Informação. O cenário presente é de um mundo conectado com inúmeras facilidades trazidas pelas ferramentas de tecnologia da informação, banco, academia, biblioteca, shopping, nos comunicamos com qualquer lugar do mundo como se estivéssemos na mesma sala. Tudo isso gera um mercado bilionário, *big techs* se criaram, cresceram e são referências tendo como negócio o tratamento de dados. Contudo, somos uma sociedade complexa, temos questões históricas e bem atuais de discriminação a diferentes grupos, tratamentos e oportunidades totalmente dispares a depender da cor da pele, da condição econômica, de quem sexualmente você seja, por exemplo. Nesse contexto, tais visões podem ser trazidas aos modelos que executam os processamentos em nossa Sociedade da Informação, tornando os algoritmos, abstrações para resolução de problemas, discriminadores, perpetuando condições, privilégios, falta de oportunidades, mas com uma velocidade, abrangência muito maior, dado a capacidade de processamento e comunicação que as tecnologias da informação possuem e, se a Inteligência Artificial diz que é assim, então está certo, o que veremos, é uma falácia. Neste contexto de tecnologia, privacidade e proteção de dados pessoais e discriminação a grupos menorizados, focando aqui na questão racial, a pesquisa busca analisar esses pontos, trazendo a tecnologia do reconhecimento facial como objeto de estudo a fim de verificar como esse algoritmo pode causar a discriminação desses grupos e principalmente como podemos superar essas questões a fim de que as oportunidades e a conectividade tão marcante nesta Sociedade da Informação seja para com todos e não apenas para aqueles que já são, respeitando assim direitos e garantias basilares e esculpidos em nossa Constituição Federal. Esse é o objeto de estudo da presente pesquisa.

**PALAVRAS-CHAVE:** Sociedade da Informação; Privacidade; Proteção de Dados Pessoais; Discriminação; Reconhecimento Facial.

**ABSTRACT:** This dissertation was written within the scope of Line of Research 1: Theory of Legal Relation in the Information Society, of the Master's Program in Information Society Law at Centro Universitário das Faculdades Metropolitanas Unidas – SP. It is situated in the context of social transformations in which data has a high value, generating services that connect billions of people around the world, called Information Society. The current scenario is a world connected with countless facilities brought by information technology tools, bank, gym, library, shopping, we communicate with any place in the world as if we were in the same room. All this generates a billionaire market, big techs were created, grew and are references with data processing as a business. However, we are a complex society, we have historical and very current issues of discrimination against different groups, totally different treatments and opportunities depending on skin color, economic status, who sexually you are, for example. In this context, such visions can be brought to the models that perform the processing in our Information Society, making algorithms, abstractions for problem solving, discriminators, perpetuating conditions, privileges, lack of opportunities, but with a speed, much greater scope, given the processing and communication capacity that information technologies have and, if Artificial Intelligence says that it is so, then it is right, what we will see, it is a fallacy. In this context of technology, privacy and protection of personal data and discrimination against smaller groups, focusing here on the racial issue, the research seeks to analyze these points, bringing facial recognition technology as an object of study in order to verify how this algorithm can cause the discrimination against these groups and especially how can we overcome these issues so that the opportunities and connectivity so striking in this Information Society are for everyone and not just for those who already are, thus respecting basic rights and guarantees and carved in our Federal Constitution*. This is the object of study of this research.

**KEYWORDS**: Information Society; Privacy; Protection of Personal Data; Discrimination; Facial recognition.

## LISTA DE ILUSTRAÇÕES

Figura 1: Pontos nodais usados no mapeamento do rosto ..... 72

## LISTA DE TABELAS

Tabela 1: Definições de inteligência artificial ..... 49

Tabela 2: Taxonomia biométrica ..... 73

Tabela 3: Casos de vieses algoritmos ..... 76

# SUMÁRIO

**INTRODUÇÃO** ..... **10**

**1. PRIVACIDADE E PROTEÇÃO DE DADOS** ..... **15**

**1.1. BREVE HISTÓRICO DA PRIVACIDADE E PROTEÇÃO DE DADOS** ..... 15

**1.2. PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL** ..... 18

**1.3 OS AGENTES DE TRATAMENTO DE DADOS PESSOAIS** ..... 20

**1.4 OS PRINCÍPIOS DA LGPD** ..... 22

**1.5 DAS BASES LEGAIS PRESENTES NA LGPD** ..... 26

**1.6 APROFUNDANDO O LEGÍTIMO INTERESSE** ..... 30

**1.7 A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL** ..... 31

**2. DADOS PESSOAIS SENSÍVEIS** ..... **34**

**2.1 AS BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS** ..... 35

**3. BIG DATA, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS** ..... **38**

**4. O PRINCÍPIO DA NÃO DISCRIMINAÇÃO, UM OLHAR SOBRE ALGORITMO, INTELIGÊNCIA ARTIFICIAL E A ÉTICA** ..... **43**

**4.1 PRECONCEITO, DISCRIMINAÇÃO E RACISMO – PRINCÍPIO DA NÃO DISCRIMINAÇÃO** ..... 43

**4.2 ALGORITMO** ..... 48

**4.3 INTELIGÊNCIA ARTIFICIAL5** ..... 49

**4.4 UM ALGORITMO DISCRIMINA?** ..... 53

**4.5 UMA INTELIGÊNCIA ARTIFICIAL ÉTICA** ..... 59

**4.7 DIREÇÕES PARA O DESENVOLVIMENTO DE IA – CASOS BRASIL E EUROPA** ..... 67

**5. O RECONHECIMENTO FACIAL** ..... **70**

**5.1 VIESES EM PROCESSOS DE COLETA E RECONHECIMENTO** ..... 75

**5.2 O PRINCÍPIO DA PRECAUÇÃO APLICADO AO RECONHECIMENTO FACIAL** ..... 80

**5.3 O PERIGO DO OLHAR LOMBROSIANO E A FALÁCIA DA TECNOLOGIA NEUTRA** ..... 81

**CONSIDERAÇÕES FINAIS** ..... **84**

**REFERÊNCIAS** ..... **89**

## INTRODUÇÃO

O tratamento de dados pessoais e dados pessoais sensíveis foi disciplinado pela Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), visando trazer o titular para o controle de seus dados pessoais, assegurando-lhe direitos e resguardando suas garantias em um mundo hiperconectado.

Em relatório de janeiro de 2022, a DATAREPORTAL[1], estimou a população mundial em aproximadamente de 7,91 bilhões de pessoas, dessas, 5,31 bilhões acessam a internet apenas através de dispositivos móveis; em torno de 4,95 bilhões são usuários da internet e 4,62 bilhões são usuários ativos em redes sociais. Ocorreu um crescimento de 4% em relação ao ano de 2021 no número de usuários da internet, significando mais de 192 milhões de pessoas que passaram a utilizar a rede entre 2021 e 2022. No contexto do Brasil, houve um aumento de 3,3% na quantidade de usuários da internet representando mais de 5,3 milhões de internautas[2]. Dessa forma, cerca de 77% da população brasileira está conectada à Internet e o total de desconectados gira em torno de 49 milhões de pessoas.

Em termos de horas de acesso, o mesmo relatório traz que a média de uso da internet fica em 6h58min, significando um pequeno crescimento de 1%, ou mais 4 minutos, ao que se vinha utilizando na comparação com o relatório de 2021. O Brasil fica acima dessa média mundial, figurando em terceiro lugar, atrás somente da África do Sul e das Filipinas, com uma média de uso da internet em 10h19min, ou 42,99% do dia.

Na pesquisa realizada pelo Comitê Gestor da Internet no Brasil (2021) e consolidada através da TIC Domicílios de 2020, observa-se que 61,8 milhões dos domicílios brasileiros, o que representa 83% do total de domicílios, possuem internet. Em comparação ao relatório de 2019, houve um aumento de doze pontos percentuais, sendo tal movimento observado em todas as classes

---

[1] DATAREPORTAL. **DIGITAL 2022:** GLOBAL OVERVIEW REPORT. Disponível em: https://datareportal.com/reports/digital-2022-global-overview-report Acesso em: 09 abr. 2022.

[2] DATAREPORTAL. **DIGITAL 2022:** BRAZIL. Disponível em: https://datareportal.com/reports/digital-2022-brazil Acesso em: 09 abr. 2022.

sociais, mas de forma mais visível na classe C, saindo de 80% e atingindo 91% e na classe D/E, passando de 50% para 64% (Cetic.BR, 2021, p. 27).

Esses números dão a dimensão do universo de pessoas que fazem uso da internet e do tempo dedicado por elas em atividades na rede. Todos esses acessos geram pegadas digitais, trilhas da utilização da internet em seus diferentes serviços, o que em um contexto de Sociedade da Informação, deu origem a um novo segmento de negócio voltado à vigilância e tratamento de dados, movimento que a autora Shoshana Zuboff chama de capitalismo de vigilância[3] (2020).

Dentro deste cenário, pretendemos através da presente pesquisa, analisar se a alimentação dos modelos computacionais (Big Data, Inteligência artificial e outros) gerará algoritmos que vão propagar a discriminação, agora de forma muito mais otimizada, veloz e de maior alcance. Será possível compreender tais processos? A opacidade dos modelos desconectará ainda mais os vulnerabilizados pela sociedade que tem como ponto central a conexão? Quais são os caminhos que podem ser adotados visando a evolução tecnológica, afastando-se a discriminação, a fim de que esta ferramenta seja boa não só para os já privilegiados, mas para aqueles que são mais necessitados? Em uma sociedade onde dia após dia se assiste a mais pessoas mortas e excluídas apenas pela cor de sua pele e/ou condição social, é importante observar como a Sociedade da Informação, que tem esse "passivo analógico" trabalha o tema e pensar o que faremos daqui para frente, observando a questão do reconhecimento facial e a discriminação algorítmica no recorte desta pesquisa.

Como metodologia aplicada temos a pesquisa exploratória e bibliográfica, trazendo para a análise o Direito, a Tecnologia e a Sociologia, a fim de dialogar

[3] O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturando em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde (ZUBOFF, 2020, p. 18).

em busca de uma melhor compreensão e vislumbre de caminhos a serem adotados.

A problemática abordada na pesquisa compreende o referencial teórico de Castells (2020, p. 124), que conceitua a nossa comunidade como uma sociedade em rede, onde a informação é a matéria prima. Além dessa característica, traz ainda a penetrabilidade das novas tecnologias, a implementação da lógica das redes e com isso das interações, a flexibilidade que possibilita transformar, readequar, remodelar as características dessa sociedade e a convergência, interdependência das tecnologias, gerando um sistema altamente integrado.

Nesse contexto, a tecnologia da informação tem um papel fundamental viabilizando as mudanças na sociedade e retroalimentando o fluxo de evoluções, desenvolvendo novas formas de utilização dos dados que poderão ou não replicar o padrão discriminatório que temos. Paradoxalmente, vivemos em um mundo desigual, em que características como raça, etnia, classe, sexualidade determinam muito mais do que o acesso a oportunidades, mas definem lugares ou papéis sociais (ALMEIDA, 2019).

A proximidade de um indivíduo com o “padrão” de sujeito universal referido por Kilomba (2019) - homem, branco, hétero, se reflete em privilégios estruturais, por vezes sequer percebidos por quem os usufrui. Um exemplo são as abordagens policiais, estatisticamente diferenciadas a depender de marcadores como a raça e classe.

No polo oposto estão marcantes desvantagens. Sabe-se que a escravidão e os mecanismos desenvolvidos pelo racismo ao longo dos tempos, limitaram e segregaram pessoas negras no decorrer da história (ALMEIDA, 2019). Nessa perspectiva, a adoção de tecnologias que otimizem o tratamento de dados é algo que acende um sinal de alerta.

Para abordar esses desafios, o trabalho está desenvolvido conforme os capítulos a seguir.

O primeiro capítulo apresenta uma visão histórica da privacidade e proteção de dados, com o intuito de mostrar os caminhos que nos conduziram ao cenário e estrutura atuais, revelando que o tema há algumas décadas é objeto de estudos, legislações, resoluções e decisões de Tribunais internacionais, caminhando até a realidade brasileira atual de privacidade e proteção de dados. O nascimento da Lei Geral de Proteção de Dados, e antes ainda, com o próprio Marco Civil da Internet e a Lei do Cadastro Positivo, que trouxeram uma abordagem não tão aprofundada quanto a LGPD, mas de alguma forma discorriam sobre o direito dos titulares com relação a dados pessoais. Esse capítulo perpassa por pontos importantes da lei, como os princípios e bases que dão a sustentação para sua interpretação e para os tratamentos que serão realizados com os dados pessoais, encerrando com a recente ascensão da proteção de dados pessoais como um direito fundamental e o que isso significa.

O segundo capítulo aborda de forma mais detalhada os dados pessoais sensíveis, que como veremos, foram alvo de maior cuidado por parte do legislador em relação aos tratamentos possíveis em razão do poder de impacto sobre as garantias e direitos dos titulares.

O terceiro capítulo passa pela tecnologia Big Data, abordando sua importância no processamento e cruzamento de grandes volumes de dados a fim de gerar valor através das “descobertas” que tais cruzamentos podem trazer, com forte impacto sobre o dia a dia das pessoas. Nesse capítulo abordarmos alguns exemplos do uso de Big Data.

O quarto capítulo trabalha o princípio da não discriminação, conceituando preconceito, discriminação, racismo e seus tipos. Em uma sociedade marcada por desigualdades, injustiças provenientes de questões raciais, religiosas, étnicas, sexuais, de saúde, a discriminação migra do contexto “analógico” para o digital, não sendo assim algo da Sociedade da Informação, mas com forte potencial de força na sociedade como um todo. É inevitável assim abordar o contexto digital de algoritmo, processos, modelos, que tanto impactam a sociedade atual, explicitando ainda neste capítulo o que é um algoritmo, o contexto não computacional para o computacional, inserindo o quão discriminatórios esses algoritmos podem ser, com exemplos que ilustram isso.

Dado o problema, são analisadas, ainda, quais linhas podem ser adotadas a fim de trazer a ética ao processamento dos dados nos modelos de inteligência artificial, trazendo algumas ideias práticas.

Por fim, o quinto capítulo aborda o reconhecimento facial, sua definição e tipos, forma de execução, a importância para uma Sociedade da Informação e os impactos aos titulares, com o ressurgimento da antiga ideia lombrosiana, tão perigosas de características físicas com maior propensão ao cometimento de crimes com a visão de que a tecnologia é neutra.

# 1 PRIVACIDADE E PROTEÇÃO DE DADOS

Este capítulo tem a intenção de dar uma visão histórica sobre a privacidade e proteção de dados, mostrar as origens e o desenvolvimento deste assunto nas últimas décadas, até culminar nos nossos dias atuais e a publicação da Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro, adentrando nesta lei, trazendo pontos importantes para o contexto deste trabalho.

## 1.1 BREVE HISTÓRICO DA PRIVACIDADE E PROTEÇÃO DE DADOS

A privacidade e proteção de dados pessoais são temas discutidos há algumas décadas. A Lei de Proteção de Dados do *Land* alemão de Hesse*,* de 1970, é identificado como o primeiro diploma normativo que trata especificamente dessa matéria. Após esse marco, surgiram outras leis que começaram a abordar o tema da proteção de dados pessoais, tais como a lei sueca (*Datalagen*), a lei francesa de proteção de dados de 1978 (*Informatique et Libertées*) e movimento realizado pelo Tribunal Constitucional alemão, que em 1983 deu um significativo passo ao direito da proteção de dados ao reconhecer a garantia constitucional diante da lei federal do censo de 1982 (DONEDA, 2021, p. 27).

Os dados pessoais também foram utilizados pela máquina de morte nazista para identificação dos grupos que eram caçados e enviados aos campos de concentração.

> A coleta de dados dos cidadãos judeus, ciganos, deficientes e homossexuais realizada pelos nazistas foi o que tornou o Holocausto possível e cruelmente eficiente. Na sequência da Segunda Guerra Mundial e entrando na era digital, os legisladores na Europa garantiram que as leis de dados fossem rigorosas a fim de impedir que algo assim acontecesse de novo. A privacidade em relação à informação era, de fato, um princípio inerente da União Europeia — regras claras limitavam a capacidade de um sujeito desonesto cometer algum abuso quanto aos dados e violar direitos humanos (KAISER, 2020, posição 1970).

A coleta de dados se mostrou de grande importância para aprimorar a eficiência nazista na eliminação de judeus, ciganos, pessoas com deficiência e homossexuais, comprovando a relevância que a proteção de dados tem e o motivo pelo qual ações legislativas relacionadas a privacidade e proteção de dados pessoais vêm ocorrendo na Europa há algumas décadas.

A privacidade é vista muitas vezes como uma *porta de acesso* a outros direitos, incluindo o direito à igualdade e não discriminação, liberdade de expressão e de reunião, isso tanto no *online* quanto no *offline*, mas ela possui valor por si só, sendo essencial para o desenvolvimento da personalidade e proteção da dignidade humana. A privacidade permite limitar quem tem acesso aos nossos corpos, lugares e coisas, assim como nossas comunicações e nossas informações[4].

Logo no pós-guerra, com a criação da Organização das Nações Unidas (ONU), houve a concepção da Declaração Universal dos Direitos Humanos (DUDH) que em 1948 em seu artigo 12 estabeleceu:

> Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948, on-line).

Anos depois, a Sociedade da Informação modificou a forma como interagimos, mas a privacidade e proteção de dados continuam sendo temas da ordem do dia, motivando a proliferação de legislações de Privacidade e Proteção de Dados por diferentes países, saindo das fronteiras europeias e ganhando contornos globais.

> A partir das suas raízes fortemente vinculadas a uma tradição referente ao direito à privacidade e, de forma geral, ao fortalecimento dos direitos individuais, a proteção de dados pessoais começou a se estruturar com maior autonomia no momento em que o processamento automatizado de dados passou a representar, por si só, um fator de risco para o indivíduo.
>
> De fato, o aumento exponencial no volume, na intensidade e mesmo na complexidade nos tratamentos de dados pessoais desde a

[4] OLMA. Artigo 12: Direito à privacidade. Disponível em: https://olma.org.br/2018/11/29/artigo-12-direito-a-privacidade. Acesso em: 23 jun. 2021.

> fundação da disciplina fez com que ela fosse, constantemente, incorporando novos elementos para garantir a tutela integral da pessoa. Assim, desde um primeiro momento no qual a regulação e o controle direto dos então poucos bancos de dados pessoais foi viável, passou-se ao fortalecimento dos instrumentos de garantias individuais, necessárias diante da multiplicação desses bancos de dados. (DONEDA, 2021, p. 22)

Nesse processo de desenvolvimento da privacidade e proteção de dados pessoais, destacam-se dois documentos dos quais se deduziram princípios que até hoje figuram em legislações de privacidade, como é o caso da nossa Lei Geral de Proteção de Dados (LGPD): a Convenção da Europa de 28 de janeiro de 1981, que tem como foco a proteção das pessoas em relação às coletas automáticas de dados de caráter pessoal e a Recomendação da OCDE de 23 de setembro de 1980, que possui diretrizes para proteção da vida privada e a circulação transnacional de dados pessoais. Nessa junção, é possível observar os princípios da correção, da exatidão, da finalidade, da publicidade, do acesso individual e da segurança física e lógica da coletânea de dados (RODOTÁ, 2008, p. 59).

Com a passagem do tempo houve no contexto europeu um movimento de regulação detalhada mediante atos normativos da União Europeia, mas apenas em 2018 entrou em vigor o novo Regulamento Geral de Proteção de Dados da Europa (RGPDE), que reconheceu e concretizou o direito fundamental previsto na Carta de Direito Fundamental da União Europeia (CDFUE), e que também, em grande medida, fez com que fosse autoaplicável, vinculando direta e imediatamente todos os seus integrantes (SARLET, 2021, p. 41).

Tal movimento trouxe em 2018 a privacidade e proteção de dados pessoais para o ordenamento jurídico brasileiro, com a aprovação da Lei 13.709/2018, chamada de Lei Geral de Proteção de Dados (LGPD).

## 1.2 PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL

Passado o contexto geral, onde verificamos que em 1970 começaram a surgir os primeiros diplomas explicitando a privacidade e proteção de dados pessoais, no Brasil tivemos a edição da LGPD que tratou do assunto, entrando em vigor em 2020 e totalmente em 2021. Nesta seção abordaremos a LGPD, aprofundando em alguns pontos sensíveis ao seu entendimento e prática, como princípios, bases legais e os papéis dos agentes de tratamento.

A Lei 13.709/2018 (Lei Geral de Proteção de Dados) trouxe a privacidade e proteção de dados pessoais para a legislação brasileira. Segundo Patrícia Peck Pinheiro (2020, p. 16)

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis.

A lei foi aprovada em 2018 e passada a *vacatio legis*, entrou em vigor em agosto de 2020, sendo que a parte das penalidades começou a viger em agosto de 2021. Em seu primeiro artigo, a lei define seu objetivo.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018)

A Lei Geral de Proteção de Dados (LGPD) regula uma lista de ações de tratamento que cobrem atividades desde a coleta, isso é, a obtenção dos dados pessoais, até a exclusão desses dados e com isso, contempla-se as atividades que são realizadas com os dados pessoais, incluindo as feitas fora dos meios digitais, como, por exemplo, formulários em papel e cartões. Dessa forma, não

importa o meio onde o dado esteja guardado. A LGPD indica também exceções em seu Artigo 4º, que diz

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
>
> II - realizado para fins exclusivamente:
>
> a) jornalístico e artísticos; ou
>
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
>
> III - realizado para fins exclusivos de:
>
> a) segurança pública;
>
> b) defesa nacional;
>
> c) segurança do Estado; ou
>
> d) atividades de investigação e repressão de infrações penais; ou
>
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Temos assim uma relação fechada de situações em que a LGPD não seria aplicada, onde há uma atenção especial do legislador ao inciso III ao indicar a necessidade de legislação especifica que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observando ainda o devido processo legal, os princípios gerais de proteção e os direitos do titular (Art. 4º, §1º da LGPD). Sendo assim, mesmo em situações especificas relacionadas a investigações de infrações penais, segurança e defesa nacional, não há uma autorização de tratamento como bem aprouver ao Controlador, sendo necessária uma legislação que regule tais tratamentos.

Conforme explicita Bioni (2021, p. 60) o conceito de dados pessoais pode direcionar-se para um vocábulo reducionista ou expansionista, isso é, restringindo ou ampliando o que se entende por dados pessoais.

No olhar expansionista temos pessoa identificável, indeterminada, com um vínculo mediato, indireto, impreciso, inexato. Por sua vez, na visão reducionista há a pessoa identificada, especifica, determinada, vínculo imediato, direto, preciso ou exato (BIONI, 2021, p. 60).

Patrícia Peck Pinheiro traz a seguinte definição para os dados pessoais, sendo eles:

> Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do *Internet Protocol* (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva (PINHEIRO, 2020, p. 34).

A lei traz um universo amplo do que venha a ser um dado pessoal sob sua égide, pois além dos dados pessoais típicos, ela versa ainda que o dado que puder levar à identificação ou tornar identificável uma pessoa natural, será considerado um dado pessoal.

Esse conjunto amplo de dados pessoais dos titulares são tratados por pessoas físicas ou jurídicas para uma determinada finalidade. Na legislação, essas pessoas são denominadas agentes de tratamento, com papéis, responsabilidades e obrigações que veremos a seguir.

## 1.3 OS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Os agentes de tratamento de dados pessoais, conforme a LGPD, são o Controlador e o Operador. Ambos podem ser pessoa natural ou jurídica, de direito público ou privado, porém a diferença entre eles reside no final dos incisos que lhes descrevem.

> Art. 5º Para os fins desta Lei, considera-se:
>
> (...)
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018);

Ao Controlador caberão as decisões do tratamento sobre os dados pessoais e dados pessoais sensíveis. A definição da finalidade, quais dados pessoais serão tratados, qual a base legal deverá ser utilizada, são alguns pontos que o Controlador deverá definir, porém, caberá também ao Controlador a elaboração do Relatório de Impacto a Proteção de Dados (RIPD), informar à Autoridade Nacional de Proteção de Dados (ANPD) no caso de incidentes de segurança, dentre outros pontos. Já o Operador, irá realizar o tratamento seguindo as orientações que o Controlador lhe passou, operacionalizando o tratamento, dado o seu conhecimento técnico, de infraestrutura, *know-how*. O Operador tomará decisões técnicas para melhor implementar o tratamento, mas as decisões essenciais para o tratamento são exclusivas do Controlador (ANPD, 2021).

Conforme preconiza o Guia Orientativo da ANPD sobre Agentes de Tratamento, estes devem ser definidos a partir de seu caráter institucional, não sendo considerados os funcionários, servidores públicos ou as equipes de trabalho, atuando esses sob o poder diretivo do agente de tratamento (ANPD, 2021, p. 5).

Pode ainda existir a figura do sub operador, no qual há a celebração de um contrato entre o Operador e um outro Operador para apoiá-lo na realização das atividades, porém, este último deverá seguir as orientações do Controlador, assim como o Operador com o qual firmou contrato (ANPD, 2021, p. 19).

Temos então o Controlador e o Operador como figuras que tratam dados pessoais dos titulares. Esses dois papeis podem estar sob a mesma pessoa natural ou jurídica, ficando tanto as definições como a implementação sob o mesmo agente.

## 1.4 OS PRINCÍPIOS DA LGPD

A lei de proteção de dados pessoais é uma legislação principiológica e guarda princípios que devem ser observados para a sua correta implementação por aqueles que realizam tratamento de dados. A LGPD traz os seguintes princípios com explicações a partir Flumignan (2020, p. 124-138), sintetizados a seguir:

- **Boa fé**: princípio norteador, o qual pode ser encarado como sinônimo de boa intenção, onde em nenhuma hipótese pode-se aceitar a atitude deliberada de desrespeito à proteção de dados. Espera-se um comportamento leal, com lisura, corretude e probidade;
- **Finalidade**: para tratamento dos dados deve-se seguir propósitos legítimos, que devem ser específicos, explicitados e informados, não podendo realizar tratamento dos dados pessoais de forma incompatível com a finalidade usada para sua obtenção. O Controlador não pode fazer o que bem quiser com os dados pessoais do titular;
- **Adequação**: esse princípio é muito próximo do princípio da finalidade, pois um tratamento para ser tido como adequado, deverá estar alinhado com a finalidade. O tratamento precisa ser justificável pela finalidade;
- **Necessidade**: tal princípio implica um aumento de responsabilidade para quem coleta os dados e visa impedir a coleta não imprescindível. Deve-se avaliar quais dados são essenciais para o negócio, tendo uma visão de minimização do tratamento de dados, ou seja, apenas os dados imprescindíveis para a finalidade pretendida deverão ser tratados;
- **Livre Acesso aos Dados pelos Titulares**: mediante requisição do titular, aquele que realiza o tratamento informará quais são os dados e quais tratamentos são feitos com esses dados, o período de retenção, além de outras informações que permitam ao titular ter conhecimento do que é realizado com os dados pessoais;
- **Qualidade dos Dados**: deverá ser verificada a corretude em todos os procedimentos e operações. A atualização regular dos dados e a

garantia da segurança. Eventuais equívocos deverão ser apagados ou retificados de forma imediata, salvo se essa atualização não puder ser feita de forma unilateral;

- **Transparência**: garantia de informações claras, precisas e acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observando-se os segredos comercial e industrial;
- **Segurança**: percebe-se uma clara importância dada pelo legislador às questões envolvendo a segurança dos dados pessoais. Busca-se a proteção a acessos não autorizados e de situações acidentais ou ilícitas que possam acarretar danos ao titular. Para isso, dever-se-á fazer uso de medidas técnicas e administrativas para proteger os dados;
- **Prevenção**: determina a utilização de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Aqui deve-se atuar antes para mitigar a probabilidade de ocorrência de danos e não somente quando o dano ocorre;
- **Não Discriminação**: dados pessoais não podem ser utilizados para discriminar ou promover abusos contra os seus titulares. Esses tipos de dados são denominados dados pessoais sensíveis e a LGPD traz regras especificas para o seu tratamento;
- **Responsabilização e Prestação de Contas**: além do dever de cumprir integralmente a LGPD, quem realizar o tratamento de dados pessoais deverá ter evidências de todas as medidas adotadas, com a finalidade de demonstrar a sua boa-fé e diligência.

O tratamento de dados pessoais deve ocorrer para uma determinada finalidade que deverá ser informada ao titular dos dados. Com a entrada em vigor da LGPD, o Controlador não poderá mais utilizar os dados como bem quiser, mudando a finalidade, agregando outros tratamentos, sem que exista uma base legal que autorize tal tratamento.

O quarteto *finalidade, adequação, necessidade e transparência* dão o norte sobre o que deverá ser coletado, pois a partir de uma finalidade, os dados que serão tratados deverão estar adequados a essa finalidade e ter somente os

dados que sejam indispensáveis para o tratamento. Guardar mais dados do que seria necessário para o tratamento poderá trazer questionamentos e solicitações por parte dos titulares, além de aumentar os riscos decorrentes de vazamentos de dados pessoais. Além disso, toda essa relação com o titular deverá ser transparente, para que este entenda adequadamente os motivos, o que será realizado, e tomar as ações cabíveis, no caso de entender haver alguma má conduta.

Da relação entre finalidade e adequação, um exemplo interessante trazido por Flumignan; Flumignan (2020, p. 131) ajuda a elucidar a diferença e a complementação que um princípio dá ao outro.

> Em uma leitura a *contrário sensu*, não atenderá o princípio da adequação se o tratamento estiver em desacordo com as finalidades informadas ao titular dos dados pessoais.
>
> A título de exemplo, imagine que um aplicativo de transporte queira que os usuários forneçam dados sobre sua saúde. Neste caso, o tratamento se torna inadequado e, portanto, inviável, pois não há uma justificativa plausível para que tal fato ocorra (FLUMIGNAN; FLUMIGNAN, 2020, p. 131).

A justificativa plausível é chave para verificação de abusos por parte do Controlador, que busca mais dados do que o necessário e com tratamento que não guarda lastro com a finalidade estabelecida e informada ao titular.

A LGPD coloca o titular no centro, permitindo que este possua o controle dos seus dados e de sua utilização e numa sociedade orientada a dados, possibilita conhecer e atualizar os dados que estão em uso e que são de suma importância para sua existência dentro de um contexto de Sociedade da Informação. Isso permite que o titular possa exercer os seus direitos e ter a utilização dos dados de forma mais fidedigna a realidade, pois um dado incorreto, poderá inviabilizar um direito, dificultar uma comunicação, trazendo assim transtornos ao titular.

Para as figuras do Controlador e Operador, em questões técnicas para este último, a legislação traz um dever de segurança, onde esses agentes de tratamento tomem todas as medidas possíveis e ao seu alcance para garantir a segurança dos dados, evitando assim o vazamento que pode trazer sérios riscos

aos titulares afetados. Em função dos avanços tecnológicos, as diferentes ferramentas e tecnologias utilizadas e cada vez mais pessoas e grupos que vem se especializando em atividades hackers, trata-se de uma tarefa contínua de planejamento, monitoramento, ajustes e investimentos em equipamentos, ferramentas e capacitação, buscando assim diminuir a probabilidade e o impacto. É muito fácil encontrar casos de empresas e governos que tenham passado por problemas relacionados a segurança nos últimos tempos.

Por fim, os agentes de tratamento deverão demonstrar todas as ações que tomam em uma eventual fiscalização. Evidenciar a preocupação e ações que realizadas, demonstrando a maturidade, pode diminuir a extensão de sanções que a serem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), conforme artigo 52 da LGPD.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> (...)
>
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
>
> (...)
>
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas (BRASIL, 2018);

Temos aqui a necessidade de tomada de ações pelos agentes de tratamento como algo de extrema relevância, pois além de diminuir a probabilidade de um incidente de segurança com dados pessoais, na fatalidade, tais ações poderão auxiliar a empresa na diminuição das penas administrativas cabíveis ao caso concreto pela ANPD. Por fim, temos o princípio da não discriminação que será abordado mais a frente desta pesquisa.

Além de observar os princípios, toda a atividade de tratamento precisa amparar-se em uma base legal que dará a sustentação ao tratamento, podendo

ou não, a depender da base a ser utilizada, ser necessária a obtenção da autorização do titular para que o tratamento seja legítimo. A próxima sessão abordará as bases legais previstas na LGPD.

## 1.5 DAS BASES LEGAIS PRESENTES NA LGPD

Não sendo um dos casos de dispensa previsto no artigo 4º da LGPD, para que um tratamento de dados pessoais ocorra de forma legítima e lícita, esse precisará acontecer sobre a sustentação de uma base legal (TEFFÉ; VIOLA, 2020, p. 3). A LGPD traz em seu artigo 7º as bases legais para o tratamento de dados pessoais (BRASIL, 2018), sendo elas:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros;
>
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
>
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e

> liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

No primeiro inciso temos a necessidade de o titular dos dados realizar a autorização para que o dado pessoal possa ser tratado, nessa situação, caso o titular não forneça o consentimento e não haja uma outra base legal, o tratamento não poderá ser realizado. Tal consentimento deverá ser livre, inequívoco e informado (BRASIL, 2018), o titular poderá dar seu consentimento ou não, ficando clara essa ação e ele deverá ter as informações necessárias para poder entender com o que está consentindo, não podendo o titular ser levado ao engano para levá-lo a consentir. No guia disponibilizado pela ANPD para tratamento de dados pelo poder público temos a seguinte explicação.

> (...) a autorização do titular deve ser intencional e ele deve saber exatamente para que fim seus dados serão tratados, sendo vedada a autorização tácita e para finalidades genéricas. Além disso, o consentimento pressupõe uma escolha efetiva entre autorizar e recusar o tratamento dos dados pessoais, incluindo a possibilidade de revogar o consentimento a qualquer momento (ANPD, 2022, p. 6).

Já as demais bases legais, acontecem sem o titular autorizar o tratamento, mas não se tratando de um cheque em branco, onde o Controlador pode estabelecer os tratamentos essenciais como bem entender. Os princípios já abordados devem ser aplicados a todos os casos, conforme explicita o §6º do artigo 7º, cuja redação diz que eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas na lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular (BRASIL, 2018). Essas bases legais são:

**Cumprimento de obrigação legal ou regulatório**: o tratamento deve ocorrer devido a um comando legal. O Controlador deverá realizar o tratamento para atender a esse comando que poderá vir de uma norma de conduta ou de uma norma de organização.

As normas de conduta estabelecem obrigações prevendo consequências pelo não cumprimento. Já as de organização estabelecem obrigações que estão inseridas ao próprio cumprimento de atribuições legais típicas de entidades ou órgãos públicos (ANPD, 2022. p. 10).

**Execução de políticas públicas**: aqui é necessário observar dois conceitos, administração pública e políticas públicas, que são chave para essa base legal.

A função de administração pública é típica do Poder Executivo, mas que não se restringe a tal Poder, podendo ser aplicável também aos demais Poderes (Legislativo e Judiciário) e entes federativos, incluindo também as Cortes de Contas e o Ministério Público, desde que todos esses estejam atuando em suas funções administrativas.

Por políticas públicas, a ANPD orienta a interpretação de forma ampla, abrangendo programa ou ação governamental, definido em lei, regulamento ou ajuste contratual, onde defina-se regras, objetivos, metas, prazos e meios de execução (ANPD, 2022, p. 12).

**Estudo por órgãos de pesquisa**: essa base legal é voltada para pesquisas devendo ser um “órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico” (Art. 5º, XVIII da LGPD). Essa base é restrita a um grupo definido de Controladores, conforme o texto legal que realiza pesquisas.

A LGPD traz em diversos pontos (Artigo 7º, IV; Artigo 11, II, c; Artigo 13, Artigo 16, II) que a realização da pesquisa deve buscar, sempre que possível, a anonimização dos dados pessoais. Isso confere maior segurança ao titular, pois a anonimização faz com que se perca a relação do dado com o titular, não sendo inclusive mais considerado dado pessoal, salvo se puder ser revertido, conforme o Artigo 12.

***Execução de contrato ou procedimentos preliminares***: os dados pessoais poderão ser trabalhados para a celebração de um contrato ou nas atividades pré celebração, devendo para isso o titular ser parte do contrato em questão.

***Exercício regular de direitos em processo judicial, administrativo ou arbitral****:* permite o uso de dados pessoais em processos para produção de provas de uma parte contra a outra. Tal exercício compreende ações autorizadas pela existência de direitos previstos em lei.

Seria impraticável solicitar consentimento da outra parte para que os dados pessoais dessa pudessem figurar em um processo, impedindo assim a busca, de forma legítima, da defesa (TEFFÉ; VIOLA, 2020, p. 26).

***Proteção da vida ou da incolumidade física do titular ou de terceiros***: havendo uma necessidade excepcional e pontual, poder-se-á utilizar dados pessoais para proteger a vida ou retirar o titular ou terceiro de um perigo. Um exemplo seria o resgate de pessoas em um acidente ou perdidas, onde buscaria a localização para auxiliar nas buscas (TEFFÉ; VIOLA, 2020, p. 26).

***Tutela da saúde***: quando for necessário por motivos de saúde, poder-se-á utilizar os dados pessoais, devendo o procedimento ser realizado por profissional da saúde, serviço de saúde ou autoridade sanitária (BRASIL, 2018).

***Proteção do crédito***: busca-se ampliar e facilitar a concessão de crédito, o aprimoramento das análises de risco e impulsionar o mercado de consumo.

***Legítimo Interesse***: visa possibilitar tratamentos de dados que se encontram no escopo de atividades praticadas pelo controlador ou terceiro. Deve-se levar em consideração as expectativas dos titulares, a finalidade, necessidade e a proporcionalidade do tratamento dos dados pessoais, sendo que, quanto mais invasivo, inesperado ou genérico for, mais difícil será encontrar sustentação para uso desta base legal (TEFFÉ; VIOLA, 2020, p. 14).

O legitimo interesse é uma forma de reconhecer outros valores constitucionais que não apenas a privacidade. Esses valores são a livre iniciativa, livre concorrência e o desenvolvimento econômico e tecnológico, que

deverão conviver e algumas vezes confrontar a privacidade (BUCAR; VIOLA, 2020, p. 461).

## 1.6 APROFUNDANDO O LEGÍTIMO INTERESSE

Como é possível observar, a base do legítimo interesse é ampla e flexível, oferecendo a oportunidade ao Controlador ou terceiro realizar um tratamento de dado pessoal. A LGPD em seu Artigo 10 traz as linhas orientadoras para essa base legal.

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> I - apoio e promoção de atividades do controlador; e
>
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
>
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
>
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
>
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (BRASIL, 2018).

A ANPD, em seu guia orientativo ao setor público orienta que o uso dessa base legal deve ocorrer apenas após uma avaliação que demonstre a proporcionalidade entre os interesses do Controlador e as legítimas expectativas do titular, além de considerar o direito de oposição ao tratamento, conforme Artigo 18, §2º da LGPD (ANPD, 2022, p. 8).

Observando o pronunciamento de uma outra autoridade, a *Information Commissioner's Office* (ICO.), autoridade de proteção de dados do Reino Unido, traz em sua página que é mais apropriado a utilização dessa base legal quando

os titulares razoavelmente esperariam pelo tratamento a ser realizado e que tal tratamento tenha um impacto mínimo sobre a privacidade, ou quando houver justificativa convincente para o tratamento. Deve-se ainda verificar se não haveria alguma outra forma razoável de alcançar o mesmo resultado de forma menos intrusiva[5].

É observável uma grande preocupação com relação a essa base legal, buscando evitar que ela seja utilizada de forma indevida e traga riscos aos titulares. Um dos pontos que veremos é que a presente base não pode ser utilizada para dados pessoais sensíveis, não estando prevista no Artigo 11, e uma avaliação deverá demonstrar se é uma base legal válida a ser utilizada no caso concreto.

Além disso, o §3º do Artigo 10, traz ainda que a ANPD pode solicitar ao Controlador o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), em razão do risco que tal tratamento pode trazer ao titular.

## 1.7 A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL

Em 10 de fevereiro de 2022 o presidente do Congresso Nacional, senador Rodrigo Pacheco promulgou a Emenda Constitucional 115[6] que introduz no artigo 5º da Constituição Federal da República o inciso LXXIX, com a seguinte redação: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”, acrescentando ainda a competência da União por organizar e fiscalizar a proteção e o tratamento dos dados pessoais (Art. 21, XXVI CF) e privativamente legislar sobre proteção de dados pessoais (Art. 22, XXX CF) (BRASIL, 2022, online).

---

[5] Information Commissioner’s Office (ICO.). Legitimate interests. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ Acesso em: 16 abr. 2022.

[6] OLIVEIRA, José Carlos. Promulgada PEC que inclui a proteção de dados pessoais entre direitos fundamentais do cidadão. Câmara dos Deputados. 10 fev. 2022. Disponível em: https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/ Acesso em: 20 out. 2022.

Essas são mudanças importantes, organizam o ato de legislar e fiscalizar, o que ficando a cargo da União uniformizará o desenvolvimento do tema e seu acompanhamento no território nacional, evitando conflitos de legislações em um assunto que não tem fronteiras e quanto mais padronizado melhor para sua prática, conforme explicitado nas justificativas do Projeto de Emenda Constitucional 17/2019

> Sabemos que existem diversas propostas de leis estaduais e municipais versando sobre o assunto, inclusive em flagrante réplica da LGPD. Não há racionalização nisso: a fragmentação e pulverização de assunto tão caro à sociedade deve ser evitada. O ideal, tanto quanto se dá com outros direitos fundamentais e temas gerais relevantes, é que a União detenha a competência central legislativa. Do contrário, pode -se correr o risco de, inclusive de forma inconstitucional, haver dezenas - talvez milhares- de conceitos legais... (SENADO FEDERAL, 2019, online).

Já se tornar um direito fundamental eleva o grau da proteção de dados dentro do ordenamento jurídico pátrio. Segundo Silva (2013, p. 180) qualificar como fundamental indica se tratar de uma situação jurídica sem a qual a pessoa humana não se realiza, não convive e algumas vezes não sobrevive, não devendo apenas serem direitos formalmente reconhecidos, mas concreta e materialmente efetivados. Fazendo parte do Artigo 5º da Constituição Federal, faz parte ainda de uma cláusula pétrea, não podendo esse direito ser suprimido, apenas evoluído.

No entanto, a proteção dos dados pessoais ser considerada direito fundamental? Para a Sociedade da Informação, como já vimos, onde os dados têm uma importância muito grande e o impacto dos tratamentos sobre as pessoas pode causar graves transtornos a direitos e liberdades, tanto individuais, quanto coletivas, é muito bem-vinda essa inclusão, como presente nas justificativas da PEC 17/2019 que deu origem a Emenda Constitucional 115.

> A proteção de dados pessoais é fruto da evolução histórica da própria sociedade internacional: diversos são os Países que adotaram leis e regras sobre privacidade e proteção de dados. Isso porque o assunto, cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão.
>
> O avanço da tecnologia, por um lado, oportuniza racionalização de negócios e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por outro

> lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados (SENADO FEDERAL, 2019, online).

Pelo exposto, trata-se de uma evolução importante na busca de se avançar na tutela de direitos e garantias numa sociedade extremamente conectada, onde os dados possuem elevada preponderância.

No capítulo que segue, abordaremos agora os dados pessoais sensíveis que dado o seu potencial de causar prejuízos aos titulares, mereceram do legislador de um destaque perante os demais dados pessoais.

## 2. DADOS PESSOAIS SENSÍVEIS

Após uma visão geral sobre a LGPD, neste capítulo iremos nos aprofundar especificamente nos dados pessoais sensíveis, que são um conjunto de dados que podem causar impactos a direitos e garantias dos titulares e, por esse motivo, acabam recebendo uma atenção maior do legislador, que restringe o uso e demanda mais controle, tendo uma relação de bases legais referentes a esses tipos de dados, os quais serão abordados neste capítulo também. A Lei Geral de Proteção de Dados (LGPD) explicita em seu Artigo 5º, II que dados pessoais sensíveis são

> aqueles que abordam 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).

Tais dados recebem uma proteção especial devido ao seu potencial de causar discriminação a seus titulares (ROSÁRIO, 2021, p. 25). Como já mencionado anteriormente, o holocausto é um exemplo do uso de dados pessoais, aqui definido nas legislações atuais como dados pessoais sensíveis relacionados a raça, etnia, saúde e vida sexual, mas infelizmente há casos mais recentes como o da minoria muçulmana *Rohingya*, no Mianmar, que foi atacada pela maioria budista, onde, segundo análises, a rede social Facebook foi um catalisador para a violência[7]. Konder entende que os elementos presentes no Artigo 5º, II da LGPD são exemplificativos e não taxativos.

> (...) é inviável conceber rol taxativo de dados sensíveis, já que eles são definidos pelos efeitos potencialmente lesivos do seu tratamento (...) por exemplo, dados de localização geográfica, hábitos de compras, preferências de filmes e histórico de pesquisa podem parecer inofensivos isoladamente, mas um rápido tratamento em conjunto pode servir a identificar orientação religiosa, política e mesmo sexual (KONDER, 2020, p. 451).

[7] ASHER, Saira. **Facebook:** como a rede social se tornou peça central na crise política de Mianmar. BBC News Brasil. Disponível em: https://www.bbc.com/portuguese/internacional-55944504. Acesso em: 12 abr. 2022.

Em análise do respectivo autor, KORKMAZ (2019, p. 45) traz que a configuração de um dado pessoal como sensível não poderia ser estabelecida em abstrato, uma vez que verificando-se o contexto de utilização do dado e a combinação de dados, pode ser verificada a potencialidade lesiva do seu tratamento.

## 2.1 AS BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Em razão do maior rigor presente na LGPD para o tratamento dos dados pessoais sensíveis, e de seu impacto em garantias fundamentais do titular, o legislador trouxe um rol diferente de bases legais, estando elas presentes no Artigo 11 da presente lei.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiros;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018).

Algumas bases legais presentes no Artigo 11 são as mesmas previstas no Artigo 7º. São elas, o consentimento, cumprimento de obrigação legal ou regulatório pelo controlador, execução de políticas públicas, estudos por órgãos de pesquisa, exercício regular de direito, proteção da vida ou da incolumidade física do titular ou terceiro e tutela da saúde.

De novas bases legais, isso é, não presentes no Artigo 7º, temos a garantia da prevenção à fraude e à segurança do titular e não estão presentes no Artigo 11 as bases legais do legítimo interesse do controlador ou de terceiro e a proteção do crédito.

Com relação a base de proteção do crédito, a Lei 12.414/2011 (Lei do cadastro positivo) já proibia a anotação de dados sensíveis em bases de dados ligadas à análise de crédito. Para esta lei, as informações sensíveis são aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (BRASIL, 2011). Na LGPD, a proibição do tratamento de dados pessoais sensíveis baseado na proteção do crédito se manteve.

Já o legítimo interesse, como verificamos, trata-se de base legal muito flexível e em razão do contexto de proteção aos dados pessoais sensíveis, é adequado não permitir que tal base legal seja suporte para o tratamento de tais dados. Em relação à base legal, garantia da prevenção à fraude e à segurança do titular, temos os seguintes exemplos.

> (...) instituições bancárias e empregadores podem tratar dados biométricos para a prevenção de fraudes, sem o consentimento prévio dos titulares dos dados, a fim de confirmar que é o empregado autorizado que está entrando em área de acesso restrito da empresa ou que é determinado cliente que está realizando uma transação bancária por meio de um caixa eletrônico, por exemplo. Adicionalmente, pode-se mencionar a exigência para atendimento médico-hospitalar, com a utilização de seguro ou plano de assistência à saúde, que o segurado/beneficiário coloque seu polegar em um leitor biométrico para confirmar sua identidade, a fim de evitar que outra pessoa utilize a cobertura securitária em seu lugar (TEFFÉ; VIOLA, 2020, p. 32).

Nos exemplos acima mencionados, temos a utilização de dados biométricos, tais como digitais, reconhecimento facial, leitura da íris, para atestar

que a pessoa que está buscando acesso a um local ou serviço é mesmo a pessoa autorizada. A biometria funciona como uma chave de acesso.

# 3 BIG DATA, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Os dados são a matéria prima na Sociedade da Informação, são gerados em grandes quantidades e de diferentes formas. Para processar esse considerável volume, efetuar cruzamentos e gerar valor, faz-se necessário utilizar tecnologias da informação e é aqui que entra o *Big Data*. Moraes, Gonçalves, Ledur, Córdova Junior, Saraiva e Frigeri (2018, p. 13) trazem a seguinte definição desta tecnologia.

> Conjunto de dados extremamente amplos e que, por esse motivo, necessitam de ferramentas preparadas para lidar com grandes volumes de dados, de forma que toda e qualquer informação nesses meios possa ser encontrada, analisada e aproveitada em tempo hábil.

O Big Data permite o processamento de grandes volumes de dados em tempo bastante reduzido, que podem estar estruturados, não estruturados ou semiestruturados, tendo como objetivo verificar padrões de comportamento. O tempo aqui é um fator importante, pois numa sociedade em mudança constante, não conseguir obter a informação no momento certo para tomada de decisão, causa a perda de oportunidade e a frustração econômica, com o não atendimento de uma necessidade. Existem cinco conceitos (volume, velocidade, variedade, veracidade e valor) que caracterizam o *Big Data,* são eles:

> - Volume: trata-se do volume diário de troca de e-mails, transações bancárias, interações em redes sociais, registro de chamadas e tráfego de dados em linhas telefônicas. Essas situações servem de ponto de partida para a compreensão do volume de dados presentes no mundo atual. É importante, também, compreender que o conceito de volume é relativo à variável tempo, ou seja, o que é grande hoje pode ser nada amanhã.
>
> - Velocidade: as empresas necessitam de dados atuais sobre seus negócios, por isso a importância da velocidade é tamanha e, em algum momento, deverá existir uma ferramenta capaz de analisar os dados em tempo real. Atualmente, os dados são analisados somente após serem armazenados, mas o tempo gasto para o armazenamento em si já desclassifica esse tipo de análise como uma análise 100% em tempo real. A velocidade com a qual se obtém essa informação é uma vantagem competitiva das empresas. A velocidade pode limitar a operação de muitos negócios — quando utilizamos o cartão de crédito, por exemplo, se não obtivermos uma aprovação da compra em alguns segundos, pensamos em utilizar outro método de pagamento. É a operadora perdendo uma oportunidade de negócios pela falha na velocidade de transmissão e análise dos dados do comprador.

> - Variedade: diferentemente do passado, hoje em dia, os dados não são estruturados e armazenados em tabelas relacionais, pois uma grande variedade de dados, como mensagens, fotos, vídeos e sons, torna mais complexa a análise desses dados. Os dados não estruturados podem ser administrados juntamente aos dados tradicionais.
>
> - Veracidade: para colher bons frutos do processo de Big Data, é necessário obter dados verídicos de acordo com a realidade. O conceito de velocidade, já descrito, é bem alinhado ao conceito de veracidade pela necessidade constante de análise em tempo real — isso porque dados passados não podem ser considerados dados verídicos para o momento da análise.
>
> - Valor: quanto maior for a riqueza de dados, mais importante será saber realizar as perguntas certas no início de todo o processo de análise. É necessário estar focado para a orientação do negócio, para o valor que a coleta e a análise dos dados trarão para o negócio. Não é viável realizar todo o processo de Big Data se não se tem questionamentos que ajudem o negócio de modo realístico. (MORAES; GONÇALVES; LEDUR; CÓRDOVA JUNIOR; SARAIVA; FRIGERI, 2018, p. 16-17)

Um bom desenho de *Big Data* precisa levar em consideração esses conceitos a fim de trabalhar com dados que possam trazer o máximo de valor para o negócio. É estimado que cada pessoa produza em torno de 1.7 Mb (Megabytes) de dados por segundo, o que representa uma geração em torno de 2.5 quintilhões de bytes de dados por dia[8]. A coleta precisa ser direcionada para trazer valor, pois mesmo que em um grande volume, os dados não passam de dados, sendo necessário gerar informação e conhecimento para explorar os benefícios desses dados brutos, ou seja, eles necessitam ser analisados. (MORAES; GONÇALVES; LEDUR; CÓRDOVA JUNIOR; SARAIVA; FRIGERI, 2018, p. 15). A base do Big Data está na confluência de algumas tecnologias que quando trabalham em conjunto geram essa capacidade. Segundo MASSENO (2019, p. 3),

> Simplificando, o Big Data resulta da confluência de três avanços tecnológicos, de origem diferente, mas que se reforçaram entre si. Designadamente, decorre da Computação em Nuvem, a qual passou a possibilitar o armazenamento de volumes crescentes de dados, com disponibilidade permanente e uma fiabilidade assegurada pela redundância, tudo isto com custos cada vez menores. A que se juntaram as comunicações de banda muito larga, em fibra ótica e ponto a ponto, com velocidades de acesso tais que deixaram deixou de ser necessário manter centros de dados próprios, também com custos

[8] Saas Scout Research Group. **Big Data Statistics, Growth & Facts 2021**. Disponível em: https://saasscout.com/statistics/big-data-statistics/ Acesso em: 20 jun. 2021.

> decrescentes. A ambas, acresceram algoritmos de análise assentes em Inteligência Artificial, mais do que em força bruta computacional, ainda que distribuída, pelo menos na pendência da computação quântica, os quais vieram acrescentar a viabilidade de gerir pacotes cada vez maiores de dados, em tempo real. Finalmente, a proliferação de sensores interligados, a que se tem dado o nome de Internet das Coisas, ou de Tudo, conduziu ao multiplicar da informação disponível, a qual respeita sempre e em definitiva aos cidadãos-consumidores.

Tal avanço traz um grau de conhecimento que possibilita uma interação mais precisa, baseada nos gostos, padrões comportamentais, direcionando o Marketing Digital de forma mais personalizada, com maior probabilidade de alcançar seus objetivos. Isso é muito interessante para as empresas, mas também representa um risco à privacidade das pessoas, que muitas vezes desconhecem o destino de seus dados e o poder que isso dá a quem os possui. O caso da *Cambridge Analytica* é um exemplo prático disso.

A *Cambridge Analytica*, empresa de análise de dados online, ficou conhecida pelo uso de dados do Facebook nas campanhas de saída do Reino Unido da União Europeia, movimento este que ficou conhecido como *Brexit*, a eleição de Donald Trump para a presidência do Estados Unidos da América e de Jair Bolsonaro para a presidência do Brasil (BRUZZONE, 2021, p. 64). Mais especificamente sobre a eleição de Donald Trump, Bruzzone (2021) escreve:

> Na eleição de Donald Trump em 2016, a base de dados e a metodologia usadas para criar perfis de cada cidadão com direito ao voto: quase 250 milhões de perfis. Na campanha que elegeu Barack Obama tinham sido utilizados 16 milhões de perfis, o que já era uma revolução, mas que é pouco em relação ao que aconteceu anos mais tarde. Em média, há 5 mil "pontos de dados" por cada votante norte americana. Chamam-se de pontos de dados as informações que, combinadas, servem para traçar o contorno de uma personalidade e permitem criar centenas de milhares de versões de uma mesma mensagem, adequadas às preferências de grupos cada vez menores de usuários (BRUZZONE, 2021, p. 67).

Com o processamento desses pontos de dados é possível conhecer a pessoa melhor do que ela mesma e a partir de um trabalho de marketing atuar de forma mais certeira ao convencimento, trazendo o que a pessoa gosta, reforçando suas crenças.

A utilização desse grande lago de dados por algoritmos gera a probabilidade de que uma pessoa é a pessoa certa ou errada para uma possível contratação, um devedor de risco, um terrorista, um mal professor, e esse resultado pode colocar a vida de alguém de ponta cabeça (O'NEIL, 2020, p. 19).

A LGPD traz a preocupação com o processamento automatizado e geração de perfil que possa de alguma forma discriminar o titular. A lei em seu artigo 20 explicita que:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade
>
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
>
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (BRASIL, 2018).

Temos então o comando legal que possibilita ao titular se contrapor, questionando um processamento realizado de forma automatizada, assim como o enquadramento em determinado perfil. Um exemplo desse processamento é a obtenção de crédito, cruzam-se diferentes dados que gerarão um perfil determinando a concessão ou não do crédito, qual a taxa de juros etc.

O'Neil (2020) fala sobre alguns casos de processamento automatizado, um deles é a ferramenta de avaliação de professores chamada IMPACT, que visava alcançar os professores com baixa performance, demitindo-os.

> As aplicações matemáticas fomentando a economia dos dados eram baseadas em escolhas feitas por seres humanos falíveis. Algumas dessas escolhas sem dúvida eram feitas com as melhores das intenções. Mesmo assim, muitos desses modelos programavam preconceitos, equívocos e vieses humanos nos sistemas de software que cada vez mais geriam nossas vidas. Como deuses, esses modelos matemáticos eram opacos, seus mecanismos invisíveis a todos exceto os altos sacerdotes de seus domínios: os matemáticos e cientistas da computação. Suas decisões, mesmo quando erradas ou danosas, estavam para além de qualquer contestação. E elas tendiam a punir os

> pobres e oprimidos da sociedade enquanto enriquecia ainda mais os ricos (O’NEIL, 2020, p. 8).

No caso do algoritmo de avaliação dos professores, ocorreram demissões de profissionais que, na prática, no dia a dia, era tidos como exemplos e a dificuldade de conseguir entender o porquê do resultado, tornava difícil a argumentação e defesa desses professores. O algoritmo era uma caixa preta, com modelos complexos de difícil explicação, mas que levaram pessoas à demissão, com forte impacto em suas vidas (O’NEIL, 2020, p. 16-19).

# 4. O PRINCÍPIO DA NÃO DISCRIMINAÇÃO, UM OLHAR SOBRE ALGORITMO, INTELIGÊNCIA ARTIFICIAL E A ÉTICA

Este capítulo tem o intuito de abordar conceitos sobre preconceito, discriminação e racismo, mostrando como estão presentes na nossa sociedade, dificultando a vida de uma grande parcela da sociedade. Aprofundar nesses pontos tem a função de compreender melhor o princípio da não discriminação que está presente na Constituição Federal e na Lei Geral de Proteção de Dados que abordamos em capítulo anterior, com um olhar mais prático, demonstrando o quão enraizado está na nossa sociedade. Além disso, buscar-se-á transpor a discriminação para o contexto tecnológico, introduzindo o conceito de algoritmo e encaminhar para a inteligência artificial, seu funcionamento e como ela pode gerar resultados enviesados e de impacto aos minorizados.

## 4.1 PRECONCEITO, DISCRIMINAÇÃO E RACISMO – PRINCÍPIO DA NÃO DISCRIMINAÇÃO

O princípio da não discriminação é fundamento da República Federativa do Brasil, presente no Artigo 3º da Constituição Federal de 1988, onde constitui-se como um dos objetivos a promoção do bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (BRASIL, 1988).

A Lei Geral de Proteção de Dados também traz como princípio a não discriminação, levando a preocupação para o contexto do tratamento dos dados pessoais e dados pessoais sensíveis. A discriminação que aqui busca-se evitar é decorrente de um tratamento desvantajoso que uma pessoa dá a outra a partir de um julgamento moral negativo (MOREIRA, 2017, p. 27). Temos aqui o tratamento dado a pessoas negras, LGBTQIA+, pessoas com deficiência, portadoras de enfermidades, dentre outros grupos que acabam sofrendo discriminação.

Conforme Moreira (2017) os preconceitos são avaliações baseadas em generalizações em relação a um grupo, podendo ser verdadeiras para alguns, mas não para o grupo como um todo e as reações a partir do preconceito estão

fundamentadas nas poucas informações que o indivíduo tem sobre o grupo que enxerga ser diferente (MOREIRA, 2017, p. 40).

A discriminação que ocorre no mundo “analógico” passa ao mundo “digital”, e faz-se necessário, num contexto de Sociedade da Informação, ter atenção aos tratamentos que são realizados, tanto no mundo “analógico” quanto no mundo “digital”.

> A discriminação pode impedir a realização da igualdade de tratamento ao não permitir que diferentes classes de pessoas tenham acesso às mesmas oportunidades (...) isso acontece por exemplo quando uma empresa sistematicamente excluí candidatos homossexuais a cargos de trabalho. Temos aqui um caso no qual as pessoas são privadas de tratamento igualitário em função de uma característica que não está relacionada com a competência profissional (MOREIRA, 2017, p. 35).

Temos no trecho trazido da obra de Adilson José Moreira (2017) um exemplo de tratamento de dado pessoal sensível, no caso um dado referente à vida sexual com consequências para os candidatos que perdem qualquer possibilidade a concorrer a uma vaga de trabalho não por falta de conhecimento, competência, experiência, e sim por algo totalmente fora do contexto do trabalho a ser realizado.

Almeida (2019) traz que o racismo é uma forma sistemática de discriminação que tem na raça o fundamento, que culmina em privilégios ou desvantagens para indivíduos, a depender de qual grupo racial o indivíduo pertença (ALMEIDA, 2019, p. 32).

O mesmo autor ainda difere o preconceito e a discriminação em uma contextualização racial, segundo ALMEIDA (2019, p. 32) o preconceito é um juízo baseado em estereótipos, como considerar os negros mais violentos, judeus avarentos ou orientais preparados naturalmente para exatas (ALMEIDA, 2019, p. 32).

Por fim, a discriminação seria a atribuição de tratamento diferenciado tendo como requisito e fundamento o poder, a possibilidade efetiva do uso da força, sem a qual não é possível atribuir vantagens ou desvantagens. Essa discriminação pode ser direta ou indireta (ALMEIDA, 2019, p. 32).

> (...) discriminação direta é o repudio ostensivo a indivíduos ou grupos, motivado pela condição racial, exemplo do que ocorre em países que proíbem a entrada de negros, judeus, muçulmanos, pessoas de origem árabe ou persa, ou ainda lojas que se recusam a atender clientes de determinada raça (...) discriminação indireta é um processo em que a situação específica de grupos minoritários é ignorada (ALMEIDA, 2019, p. 32).

Temos aqui exemplos de diferentes grupos que por sua raça, religião, etnia sofrem alguma forma de discriminação e acabam sendo tolhidos de direitos, muitas vezes básicos, na sociedade a qual fazem parte. Em 2019 em publicação da agência Lupa, a partir de dados do IBGE, o Brasil possuía 56,10% de sua população de negros, sendo assim a maioria da população brasileira, mas com presença diminuta em conselhos de administração (4%), executivos (4%) e gerência (6%). Em relação a rendimentos a discrepância mantem-se, dos 10% da população que possuem maiores rendimentos, apenas 27,7% são negros[9].

Em números totalmente opostos estão as abordagens policiais da população negra. Em pesquisa realizada pela CESeC (Centro de Estudos de Segurança e Cidadania), tendo como foco de pesquisa o Estado do Rio de Janeiro, mostra que a população carioca é composta por 48% de negros, 51 % de brancos e 1% de outros, sendo que a população negra representa 63% das pessoas paradas/abordadas. No grupo de pessoas que foram paradas/abordadas mais de 10 vezes, a população negra representou 66% das ações. O estudo também trouxe algumas expressões usadas por policiais militares cariocas nas abordagens, são elas: Neguinho, Negão, Meliante, Elemento, Seu Jorge, Bob Marley, Escurinho, Favelado, Moleque, Ganso e Marmita (RAMOS, SILVA, 2022, p. 12-19).

> (...) raça, classe social, pertencimento territorial e perfil etário tem sido determinante na produção dos critérios de suspeição na prática policial brasileira. Jovens negros, pobres e moradores de favelas configuram o público alvo das abordagens policiais (ANUNCIAÇÃO; TRAD; FERREIRA, 2020, p. 1).

[9] ALFONSO, Nathália. **Dia da Consciência Negra:** números expõem desigualdade racial no Brasil. Agência Lupa. Disponível em: https://piaui.folha.uol.com.br/lupa/2019/11/20/consciencia-negra-numeros-brasil/ Acesso em: 22 abr. 2022.

Em pesquisa realizada por Anunciação, Trad, Ferreira (2020, on-line) sobre a abordagem policial, racismo e violência estrutural entre jovens negros de três capitais de Nordeste (Salvador, Recife e Fortaleza), o público que assume a liderança nas estatísticas tem cara bem semelhante à pesquisa realizada no Rio de Janeiro, à população negra e pobre. A pesquisa nordestina traz o olhar sobre os jovens, o que mostra que novas gerações são afetadas pelo mesmo estigma, praticamente institucional, de que negro e pobre são mais perigosos e precisam ser observados mais de perto.

Silva (2022), citando estudo coordenado por Jacqueline Sinhoretto sobre desigualdade racial e letalidade policial e prisões em flagrante em São Paulo, demonstra a prevalência da vigilância sobre a população negra, reconhecendo essa população como suspeitos criminais. A letalidade policial é três vezes maior sobre a população negra em comparação à população branca, sendo que 96% dos casos não geraram indiciamento dos policiais ou os processos foram arquivados.

O próprio enquadramento do tráfico de drogas passa por um olhar de raça. Silva (2022) mostra uma pesquisa realizada por jornalistas da Pública que analisaram 4 mil sentenças de tráfico em São Paulo, e identificaram maior incidência de imputações deste crime para as pessoas negras.

> (...) pessoas negras são mais condenadas por esse delito portando menor quantidade de droga – no caso da maconha, a média das apreensões variou de 136,5g (pessoas negras) a 482,4g (pessoas brancas) no estudo. A discrepância mais acentuada esteve na tipificação de presos com quantidades de até 10 gramas de maconha: 68,4% dos abordados negros foram considerados traficantes contra 18,1% dos brancos (SILVA, 2022, p. 123-124).

A discrepância de tratamento é clara, mesmo portando quantidades menores, as pessoas negras recebem tratamento mais pesado do que as pessoas brancas, mostrando de forma cristalina como a variável raça repercute diretamente nesta equação, trazendo um resultado com viés racista que está entranhado na sociedade e em suas instituições.

No racismo institucional ocorre o domínio através do estabelecimento de parâmetros discriminatórios que são baseados na raça, fazendo com que a

cultura, padrões estéticos e as práticas de poder tornem-se o padrão, o horizonte civilizatório. O padrão homem branco nas instituições dificulta a ascensão de outros grupos como negros e mulheres, além de dificultar as discussões sobre a própria desigualdade (ALMEIDA, 2019, p. 40 - 41).

Porém, o racismo perpassa a própria instituição, sendo essa um reflexo da sociedade na qual está inserida. Nesse sentido, Almeida (2019) traz que o racismo é reflexo da própria estrutura social, algo normal da constituição da política, da economia, do jurídico e da família, não tratando-se de uma patologia social e nem um desarranjo institucional, é algo estrutural, o racismo é regra e não exceção (ALMEIDA, 2019, p. 50).

Nossa sociedade está repleta de discriminação, contra raça, gênero, orientação sexual, pessoas com deficiência, xenofobia regional, como afirmar que “todo o baiano é preguiçoso”, por exemplo. Estereótipos incrustados na sociedade e muitas vezes reproduzidos no *piloto automático*, vieses inconscientes que perpetuam as escolhas para preencher vagas de trabalho, ou ações como mudar de calçada ao ver uma pessoa negra em uma rua deserta à noite. Infelizmente tais ações não vem de hoje e parecem não ter um prazo de validade sem a revisão crítica e intencional de posturas. Com os meios digitais, as discriminações já presentes no dia a dia, podem ser potencializadas, automatizadas, uma vez que tais vieses são trazidos para o mundo computacional.

Estando cada vez mais dependentes da tecnologia, os cruzamentos de dados, processamentos em grande escala, as decisões são tomadas com base em operações de tratamento de dados que poucos tem noção de como são feitos e com tais vieses, podemos ter uma resposta computacional que confirme que pessoas negras e pobres precisam ser realmente monitoradas de perto, homens são mais capazes para desempenhar papeis de decisão e liderança, que o perfil homem, branco, cisgênero e heterossexual é o correto e qualquer diferença disso, pode não ser uma boa escolha.

Tratar a não discriminação como um princípio conforme o legislador esculpiu na LGPD, traz à tona a preocupação de que todas as ações e

interpretações devem levar em consideração afastar um resultado discriminatório e que respeite os direitos e garantias.

Nesse contexto, surgem questionamentos sobre o reconhecimento facial. Mas antes de abordarmos a tecnologia do reconhecimento facial em si, é mister nos debruçarmos sobre a discriminação algorítmica, a transposição do mundo “analógico” para o mundo digital da discriminação.

## 4.2 ALGORITMO

No mundo da Sociedade da Informação o termo algoritmo é muito utilizado, sendo base para tudo que é realizado pelos computadores. Dessa forma, se faz importante uma contextualização sobre, a fim de equalizar o conhecimento. Um algoritmo é uma sequência de passos para se conseguir alcançar determinado objetivo, um exemplo é uma receita de bolo, temos os ingredientes, a sequência, os tempos, seguindo o passo a passo, conforme determinado por quem escreveu a receita, teremos um bolo ao final do processo. Um outro exemplo são manuais de montagem, eles trazem o passo a passo de como montar o objeto adquirido, uma cadeira ou mesa, por exemplo, qual peça encaixa em qual, qual a ordem a ser seguida, qual parafuso utilizar. Esses são exemplos de algoritmos.

Para um computador, a lógica é parecida. Segundo Cormen (2014, p. 1) o algoritmo de computador é um conjunto de etapas que são executadas para realizar uma determinada tarefa. Essas tarefas precisam ser descritas com precisão para que o computador possa executar os comandos e alcançar o objetivo conforme as entradas de dados que lhe são oferecidas.

Pellizzari e Barreto Junior (2019, p. 59) explicita que as aplicações são desenhadas na forma de algoritmos que podem ser imaginados como sequências de linhas de códigos e repletas de complexos cálculos matemáticos.

Então temos uma necessidade a ser atendida, uma solução é desenhada com um passo a passo que é vertido em linguagem de programação, que por sua vez é compilada e processada pelo computador que seguirá a programação,

pegando os dados de entrada, inseridos pelo usuário, banco de dados, outros serviços, executando o passo a passo e entregando o resultado. Um exemplo muito utilizado hoje em dia é o cálculo de rotas, utilizando um algoritmo de melhor rota, dado o ponto de partida e de chegada, as condições atuais de tráfego, calcula-se a melhor rota que é apresentada ao condutor, passando por complexos cálculos matemáticos.

Até aqui observa-se que um algoritmo é um passo a passo com as ações que o computador deve fazer para resolver um problema, atingir um objetivo. Os algoritmos são descritos em códigos de programação para que sejam possíveis de serem compreendidos pelos computadores.

Mas com a imensa quantidade de dados, os problemas cada vez mais complexos da sociedade, pensar em todas as possibilidades, em uma codificação linear, torna-se muito complexo, com isso o uso da Inteligência Artificial, mostra-se uma estratégia interessante, mas o que é uma Inteligência Artificial e como ela funciona? Veremos a seguir.

## 4.3 INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial é algo que habita o imaginário popular com computadores pensando e tomando decisões de forma autônoma, com robôs para ajudar a humanidade ou os mesmos robôs para exterminar a humanidade. Russell e Norvig (2004) organizam algumas definições sobre IA agrupando em quatro categorias, conforme tabela abaixo.

Tabela 1: Definições de inteligência artificial

| Sistemas que pensam como seres humanos | Sistemas que pensam racionalmente |
|---|---|
| “O novo e interessante esforço para fazer os computadores pensarem ... máquinas com mentes, no sentido total e literal.” (Haugeland, 1985) | “O estudo das faculdades mentais pelo uso de modelos computacionais (Charniak e McDermott, 1985) |

| | |
|---|---|
| “(Automatização de) atividades que associamos ao pensamento humano, atividades com a tomada de decisões, a resolução de problemas, o aprendizado ...” (Bellman, 1978) | “O estudo das computações que tornam possível perceber, raciocinar e agir.” (Winston, 1992) |
| Sistemas que atuam como seres humanos | Sistemas que atuam racionalmente |
| “A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas” (Kuzweil, 1990) | “A inteligência Computacional é o estudo do projeto de agentes inteligentes.” (Poole et al., 1998) |

Fonte: RUSSELL; NORVIG, 2004, p. 5.

As definições da parte superior estão atreladas ao processo do pensamento e raciocínio, já as da parte inferior estão atreladas ao comportamento. As do lado esquerdo medem o sucesso em relação à fidelidade em comparação ao desempenho humano e o lado direito medem o sucesso em relação ao que os autores chamam de racionalidade – sistema é racional se faz o certo a partir das entradas que lhe são oferecidas (RUSSELL; NORVIG, 2004, p. 4).

Pelas definições trazidas, remete-se a busca à recriação da inteligência humana através da programação das máquinas de forma que ela possa trabalhar como nós seres humanos fazemos. É uma área da computação voltada a desenvolver algoritmos que sejam capazes de realizar tarefas que demandem habilidades da inteligência humana (GARCIA, 2020, p. 15).

Luger (2004) observa que apesar da variedade de problemas, temos características que parecem comuns, o autor traz a seguinte relação de oito pontos:

> 1 – O uso do computador para executar raciocínio, reconhecendo padrões, aprendizagem ou outras formas de inferência.
>
> 2 – Um foco em problemas que não respondem a soluções algorítmicas. Isto implica a utilização de busca heurística como uma técnica de IA para a solução de problemas.
>
> 3 – Um interesse na solução de problemas utilizando informações inexata, faltante ou pobremente definida, e o uso de formalismos representacionais que possibilitem que o programador compense estes problemas.

> 4 – Raciocínio utilizando as características qualitativas significativas de uma situação.
>
> 5 – Uma tentativa de tratar de questões envolvendo tanto significado semântico como forma sintática.
>
> 6 – Respostas que não são nem exatas nem ótimas, mas que são “suficientes” num certo sentido. Isto é um resultado de se utilizar essencialmente métodos de solução de problemas baseados em heurísticas em situações onde resultados ótimos, ou exatos, são caros demais ou mesmo impossíveis.
>
> 7 – O uso de grandes quantidades de conhecimento específico de um domínio para resolver problemas. Esta é a base dos sistemas especialistas.
>
> 8 – O uso do conhecimento de metanível para produzir um controle mais sofisticado sobre as estratégias de resolução de problemas. Embora este seja um problema muito difícil, tratado por relativamente poucos sistemas, ele está emergindo como uma área essencial de pesquisa (LUGER, 2004, p. 48).

Temos assim uma relação de problemas de difícil resolução que demandam expertises de tratamento diferentes de um algoritmo linear, necessitando de estratégias que busquem a solução através do aprendizado a partir das informações disponíveis.

Dentro desse contexto de aprendizado temos o *machine learning* (aprendizado de máquina) que é uma estratégia para a partir de dados de entrada, o programa aprenda a encontrar os padrões, soluções para as quais o programa está sendo treinado.

> (...) em vez de modelar e ensinar o computador em cada etapa do processo, são fornecidas instruções de como aprender a partir de exemplos e dados. Isso significa que as máquinas podem ser usadas para tarefas novas e complicadas sem que seja programado manualmente o passo a passo de solução. Ela deve depreender do histórico de soluções qual o padrão do problema e qual deve ser o processo de solução.
>
> Dado um grande conjunto de dados para o treinamento, um algoritmo de aprendizagem de máquina gera um modelo capaz de mapear entradas em saídas. Este modelo matemático é composto por um sistema de equações não lineares com descontinuidade. O papel do algoritmo de aprendizagem é definir os valores ótimos para os coeficientes dessas equações de tal forma a bem reproduzir os exemplos do conjunto de treinamento, mas almejando a generalização (GARCIA, 2020, p. 15-16).

Conforme Barreto Junior e Venturi Junior (2020), a formulação de novas perguntas colabora para a calibragem estatística da resposta dada pela IA sendo que quanto maior a quantidade de dados processados, maior é a probabilidade estatística de acerto da inteligência artificial.

Segundo Anderson (2018, p. 8) a maior parte das inteligências artificiais hoje utilizam o aprendizado de máquina, sendo muito mais precisos do que os humanos em diferentes tarefas, dirigir e diagnosticar certas doenças, por exemplo.

Aqui temos a junção com o tema abordado anteriormente sobre *Big Data*, pois quanto mais informação disponível para treinar o modelo, um melhor resultado estatístico poderá ser obtido, e como vimos, *Big Data* são grandes bases de dados que utilizam tecnologias que facilitam o processamento desta grande quantidade de dados. Conectar um *Big Data* a uma IA utilizando um processo de *machine learning* permite o aprendizado do modelo em treinamento, processo esse que passa pela análise das saídas e ajustes no algoritmo.

E temos também a junção com a privacidade e proteção de dados, pois dados pessoais e dados pessoais sensíveis compõem o *Big Data*. Dessa forma, os princípios, boas práticas, bases legais, direitos dos titulares, dentre os demais pontos esculpidos na Lei 13709/2018 precisam ser introduzidos no processo de desenvolvimento de uma solução e de preferência desde o início do desenvolvimento, estratégia conhecida como *privacy by design*. No *by design,* a privacidade se torna parte integrante da organização, fazendo parte das decisões de projeto, dos processos que são realizados na organização, sendo incorporada como um padrão (CAVOUKIAN, 2011, p. 2).

Temos então uma responsabilidade na construção de uma solução para que os direitos e garantias dos titulares dos dados sejam respeitados e estes não sofram as consequências de um desenvolvimento falho, enviesado, discriminatório. Mas aqui vale uma pergunta, como cálculos matemáticos, fluxos, repetições realizadas por uma máquina que calcula zeros e “uns” pode produzir discriminação? Uma máquina é desprovida da inteligência que possuímos como

seres humanos, ela é capaz de discriminar como infelizmente um ser humano faz?

## 4.4 UM ALGORITMO DISCRIMINA?

> Os circuitos eletrônicos e as linhas de códigos enquanto objetos inanimados não podem ser, por si sós, racistas. No entanto, as entradas e as saídas destes objetos podem "carregar a informação racista" e com isso ter um comportamento racista. Por exemplo, um sistema de identificação de suspeitos em aeroportos pode reconhecer 90% dos negros como suspeitos e 100% dos portadores de olhos azuis como "acima de qualquer suspeita". Sendo assim tecnologias que possam agir de forma racista, como é o caso da inteligência artificial, devem ser banidas e reeditadas com uma base de conhecimento que respeite a diversidade humana[10].

O modelo que é desenvolvido para resolução de um problema é uma abstração, segundo O'Neil (2020, p. 30) uma representação de um processo, pega o que sabemos e usa para prever as respostas nas variadas situações. Temos assim um olhar que forma o modelo que será construído para resolver determinado problema, sendo uma abstração, há simplificações e correlações e isso repercute nos resultados. Nenhum modelo consegue incluir toda a complexidade do mundo real.

> (...) o pessoal criando ADMs habitualmente carece de dados para os comportamentos em que têm mais interesse. Então trocam por dados substitutos – ou proxies, indicadores aproximados. Eles traçam correlações estatísticas entre o CEP residencial de alguém ou padrões de linguagem e seu potencial de pagar um empréstimo ou conseguir dar conta de um emprego. Essas correlações são discriminatórias (...) modelos de beisebol, em geral, não usam proxies porque usam entradas pertinentes como bolas, strikes e acertos (O'NEIL, 2020, p. 29).

Com a adoção desses *proxies*, temos novas relações entre dados, que por não ser o dado original do evento, como é o caso das estatísticas de beisebol mencionadas pela autora, podemos ter inferências que são prejudiciais, pois os

[10] RAMOS, Debora Oliveira; COSTA, Ernane José Xavier. Encruzilhada tecnológica: Um diálogo entre duas pessoas negras acerca da inteligência artificial e racismo. **Jornal da USP**. 01 set. 2022. Disponível em: https://jornal.usp.br/artigos/encruzilhada-tecnologica-um-dialogo-entre-duas-pessoas-negras-acerca-da-inteligencia-artificial-e-racismo/. Acesso em: 22 out. 2022.

resultados obtidos pelo processamento algorítmico podem destoar do mundo “real” e trazer consequências às pessoas envolvidas, como taxas mais altas de empréstimo, score de crédito, dentre outras.

Já o ranking de um jogador de beisebol está atrelado ao desempenho deste, é a quantidade de rebatidas, o acerto se o arremessador é canhoto ou destro, a quantidade de *home runs*, são números que alimentam estatísticas a partir do que o jogador faz em jogo, seus erros e acertos, não há obscuridade nos números de um jogador de beisebol, o que não se pode dizer sobre o *score* de crédito de uma pessoa, com diferentes reflexos sobre a vida desta.

O’Neil (2020) chama esses modelos nocivos de Armas de Destruição Matemáticas (ADM’s), modelos que programam preconceitos, equívocos, e vieses humanos nos sistemas de software, sistemas esses que gerenciam cada vez mais nossas vidas (O’NEIL, 2020, P. 8).

Em pesquisa realizada por Fernanda Carrera (2021) analisando dois bancos de imagens (Getty Imagens e Shutterstock) partindo de base de comparação de imagens de controle com atributos que remontam a momentos coloniais, se demonstrou a diferença na escolha pelo algoritmo.

São três imagens:

- **Jezebel** que reúne atributos relacionados a hipersexualização da mulher negra, com o corpo disponível, sobretudo, ao homem branco (CARRERA, 2021, p. 12).
- **Mammy** que está relacionada à mãe preta, ama de leite, pessoas invisibilizadas, silenciadas e envoltas em expectativa de passividade (CARRERA, 2021, p. 14).
- **Sapphire** que está relacionada à agressividade, prepotência, assertividade e expansividade exagerada, vista assim como uma imagem negativa da mulher negra para a branquitude, uma vez que traz uma ameaça ao poder (CARRERA, 2021, p. 15).

A análise dos bancos de dados a partir dos retornos trazidos pelos algoritmos ao se pesquisar por mulheres negras e mulheres brancas foi:

> analisados os bancos de imagem Shutterstock e Getty Images, com as palavras-chave “black woman” e “white woman”, assim como “nanny” e “babá”, aliando aos resultados encontrados em trabalhos anteriores a respeito das palavras-chave “aggressiveness” e “beauty”. Embora a pandemia da covid-19 tenha influenciado nos resultados, foi possível notar que, em comparação com mulheres brancas, mulheres negras são tagueadas mais frequentemente a narrativas de subordinação, que associam seus corpos a cargos de subalternidade a serviço de família branca (nanny/babá), coerentes com a imagem de controle Mammy; animalização e hipersexualização, condizentes com a imagem da Jezebel; assim como conectadas à agressividade, como a imagem de controle Sapphire.
>
> É importante notar que esses repositórios de imagem costumam atribuir à branquitude o padrão imagético ideal, portanto a análise dos resultados de busca já considera que o contexto branco será majoritário (CARRERA, 2021, p. 27).

Temos aqui um evidente viés discriminatório ao se retornar imagens negras relacionadas a subordinação, subalternidade, animalização, hipersexualização e agressividade. A pesquisa remonta a características trazidas de épocas coloniais, escravocratas, com reflexos na atualidade, nas ruas e também nos algoritmos em questão.

Buolamwini (2017) faz uma análise da forma como os vieses adentram nos modelos e são assim processados pela Inteligência Artificial, propagando-os.

> Inteligência Artificial - que está se infiltrando na sociedade, ajudando a determinar quem é contratado, despedido, concedido um empréstimo, ou mesmo quanto tempo alguém passa na prisão - tem um problema de preconceito. O escopo e a natureza desse problema estão amplamente ocultos. A seleção de dados para treinamento a fim de ajustar os sistemas de inteligência artificial é uma parte fundamental do desenvolvimento de modelos robustos de previsão. No entanto, o viés que reflete as desigualdades sociais nos dados de treinamento pode incorporar viés nos modelos que são criados. Além disso, conjuntos de dados de referência são usados para avaliar progresso em tarefas específicas, como tradução automática e detecção de pedestres. Conjuntos de dados de referência não representativos e métricas de precisão agregadas podem fornecer um falso senso de progresso universal (tradução do autor) (BUOLAMWINI, 2017, p. 13)[11].

[11] *Artificial Intelligence - which is infiltrating society, helping determine who is hired, fired, granted a loan, or even how long someone spends in prison - has a bias problem. The scope and nature*

O desenvolvimento de uma solução de Inteligência Artificial tem nos dados um importante fator de sucesso, pois, como vimos, eles auxiliam no ensino da máquina e na forma como ela irá responder aos casos semelhantes. O processo de aprendizado, com os dados de entrada e de controle devem ser possíveis de demonstrar a diversidade de situações, senão corremos o risco de perpetuar de forma muito mais otimizada que preto e pobre é um risco para a sociedade, fechando oportunidades e aumentando assim as disparidades sociais. Conforme O'Neil (2020, p. 144), o "resultado é que criminalizamos a pobreza, acreditando o tempo todo que nossas ferramentas não são apenas cientificas, mas justas".

Garcia (2020, p. 17) traz o caso de um concurso de beleza cujo jurados seriam robôs gerados a partir de inteligência artificial (Beauty.AI), decidindo através de critérios objetivos, avaliando as imagens enviadas pelos concorrentes, buscando por rugas, simetria facial, medidas faciais e uniformidade na coloração da pele. Com isso, esperava-se escolher a pessoa mais atraente sem preconceitos ou aspectos socioculturais, mas o resultado foi totalmente diferente do esperado, sendo escolhidas as imagens de homens e mulheres brancas. Dos 44 vencedores, quase todos eram brancos, alguns asiáticos e apenas um tinha pele escura.

A IA deste concurso aprendeu a partir de uma base de dados composta por artistas de Hollywood, sendo majoritariamente composta por pessoas brancas. Os dados utilizados para estabelecer os padrões não continham raças e etnias em quantidade para treinar o modelo, isso acabou reproduzindo no resultado, decidindo a partir do que aprendeu com a massa de dados de entrada. O modelo em questão discriminou as pessoas dado um descuido das pessoas envolvidas na geração da base de dados de treinamento e do próprio treinamento, o resultado definia um concurso de beleza, mas poderia ser a

---

*of this problem is largely hidden. Selecting training data to finetune artificial intelligence systems is a pivotal part of developing robust predictive models. However, bias reflecting social inequities in training data can embed unintended bias in the models that are created. Furthermore, benchmark datasets are used to assess progress on specific tasks like machine translation and pedestrian detection. Unrepresentative benchmark datasets and aggregate accuracy metrics can provide a false sense of universal progress on these tasks.*

definição de um risco em potencial ensejando uma abordagem policial, por exemplo.

Mas nem sempre se trata de uma relação direta, podendo existir vieses escondidos, onde mesmo eliminando a informação de etnia ou raça, por exemplo, o escopo dos dados tratados levaria a um resultado de privilégio. Garcia (2020, p. 20) traz um outro caso no segmento de saúde onde uma seguradora de saúde norte americana buscou analisar os casos de doenças crônicas graves frequentes e oferecer tratamentos preventivos, o que diminuiria os custos da seguradora. Buscando evitar o viés racial, foram retirados da base informações desse tipo, mas ao final as pessoas escolhidas pelo algoritmo para receber o tratamento eram em sua maioria brancas. Ao analisar o caso, verificou-se que os negros usavam menos o seguro saúde por serem mais pobres, além do temor dos assegurados negros de perder dias de trabalho indo ao médico e perderem o emprego por causa disso.

Neste caso, apesar de não existir no tratamento dados que referenciassem a raça, o que foi uma boa prática, o contexto levou o modelo a escolher as pessoas brancas, não dando oportunidade de um tratamento preventivo para pessoas negras.

Tais resultados impactam diretamente a vida de grupos socialmente minorizados, o que Moreira (2020, p. 516) trata como uma opressão algorítmica que está fundamentada nos seguintes fatores:

1. Representações sociais negativas que estão baseadas em estereótipos permeiam o algoritmo que são utilizados para a tomada de decisão de pontos centrais da vida das pessoas;
2. O funcionamento ocorre de forma invisível, as pessoas não enxergam o que está acontecendo, recebendo uma resposta e isso faz com que os resultados sejam encarados como aspectos naturais;
3. Potencializa as possibilidades de afetar diferentes aspectos da vida social, sem ser notado de forma imediata pela sociedade;

4. As decisões substituem os processos de deliberação, onde os participantes poderão trazer pontos que não são considerados por um processo automático;
5. Estratégia deliberada de dominação de certos grupos por outros, trazendo percepções negativas em relação a minorias.

A combinação destes fatores, conforme o autor, traz a opressão algorítmica, com impacto sobre a vida das pessoas. São perceptíveis os vieses nos fatores acima mencionados e que vão direcionar como os tratamentos irão ocorrer.

> A inteligência artificial promove a opressão racial porque, atua sobre uma realidade estruturada a partir de sistemas de dominação, uma combinação responsável pela manutenção de disparidades entre grupos sociais. Aqueles responsáveis pela criação de algoritmos argumentam que eles operam de forma neutra, a mesma estratégia discursiva utilizada pelos membros do grupo racial dominante. Entretanto, a realidade se mostra muito mais complexa do que essas pessoas procuram nos convencer (...) Algoritmos que pretendem prever a possibilidade de reincidência de pessoas entendem que negros são mais propensos a esse problema porque observam que muitos moram na mesma área da cidade. A previsão não decorre das particularidades do indivíduo, mas do fato que ele mora em uma sociedade racialmente segregada. O racismo estrutural presente naquela sociedade faz com que decisões sejam tomadas sem a devida consideração do contexto social e histórico no qual as pessoas estão inseridas (MOREIRA, 2020, p. 517).

Aqui aparece o racismo estrutural e este é perpetuado para o digital, trazendo os vieses que vão considerar, por exemplo, que pessoas negras têm uma possibilidade maior de delinquir e por isso devem ser tratadas como potenciais criminosas.

Esses cenários não devem ser encarados como normais ou como meros erros. Eles precisam ser tratados para que não ocorram, sendo necessária a aplicação de valores éticos no desenvolvimento do algoritmo, observando as diferenças que existem na sociedade e trazendo tais diferenças no aprendizado. Mas o que vem a ser um algoritmo ético?

## 4.5 UMA INTELIGÊNCIA ARTIFICIAL ÉTICA

Já definimos em sessão anterior o que é um algoritmo, passamos por essa receita dentro do contexto da Inteligência Artificial, agora iremos abordar como esse tratamento que ocorre poderia ocorrer de uma forma ética.

Para Leslei (2019, p. 3) a Inteligência Artificial tem o potencial para ajudar a humanidade enfrentar alguns de seus desafios, mas há uma curva de aprendizagem normal como em qualquer tecnologia, e numa curva de aprendizado íngreme como é a da Inteligência Artificial, erros de cálculo serão cometidos, trazendo impactos imprevistos e nocivos para as pessoas. Faz-se necessário considerar essa realidade e os impactos deverão ser gerenciados de forma responsável no desenvolvimento das soluções, priorizando a ética e a segurança no desenvolvimento de IA.

Essa ética é composta de um conjunto de valores, princípios e técnicas, padrões amplamente aceitos do que é certo e errado para conduzir o desenvolvimento das soluções em IA (LESLEI, 2019, p. 3). Para este mesmo autor, uma IA precisa ser ética, pois ela pode prejudicar potencialmente as pessoas, e neste contexto Leslei (2019, p. 4 - 5) traz os seguintes pontos que uma solução IA pode trazer como resultado.

- Vieses e discriminação;
- Negação da autonomia individual, recursos e direitos;
- Saídas não transparentes, inexplicáveis ou injustificável;
- Invasões de privacidade;
- Isolamento e desintegração da conexão social;
- Resultados não confiáveis, inseguros ou de má qualidade.

O’Neil (2020) traz a opacidade como um problema desses algoritmos o que liga diretamente com o ponto trazido por Leslei (2019) que aborda as saídas não transparentes, inexplicáveis ou injustificáveis que farão com que o titular dos dados não compreenda o porquê do resultado, em razão de toda a complexidade envolvida no processo. Sofrerá as consequências, sem entender as causas e os meios de como se proteger e pleitear uma mudança do *status*. O que reforça o

comportamento ético necessário da organização e das pessoas envolvidas no processo de desenvolvimento da solução.

Nesta linha o governo do Reino Unido traz uma cartilha de orientação para o uso de dados de uma forma ética para o setor público, mas que pode muito bem ser aplicável também ao setor privado. Os princípios explicitados na orientação estão baseados no seguinte tripé (UNITED KINGDON, 2020, online):

- **Transparência**: ações, processos e dados abertos à inspeção, publicando em formato aberto, compreensível, de fácil acesso e gratuito;
- **Responsabilidade**: mecanismos de governança e supervisão, permitindo uma fiscalização eficaz e o controle sobre as decisões e ações tomadas;
- **Justiça**: eliminar o potencial efeito discriminatório não intencionais sobre indivíduos e grupos sociais, garantindo que o projeto e os resultados respeitem a dignidade dos indivíduos.

Pelos princípios fica clara a necessidade da transparência frente a opacidade já comentada anteriormente, pois sem conhecer as linhas de funcionamento do modelo e como esse foi treinado, fica muito difícil atuar para que as discriminações não ocorram, sejam mitigadas e até mesmo aconteçam as devidas responsabilizações por resultados que discriminem pessoas. Nesse ponto, o princípio da justiça rege a forma da construção do modelo e seu treinamento, sempre buscando a dignidade dos indivíduos que são impactados pelo processamento.

Aqui é importante citar a Declaração de Toronto, documento publicado em maio de 2018 pela Anistia Internacional e *Access Now*, e lançada na *RightsCon* 2018 na cidade de Toronto, no Canadá. Tal declaração visa proteger o direito à igualdade e à não discriminação nos sistemas de aprendizagem de máquina. No tocante a prevenção da discriminação, a declaração explicita a obrigação dos governos e a responsabilidade do setor privado em prevenir proativamente a discriminação, tendo em vista as leis e normas de direitos humanos e caso uma discriminação ocorra, o sistema precisa ser investigado para encontrar a origem

e corrigi-la. Deve existir também uma proatividade dada a evolução constante das tecnologias, precisar-se-á encontrar novas formas de proteger os direitos humanos (AMNESTY INTERNATIONAL; ACCESS NOW; 2018; online).

Importante essa visão, a tecnologia evoluiu constantemente, não sabemos o que ela será capaz de proporcionar à nossa sociedade no futuro, então um olhar sobre as pessoas precisa caminhar junto no processo de desenvolvimento, buscando manter direitos e garantias, devendo ser uma premissa dentro do processo de criação dos produtos. O artigo 21 da Declaração traz a seguinte declaração:

> Inclusão, diversidade e equidade implicam a participação ativa e significativa de uma comunidade diversificada, incluindo usuários finais, durante a concepção e aplicação de sistemas de aprendizagem de máquina, para ajudar a garantir que os sistemas sejam criados e utilizados de forma a respeitar os direitos – particularmente os direitos de grupos marginalizados vulneráveis à discriminação (tradução do autor)[12] (AMNESTY INTERNATIONAL; ACCESS NOW; 2018; online).

Trazer o usuário final, envolver os representantes das diferentes partes interessadas antes da solução estar disponível para uso, pode diminuir a probabilidade de erros nos resultados.

Na orientação do marco ético dos dados do governos do Reino Unido destaco um ponto específico sobre o tratamento dos dados. A ação específica de número 4 traz a necessidade de rever a qualidade e as limitação dos dados utilizados no aprendizado.

> Insights sobre novas tecnologias são tão bons quanto os dados e práticas usados para criá-los. Você deve garantir que os dados do projeto sejam precisos, representativos, proporcionalmente utilizados, de boa qualidade, e que você seja capaz de explicar suas limitações (tradução do autor)[13] (UK, 2020, online).

[12] Inclusion, diversity and equity entails the active participation of, and meaningful consultation with, a diverse community, including end users, during the design and application of machine learning systems, to help ensure that systems are created and used in ways that respect rights – particularly the rights of marginalised groups who are vulnerable to discrimination.
[13] Insights from new technology are only as good as the data and practices used to create them. You must ensure that the data for the project is accurate, representative, proportionally used, of good quality, and that you are able to explain its limitations.

Como já visto, os dados utilizados são de suma importância para o treinamento e correções do modelo, e a orientação do Reino Unido traz requisitos importantes nesse processo. Como já tratado anteriormente, o concurso de beleza que utilizou robôs falhou pela falta de representatividade, uma vez que os dados utilizados para treinamento eram majoritariamente relacionados a pessoas brancas. Conhecer o público e representar este no aprendizado é necessário para evitar erros. Esse foi um caso de concurso de beleza, mas pode definir a contratação de uma pessoa ou até mesmo a liberdade desta.

Aprofundando na ação da qualidade dos dados, temos os seguintes pontos a serem observados, cada um com questões para ensejar a análise, para esta pesquisa irei trazer de forma suscinta cada um dos pontos presentes na orientação do marco ético dos dados (UNITED KINGDON, 2020, online):

- **A fonte dos dados**: conhecer a base em que se trabalhará, seus metadados, o significado das informações que estão presentes, como eles foram gerados, quais instrumentos estão disponíveis para manter a integridade dos dados, são alguns dos pontos presentes neste quesito.
- **A proporcionalidade**: utilizar apenas o necessário dos dados para o tratamento, considerando aqui os princípios da finalidade, necessidade e adequação já explorados anteriormente. Apesar do contexto da orientação ser a GDPR, é possível de se analisar frente a LGPD, dado que esses também são princípios esculpidos pelo legislador em nossa lei de privacidade e proteção de dados pessoais
- **O viés**: avaliar se os dados podem refletir alguma prática discriminatória, quais *proxys*, isso é, simplificações da realidade para aplicação no modelo podem causar um resultado discriminatório.
- **A anonimização**: verificar a possibilidade de anonimizar ou pseudoanonimizar os dados pessoais, sendo possível demonstrar essa desindentificação e o cuidado de que com o cruzamento com outros dados poderia haver o reestabelecimento da relação do dado com o titular.

- **Prestação de contas**: como validar que o algoritmo está correto, alcançando o resultado esperado quando novos dados são adicionados, o projeto é possível de ser reproduzido, a qualidade da saída e o grau de confiança sobre o algoritmo.
- **Dados abertos e compartilháveis sempre que possível**: Havendo a possibilidade de compartilhar, por não serem dados sensíveis, não pessoais, é incentivado pela orientação o compartilhamento para que outros possam reproduzir as análises.
- **Compartilhamento dos modelos para escrutínio sempre que possível**: No ponto anterior o compartilhamento era sobre os dados, aqui é sobre os modelos, os algoritmos, permitindo assim que outros analisem e reproduzam o processo. Para isso deve-se observar a privacidade dos titulares dos dados envolvidos no treinamento do modelo e a integridade do trabalho.
- **Como garantir a transparência em modelos sensíveis**: No caso de modelos que não possa ser compartilhado, como nos dois pontos anteriores, a sugestão é a liberação dos metadados e o desempenho obtido sobre o conjunto de dados. Além disso, órgãos externos, selecionados e aprovados, examinem o modelo em um contexto controlado.
- **Explicabilidade**: aqui temos a capacidade de explicar para as pessoas o funcionamento do algoritmo de aprendizado de máquina. Explicar de forma simples para que as pessoas entendam, descrever os objetivos, as variáveis e resultados, disponibilizando ao público essa visão.

A OCDE (Organização para a Cooperação e Desenvolvimento) traz uma lista de princípios que servem de valores base para o desenvolvimento da IA, são eles:[14]

[14] OCDE. Disponível em: https://oecd.ai/en/ai-principles. Acesso em: 29 nov. 2022.

- **Crescimento inclusivo, desenvolvimento sustentável e bem estar**: este princípio versa sobre a preocupação do desenvolvimento de IA que busque o benefício para as pessoas e o planeta, contribuindo para o bem estar, a sustentabilidade e a inclusão. Deve-se buscar a redução dos preconceitos e o impacto sobre populações vulneráveis e sub representadas;
- **Valores centrados no ser humano e justiça**: o desenvolvimento da IA deve ser realizada em valores centrados no ser humano, tais como as liberdades fundamentais, igualdade, justiça social, privacidade e proteção de dados, estado de direito, direitos do consumidor, dentre outros, com a adoção de salvaguardas, incluindo a intervenção e supervisão humana conforme o contexto;
- **Transparência e explicabilidade**: deixar claro que está se interagindo com uma IA habilitar as pessoas a compreendem o desenvolvimento, treinamento, operações e a entrega que as aplicações estão realizando. O titular entender o porquê, como e para que o tratamento é realizado;
- **Robustez, segurança e proteção**: capacidade de resistir ou superar as adversidades que sejam encontradas durante o tratamento realizado pela IA incluindo também a segurança digital. Neste ponto a OCDE levanta duas recomendações, aplicar uma gestão de riscos apropriada para o caso e manter a rastreabilidade para posterior análise e ajustes se for o caso.
- **Prestação de contas**: expectativa de que organizações ou indivíduos atuaram para garantir um funcionamento adequado da solução de IA, de acordo com as funções e estruturas regulatórias aplicadas ao caso, levando essa garantia de bom funcionamento para as decisões que são tomadas. Disponibilizar documentações, realizar auditorias ou permitir auditorias quando justificado, entram também neste princípio.

É possível verificar que os direcionamentos trazidos pela Declaração de Toronto, as orientações do governo do Reino Unido e da OCDE guardam forte

relação, trazendo a centralidade no ser humano, titular dos dados que estão sendo tratados pelo algoritmo, havendo uma responsabilidade por aqueles que desenvolvem os modelos e treinam estes em trabalhar a questão dos vieses discriminatórios, protegendo os marginalizados de resultados que podem perpetuar a discriminação.

Outros pontos importantes são a transparência e a prestação de contas, tais pontos são princípios da Lei Geral de Proteção de Dados e indispensáveis para que o titular compreenda o que está sendo feito com seus dados, o impacto que este poderá sofrer e entender o resultado que recebeu, para assim ter elementos para contestar.

E por falar em transparência, segundo Teixeira (2021, p. 5) a Nova Zelândia em julho de 2020 criou a Carta do Algoritmo, onde 21 órgãos assinaram garantindo transparência e regras para melhores práticas no uso dos dados pelo setor público, tendo como medidas uma documentação em linguagem de fácil compreensão, a inclusão da cultura indígena *Mãori* no desenvolvimento e uso dos algoritmos, revisão periódica visando garantir a ética, privacidade, os direitos humanos e a disponibilização de um canal para apelação de uma decisão tomada por IA. Temos assim a transparência, a inclusão e o compromisso com a melhoria contínua, centrada no humano.

Quanto a revisão das decisões tomadas de forma automatizada, a Lei 13.709/2018 (Lei Geral de Proteção de Dados) não possuí a revisão humana de tais decisões na lei em vigor. No texto original da LGPD, o artigo 20 expressava que o titular teria o direito de solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado se este tratamento em questão afetasse seus interesses. Porém, a Lei 13.853/2019 deu uma nova redação a este artigo que passou a expressar, no texto vigente no presente momento, que

> 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, online).

O veto que trouxe a mudança com a retirada da revisão por pessoa natural recebeu a seguintes justificativa:

> A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária (SENADO FEDERAL, 2019, online).

O veto foi realizado em julho de 2019, em tempo de *vacatio legis* da Lei 13.709/2018 (LGPD), fez uma importante mudança em um momento em que ainda não se tinha exercitado a legislação, assim como a Autoridade Nacional de Proteção de Dados (ANPD) se pronunciar em relação às pequenas empresas na adoção da LGPD, poderia tê-lo feito também para a questão da revisão humana das decisões automatizadas, havendo exemplos práticos, tanto do volume de solicitações, das formas de se analisar e responder.

Aliás, a Autoridade Nacional de Proteção de Dados não havia iniciado suas atividades naquele momento, o que viria a acontecer somente em 6 de novembro de 2020. O desenvolvimento de uma estratégia para análise e resposta precisaria ter sido pensada por controladores com apoio dos operadores e assim teríamos um retrato para tratar a questão e não o tudo ou nada que acabou sendo feito. Vale destacar que logo no primeiro artigo da LGPD temos a referência de que a lei tem por “objetivo de proteger direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018, online). O veto vai de encontro ao objetivo explícito na lei, uma vez que limita a proteção contra discriminações oriundas de análises baseadas em padrões preconceituosos e não inclusivos absorvidos pelos algoritmos.

Analisados os pontos, temos projetos de marco de Inteligência Artificial no Brasil e também na União Europeia, a seguir será dada uma visão suscinta de pontos para verificar como está se buscando internalizar a regulação da

Inteligência Artificial, mas por se tratar no momento de projetos, podemos ter alterações até que as legislações entrem em vigor, o que não diminui seu caráter ilustrativo.

## 4.7 DIREÇÕES PARA O DESENVOLVIMENTO DE IA – CASOS BRASIL E EUROPA

Observemos como a União Europeia e o Brasil tem caminhado para internalizar em seus ordenamentos jurídicos a regulação da inteligência artificial.

- **O caso Europeu:**

O projeto de regulação Europeu (COMISSÃO EUROPEIA, 2021, online; EUROPEAN PARLIAMENT, 2021, online) traz em seu Artigo 5º práticas que tendem a serem proibidas na União Europeia, sendo elas os sistemas que empreguem técnicas subliminares, manipulativas ou nocivas, podendo causar danos físicos ou psíquicos; que explorem grupos vulnerabilizados; utilizados por autoridades públicas, ou em nome destes, para pontuação social; identificação biométrica remota em tempo real em espaços acessíveis ao público para aplicação da lei, salvo em número limitado de casos. Esses casos possuem riscos inaceitáveis para a União Europeia pelo projeto proposto.

Outros casos como identificação e categorização biométrica de pessoas, gerenciamento e operação de infraestrutura, educação e formação profissional, administração da justiça e processos democráticos seriam permitidos, mas precisam cumprir regras como cadastrar o sistema em uma base de dados da União Europeia antes de utilizá-lo, realizar uma avaliação de conformidade e realizar uma gestão de riscos do processo de desenvolvimento da solução.

Por fim, temos aplicações de risco limitado e as de baixo risco. Para as aplicações que se enquadram na primeira categoria será necessário deixar as obrigações transparentes, deixando claro, por exemplo, que a pessoa está interagindo com uma Inteligência Artificial. Já para o grupo de baixo risco há a previsão de criação de códigos de conduta para incentivar a aplicação dos requisitos obrigatórios dos sistemas de alto risco.

O projeto também prevê a criação de um Comitê Europeu para a Inteligência Artificial visando contribuir para a cooperação das autoridades nacionais, também previstas para serem criadas pelo projeto, contribuir para a formulação de orientações e auxiliar as autoridades nacionais na aplicação do regulamento. Há ainda a previsão de acompanhamento dos sistemas de risco elevado, a comunicação de incidentes graves e anomalias, a fiscalização e as sanções.

- **O caso Brasileiro:**

Em comparação à proposta europeia, o projeto de lei brasileiro é bem mais modesto, não definindo os pontos que a lei europeia traz. Atualmente encontra-se tramitando no Senado Federal, onde o Projeto de Lei 21/2020, já aprovado na Câmara dos Deputados tramita em conjunto com outros dois Projetos de Lei (5051/2019, 5691/2019 e 872/2021) de iniciativa no Senado Federal. Há ainda uma comissão de juristas[15] para elaborar o projeto de regulação que se encontra trabalhando no tema, havendo previsão de concluir os trabalhos em dezembro/2022[16]. O resultado dessa comissão é apresentar um texto único ao Congresso Nacional para que siga o rito de tramitação.

O produto do trabalho desta comissão tende a trazer definições, direitos, critérios de avaliação de risco, governança dos sistemas, responsabilidade civil, supervisão e fiscalização[17].

Pelo apresentado na reunião da comissão, o trabalho está sendo conduzido trazendo elementos que até então não estavam presentes nos projetos em tramitação, o que é uma boa notícia, pois em um assunto tão

[15] Senado Federal. Ato do Presidente do Senado Federal nº 4, de 2022. Institui Comissão de Juristas responsável por subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nº 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/152136 Acesso em: 28 out. 2022.
[16] Agência Senado**. Inteligência artificial já tem 'esboço' de regulação**. 20 out. 2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/10/20/inteligencia-artificial-ja-tem-esboco-de-regulacao Acesso em: 28 out. 2022.
[17] PINHEIRO, Regina. Comissão de juristas já tem estrutura de projeto de lei sobre inteligência artificial. Senado notícias. 21 out. 2022. Disponível em: https://www12.senado.leg.br/noticias/audios/2022/10/comissao-de-juristas-ja-tem-estrutura-de-projeto-de-lei-sobre-inteligencia-artificial. Acesso em: 28 out. 2022.

complexo e com possibilidade de impactar as pessoas, precisamos caminhar para além de princípios, fazendo uma gestão sobre riscos e de formas de fiscalizar a prática do dia a dia.

Até aqui abordamos os algoritmos, a inteligência artificial e as preocupações, visando um uso ético desta tecnologia que possuí grande potencial para contribuir no desenvolvimento, mas também com riscos caso seja mal utilizada. Partiremos no próximo capítulo a abordar o reconhecimento facial, um uso prático da inteligência artificial, explicando o que é, como funciona e os cuidados que se deve ter.

## 5 O RECONHECIMENTO FACIAL

No decorrer desta pesquisa passamos pela Lei 13.709/2018 (Lei Geral de Proteção de Dados) onde está expresso que dados biométricos são considerados dados pessoais sensíveis, estando assim alçados ao grupo de dados que podem causar algum risco a direitos e garantias do titular. Agora vamos nos aprofundar no reconhecimento facial em si. Este capítulo visa demonstrar como o computador realiza o reconhecimento facial, como ocorre o treinamento (*machine learning*) para que a máquina saiba o que é um rosto, identifique de quem é o rosto, como o processo pode ser discriminatório, e ainda, de que forma podemos ter um processamento não discriminatório.

A tecnologia de reconhecimento facial pode ser descrita como a possibilidade, via *software*, de reconhecer e identificar rostos a partir de fotos e vídeos (COSTA, OLIVEIRA, 2019, p. 6). Isso é, a partir de uma foto ou vídeo, o programa de computador mapeia a imagem encontrando o rosto no contexto da imagem e identificando de quem seria o rosto.

> Em linhas gerais, um sistema de reconhecimento facial opera mediante o uso de biometria para mapear características faciais de uma pessoa presente em uma fotografia ou vídeo, comparando as informações obtidas com um banco de dados de rostos conhecidos para encontrar uma correspondência (COSTA, OLIVERIRA, 2019, p. 6).

Dentro da tecnologia de reconhecimento facial (*Facial Recognition Technology* – FRT) temos o LFR (*Live Facial Recognition*) em tradução livre significa reconhecimento facial ao vivo, em que há a coleta automática de dados biométricos para verificação, onde conforme a ICO, há um maior potencial de intrusão na privacidade do titular (INFORMATION COMMISSIONER'S OFFICE, 2021, p. 4). A distinção de ambas as tecnologias é feita da seguinte forma pela Autoridade de Proteção de Dados do Reino Unido.

> Reconhecimento facial é o processo pelo qual uma pessoa pode ser identificada e reconhecida a partir de uma imagem facial em meio digital. Câmeras são usadas para capturar estas imagens e o software FRT produz um modelo biométrico. O sistema estima o grau de semelhança entre dois modelos faciais (por exemplo, verificar a identidade de alguém), ou coloca um modelo em uma determinada categoria (por exemplo, faixa etária). FRT pode ser usado em uma variedade de contextos como desbloquear telefones celulares, configurar uma conta bancária on-line, ou passar através do controle

> de passaportes. Pode ajudar a tornar aspectos de nossas vidas mais fáceis, eficientes e seguras[18] (tradução do autor).
>
> Os usos do FRT referenciados acima normalmente envolvem um processo "um para um". O indivíduo participa diretamente e está ciente do uso dos dados. LFR é diferente, é tipicamente implantado de forma semelhante ao tradicional CCTV. É direcionado para todos em uma área específica, e não para um indivíduo específico. Essa tecnologia tem a capacidade de capturar os dados biométricos de todos aqueles que passem na área de alcance da câmera, de forma automática e indiscriminada. Os dados são coletados em tempo real e potencialmente em massa. Normalmente esse tipo de processamento é marcado pela falta de consciência, escolha ou controle pelos indivíduos[19] (tradução do autor) (INFORMATION COMMISSIONER'S OFFICE, 2021, p. 4).

A tecnologia envolvida no FRT, não é nova, teve início nos anos 60, e evoluiu ao longo do tempo. Com o ataque terrorista de 11 de setembro nos Estados Unidos, houve o crescimento na vigilância, a busca de antecipar-se a movimentos terroristas. Além disso, o aumento do uso da internet e de redes sociais, fez com que aparecessem novas formas de golpes e roubos de identidade, tornando o reconhecimento facial um instrumento para evitar tais problemas e trazer mais segurança a negócios no ambiente da internet. Outro ponto a se destacar são as cidades inteligentes, que fazem uso de câmeras de coleta de imagens que visam gerar *insights* para evolução do ambiente urbano, sendo que tais câmeras permitem também o rastreio de indivíduos (ANDREJEVIC; SELWYN, 2022).

Temos diferentes usos dessa tecnologia. A China possui um sistema de 200 milhões de câmeras, capaz de identificar os seus 1,4 bilhões de habitantes.

---

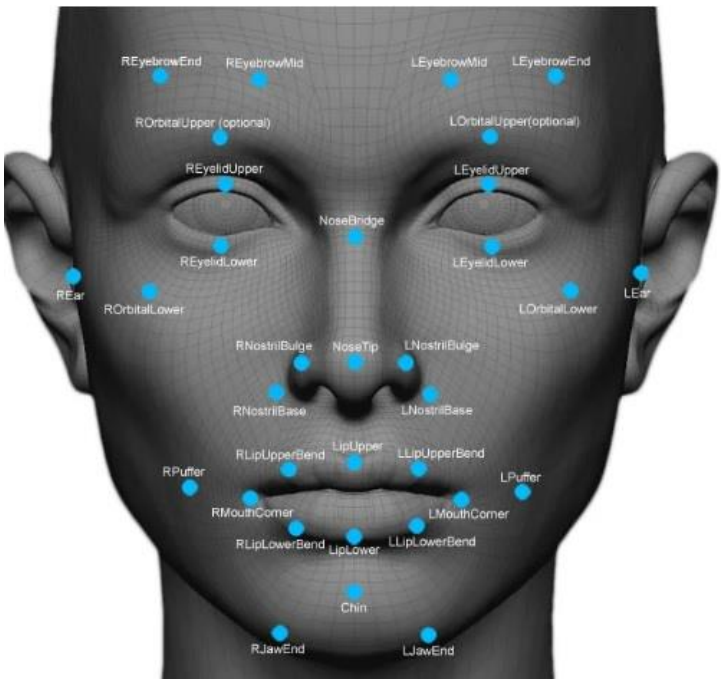
[18] Facial recognition is the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and FRT software produces a biometric template. Often, the system will then estimate the degree of similarity between two facial Templates to identify a match (eg to verify someone's identity), or to place a template in a particular category (eg age group). FRT can be used in a variety of contexts from unlocking our mobile phones, to setting up a bank account online, or passing through passport control. It can help make aspects of our lives easier, more efficient and more secure. (INFORMATION COMMISSIONER'S OFFICE, 2021, p. 4)

[19] The uses of FRT referenced above typically involve a "one-to-one" process. The individual participates directly and is aware of why and how their data is being used. LFR is different and is typically deployed in a similar way to traditional CCTV. It is directed towards everyone in a particular area rather than specific individuals. It has the ability to capture the biometric data of all individuals passing within range of the camera automatically and indiscriminately. Their data is collected in real-time and potentially on a mass scale. There is often a lack of awareness, choice or control for the individual in this process. (INFORMATION COMMISSIONER'S OFFICE, 2021, p. 4)

Em Dubai, 80 câmeras de segurança escaneiam e analisam os rostos das pessoas que chegam ao aeroporto, permitindo a entrada no país ou emitindo um alerta de segurança (COSTA, OLIVEIRA, 2019, p. 2).

A capacidade do computador analisar em uma foto ou vídeo e detectar um rosto é uma das tarefas possíveis, sendo essa um percursor essencial para a classificação e identificação de rostos (BUOLAMWINI, 2017, p. 13). Esse reconhecimento envolve medições chave da imagem da face, tais como a projeção do nariz, a distância dos olhos, como esses se alinham, a existência de covinha no queixo, cicatrizes, dentre outros pontos, chamados de pontos nodais, na imagem que está sendo avaliada (ANDREJEVIC; SELWYN, 2022, p. 27).

Figura 1: Pontos nodais usados no mapeamento do rosto




Fonte: MENA, Isabela, 2018.[20]

Na imagem é possível verificar alguns dos pontos que podem ser utilizados para a operação de um reconhecimento facial, analisando teste,

[20] Fonte: MENA, Isabela. **Verbete Draft:** o que é Reconhecimento Facial. 30 maio 2018. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/ Acesso em: 02 nov. 2022.

sobrancelhas, pálpebras, nariz, boca, queixo, bochechas. Esses pontos são calculados gerando ao final da aplicação de cálculos matemáticos, um *template*, que será avaliado contra a imagem que se quer comparar.

Uma vez detectado o rosto, a classificação pode ser realizada pelo algoritmo observando alguns atributos, Buolamwini (2017, p. 22) traz em sua pesquisa uma taxonomia biométrica conforme tabela abaixo.

Tabela 2 – Taxonomia biométrica

| | |
|---|---|
| Atributos demográficos | Idade, gênero, etnia, olhos, cabelos, cor da pele |
| Antropometria e atributos geométricos | Geometria do corpo e geometria facial |
| Atributos médicos | Condições de saúde, corpo, peso, rugas, índice de massa corpórea |
| Atributos materiais e comportamentais | Chapéu, cachecol, mala, roupas, lentes, óculos |

Tradução do autor.

Um processo de classificação é conseguido também através de um processo de treinamento para que a máquina possa aprender a classificar corretamente, pois o computador não sabe o que é um chapéu, ao menos que aqueles que estão treinando a máquina lhe deem as informações, indicando o que é e em que quantidade para poder buscar e classificar, dada as diferenças que podem existir (modelos, cores, ângulos, iluminação etc.).

Nesse contexto, entra a figura do *Big Data,* já mencionado nesta dissertação, o qual é utilizado como entrada para este treinamento, provendo diferentes dados que podem ser cruzados e trabalhados de forma mais otimizada, em razão da arquitetura estruturada para trabalhar com grandes volumes.

Temos dessa forma um forte treinamento tanto para a detecção quanto para a classificação, onde a massa de dados utilizada é de suma importância para não enviesar o aprendizado.

Neste processo de aprendizado a curadoria de todo o ciclo de desenvolvimento faz-se necessária. Para Buolamwini (2017, p. 15) deve-se coletar dados que representem a população alvo, e nessa curadoria deve trazer o questionamento contínuo sobre a representação do público alvo por esses dados. Deve ser levada em consideração ainda a variação dentro do grupo, então o reaproveitamento dos dados deve ser analisado. A autora traz, ainda, que

> (...) pessoas que se identificam com a mesma raça podem exibir uma série de características fenotípicas, como cor da pele e geometria facial. Em visão computacional, a curadoria do espectro completo para tarefas de análise facial deve atender rigorosamente à variação intragrupo bem como as diferenças intergrupais (tradução do autor)[21] (BUOLAMWINI, 2017, p. 15).

Essa é uma importante observação a ser aplicada no processo de formação da base que treinará o modelo de reconhecimento facial. Pretos, pardos, indígenas, asiáticos e brancos não são iguais dentro de seus grupos, por isso é importante que a seleção de dados de treinamento considere as diferenças de tom de pele e outras características, como por exemplo, o cabelo.

Neste sentido, um grupo aleatório de imagens de pessoas pode não representar a diversidade do público alvo do tratamento.

Conforme Moreira (2020, p. 514), grande parte dos programadores responsáveis por desenvolver as soluções não possuem contato social constante com grupos minorizados, o que tende a levá-los a considerar a homogeneidade de características dos membros. Isso impacta diretamente o processo de aprendizado do modelo que estes programadores atuam a não levar todas as características necessárias.

Desenvolver hoje utilizando a Inteligência Artificial se tornou mais fácil, empresas como IBM, Google, Microsoft e Amazon oferecem serviços para que outros desenvolvam, disponibilizando recursos para processamento de

[21] “people who self-identify with the same race can exhibit a range of phenotypic features such as skin color and facial geometry. In computer vision, fullspectrum curation for facial analysis tasks must rigorously attend to intragroup variation as well as intergroup diferences” (BUOLAMWINI, 2017, p. 15).

linguagem natural, descoberta de padrões, modelos de aprendizado de máquina e visão computacional (SILVA, 2020, p. 434). Por visão computacional se entende o processo compreendido pela coleta, análise e síntese dos dados visuais, com o objetivo de identificar rostos e realizar a biometria destes, além de outros processamentos visuais, como com objetos, por exemplo (SILVA, 2020, p. 434).

Essa disponibilidade é extremamente positiva para o desenvolvimento de soluções, dado que empresas que não possuem condições, *know-how* para montar uma estrutura, passam a ter acesso e a desenvolver soluções, porém aumenta a preocupação quanto ao desenvolvimento que não leva em consideração os pontos éticos elencados anteriormente, que podem gerar análises racistas e discriminatórias.

O próprio termo reconhecimento merece ressalvas, conforme Andrejevic e Selwyn (2022, p. 14), o modelo não reconhece efetivamente uma pessoa, ele gera uma probabilidade em razão de parâmetros de entrada *versus* os parâmetros que já possui e esse processamento não alcança 100% de certeza. O termo reconhecer acaba deixando de lado essa imprecisão, pois a máquina não conhece ou identifica, ela gera um conjunto de probabilidades. Em termos concretos, a máquina vai dizer que há, por exemplo, 95% de chances de correspondência entre o que está sendo imputado no modelo e a fonte de comparação. Vamos abordar agora um pouco mais essa imprecisão e exemplos práticos de tratamentos que ocorreram, onde os vieses acabaram interferindo no resultado.

## 5.1 VIESES EM PROCESSOS DE COLETA E RECONHECIMENTO

Existe uma falta de precisão no processo de reconhecimento facial, um exemplo disso, é o software *Amazon Rekognition*. Esse software revelou resultados não muito precisos, em um teste ele confundiu as fotos de 28 congressistas americanos indicando pessoas presas. O erro em torno de 5% não parece algo alto, mas tudo depende em qual lado da porcentagem você cairia. Para esses 5% (cinco por cento), poderia significar risco à liberdade, como no

caso de Robert Willians, que em janeiro de 2020 teve sua imagem confundida com as imagens captadas pelo circuito de CFTV, sendo solto apenas quando o dono da loja assaltada confirmou que não se tratava do assaltante. O processo todo levou mais de 30 horas e apenas para registro, Robert é um homem negro (OLIVEIRA, 2021, p. 67).

Oliveira (2021, p. 68) cita ainda como exemplo o software de reconhecimento facial utilizado nos aeroportos do Reino Unido, que possuía uma taxa de acerto em torno de 19%, informação trazida pelo autor a partir de estudo de 2020 realizado pela Universidade de Essex.

> Alguns grupos não só são deixados de lado ou ignorados na produção de tecnologias hegemônicas como são estereotipados e agredidos intelectualmente na montagem dos recursos computacionais que se tornam fundações para novas tecnologias, acumulando camadas estruturais de preconceitos (SILVA, 2022, p. 97).

Com essa visão tecnológica, os casos de vieses acabam por acontecer, abaixo temos uma tabela de Silva (2020, p. 436) com a seleção de casos relacionados ao viés racista de algoritmos no processamento facial. É possível verificar também qual foi o problema, de que forma esses processamentos foram racistas e as causas que geraram tais resultados.

Tabela 3 – Casos de vieses algoritmos

| Caso | Data | Problema | Causa |
|---|---|---|---|
| Reconhecimento de faces de computador HP não reconhece usuário negro | 12/2009 | Desumanização; Invisibilidade | Base de dados insuficiente<br><br>Ausência de testes |
| Google marca pessoas negras como gorilas | 07/2015 | Representação e associação racista; desumanização | Base de dados insuficiente<br><br>Base de dados com associações racistas intencionais<br><br>Ausência de testes |

| | | | |
|---|---|---|---|
| Robôs interagentes não encontram rosto de mulher negra | 03/2017 | Desumanização; Invisibilidade | Base de dados insuficiente<br><br>Ausência de testes |
| Faceapp embranquece pele para deixar “mais bonita” a selfie | 04/2017 | Representação eurocêntrica de beleza; desumanização | Base de dados insuficiente<br><br>Ausência de testes |
| APIs não reconhecem gênero e idade de mulheres negras | 02/2018 | Representação eurocêntrica de gênero e idade; | Base de dados insuficiente<br><br>Ausência de testes |
| Kairos retira do ar aplicativo de “diversidade” | 06/2018 | Tipologia racial essencialista | Tipologia centrada nos EUA |
| APIs de análise de expressões faciais associam emoções negativas a negros | 01/2019 | Percepção eurocêntrica;<br><br>Racismo Estereotipização | Base de dados insuficiente<br><br>Ausência de testes |
| Google Vision confunde cabelo negro com peruca | 02/2019 | Reforço de apropriação cultural; desumanização | Base de dados insuficientes<br><br>Base de dados com exemplos de apropriação estético-cultural<br><br>Ausência de testes |
| Carros autônomos têm mais chance de atropelar pessoas negras | 03/2019 | Desumanização; risco físico direto | Base de dados insuficiente<br><br>Ausência de testes |

Fonte: SILVA (2020, p. 436)

Percebe-se nos exemplos listados, que a insuficiência da dados na base de entrada mais a falta de testes trouxeram a problemática dos casos de falha do reconhecimento facial. Parece não ter havido a preocupação com outros

grupos, preocupando-se com o funcionamento para o grupo hegemônico, homem branco, em detrimento dos demais grupos possíveis. Como já abordado em diferentes pontos deste trabalho, o processo de aprendizado do modelo depende de uma base de entrada que possua diferentes condições que serão encontradas na realidade, pois o processo de aprendizagem será tão bem sucedido quanto o treinamento for capaz de apresentar as condições para que o modelo possa captar os padrões e consiga fazer as relações. No processo, como também vimos, o feedback é importante para os ajustes, então testar, verificando os resultados e ajustando o modelo para que esse funcione da forma mais adequada.

Outros casos trazidos por Silva (2019, online) são:

- *Stable difufusion* apresenta fotos de homens negros em resposta a termo sobre gangue (Agosto/2022);
- *Iphone* não reconhece rostos com tatuagens tradicionais maori (Agosto/2022);
- Desenvolvedor alterou o *thriller* do filme da pequena sereia, trocando a atriz negra por uma ruiva (Setembro/2022);
- Canva apresenta apenas fotos de noivas brancas nas 12 primeiras páginas de resultado de pesquisa (Maio/2022);
- Aplicativo Giggle impede a entrada de mulheres trans e mulheres negras cis (Dezembro/2021);
- Algoritmo do Facebook analisa vídeo e indica que homem negro é um primata (Setembro/2021);
- Um App Dermatológico da Google não funciona corretamente para pele negra (Maio/2021).

Esses são apenas alguns exemplos de muitos outros que o levantamento de Silva (2019, online) traz, uma linha do tempo com diferentes casos de vieses algoritmos, tanto de reconhecimento facial, quanto vieses de outros tipos relacionados a raça e etnia. Trago esses casos por serem extremamente recentes, o que demonstra que é uma realidade, inclusive nas grandes *big techs* como Meta e Google.

E por falar em grandes *big techs*, analisando o resultado na identificação facial por gênero e raça, é possível verificar grandes diferenças, tendo os melhores acertos para homens de pele clara, chegando a 100% na aplicação da Microsoft, 99,2% no Face++ e 99,7% no IBM. Porém, ao considerar a mudança de gênero e raça, esses percentuais caem, sendo o menor *match* a análise de imagens de mulheres de pele escura, onde a Microsoft alcança 79,2%, Face++ 65,5% e IBM 65,3%. A diferença de assertividade no pior caso, a aplicação da IBM, é de 34,4% (SILVA, 2022, p. 93).

A *National Institute of Standards and Techonology*, instituto de padrões e tecnologias dos Estados Unidos da América, realizou uma avaliação em 2019 com 189 algoritmos onde identificou-se que a taxa de falsos positivos é de 10 a 100 vezes maior quando a imagem analisada é de uma pessoa negra, asiática ou de povos originários, ocorrendo de forma mais acentuada para as pessoas negras em sistemas relacionados à atividade policial (SILVA, 2022, p. 120).

Um estudo postado no Twitter em 2020 mostra como um algoritmo de inteligência artificial do Google, o Google Vision Cloud, analisa duas fotos e quais *labels* são atribuídos a cada uma delas. A imagem é de uma mão segurando um termômetro digital de medição a distância. Em uma das imagens a mão é branca e em outra a mão é preta, sendo o termômetro o mesma para ambos os casos. Para a mão preta a etiqueta arma apareceu apontando 61% de certeza de ser uma arma, já para a mão branca, essa etiqueta não apareceu. O Google pediu desculpas pelo ocorrido e disse que corrigiu o problema, o que fez com que a mão preta não aparecesse mais a etiqueta de arma[22].

Como já observado durante este trabalho, uma aplicação de Inteligência Artificial utiliza-se de complexos modelos para alcançar seus objetivos e isso também vale para o processo de reconhecimento facial, escopo de difícil explicação e compreensão pelos titulares. Nesse sentido, manter a transparência como um meio para que o titular tenha o controle e possa se opor acaba não sendo suficiente. Neste cenário temos o princípio da precaução que

[22] KAYSER-BRIL, Nicolas. **Google apologizes after its Vision AI produced racist results**. 07 abr. 2020. Disponível em: https://algorithmwatch.org/en/google-vision-racism/ Acesso em: 10 nov. 2022.

pode auxiliar o processo de desenvolvimento da solução. Abordemos esse princípio.

## 5.2 O PRINCÍPIO DA PRECAUÇÃO APLICADO AO RECONHECIMENTO FACIAL

Bioni e Luciano (2020, p. 220) explicitam que o cenário do reconhecimento facial levanta incertezas quanto aos benefícios e os riscos de sua aplicação, e nesse sentido, apresentam-se três visões, uma que clama pelo banimento das soluções; uma que acredita ser suficiente a autorregulação e diretrizes éticas; e no meio dessas duas uma visão que busca uma arquitetura precaucionaria dos danos, com ações de quem está construindo a solução de reconhecimento facial para mitigar os riscos sobre os titulares.

O princípio da precaução tem sua gênesis nos anos 70, com iniciativas de proteção ambiental em um cenário onde as regulações de risco, com o levantamento, gerenciamento e a análise de custo benefício, não pareciam dar conta de cenários desconhecidos (BIONI; LUCIANO, 2020, p. 208). Este é um cenário que também é possível de ser trazido para o contexto da Inteligência Artificial e mais precisamente, neste trabalho, para o Reconhecimento Facial, uma vez que possui riscos de danos ou o desconhecimento dos malefícios possíveis (BIONI; LUCIANO, 2020, p. 226). O princípio apresenta dois pontos que são

> a) a abertura do debate regulatório a todos os atores envolvidos na implementação dessa tecnologia (e nas escolhas que ela impõe), de desenvolvedores àqueles que sofrerão seus possíveis efeitos, o que é um requisito obrigatório de um sistema democrático com históricas dinâmicas de assimetria de poder e informação; b) a atribuição de obrigações que reduzam as incertezas quanto aos benefícios e riscos em questão, de sorte a determinar a adoção ou não de IA (BIONI; LUCIANO, 2020, p. 226).

Como já citado anteriormente, há um desconhecimento sobre as minorias, Moreira (2020) trouxe que programadores não possuem proximidade, convívio com o público que compõe tais grupos. Este desconhecimento repercute na base de dados utilizada no treinamento, no desenho do modelo e nos ciclos de

feedback, gerando assim um algoritmo enviesado. Considerando o impacto na vida das pessoas, trazer a discussão de todos os atores envolvidos mostra-se de suma importância. *Big techs*, grupos minoritários, academia, órgãos de segurança pública, dentre outros, precisam participar dos debates visando que a regulação organize e traga mais segurança ao processo.

O segundo ponto traz a importância de uma análise de riscos logo no começo do processo, avaliando-os, documentando-os, buscando formas de mitigá-los, analisando os possíveis impactos em uma avaliação para determinar a aplicação ou não da solução frente o cenário levantado e os impactos encontrados.

Trabalhar dessa forma, ter essa preocupação, além das boas práticas já mencionadas, possibilita uma diminuição dos vieses e um acompanhamento contínuo, a detecção de casos anômalos e os ajustes necessários. Como a inteligência artificial trabalha com padrões, essa possibilidade pode trazer à tona pensamentos antigos que seriam expandidos e acelerados com o volume de dados e a capacidade de processamento dos computadores. Abordaremos agora a visão lombrosiana e o quão enviesada é essa forma.

## 5.3 O PERIGO DO OLHAR LOMBROSIANO E A FALÁCIA DA TECNOLOGIA NEUTRA

Cesare Lombroso, médico italiano, nascido em 1835 dedicou-se à medicina legal com pesquisas que buscavam relacionar características físicas à ação de delinquir. Conforme sua biografia no livro O Homem Delinquente

> foi a pesquisa constante na medicina legal, dos caracteres físicos e fisiológicos, como o tamanho da mandíbula, a conformação do cérebro, a estrutura óssea e a hereditariedade biológica, referida como atavismo. O criminoso é geneticamente determinado para o mal, por razões congênitas. Ele traz no seu âmago a reminiscência de comportamento adquirido na sua evolução psicofisiológica. É uma tendência inata para o crime (LOMBROSO, 2013, p. 9).

No pensamento de Lombroso, era possível verificar pessoas que tinham aptidão para delinquir através da análise de suas características e para esses

seu entendimento é que era necessário isolá-las para sempre, mostrando-se favorável à pena de morte e à prisão perpétua (LOMBROSO, 2013, p. 9).

Conforme Vaz e Ramos (2021, p. 156) para o médico italiano o caráter hereditário do crime poderia ser medido a partir da anatomia e seus estudos levavam em consideração “mandíbulas grandes, orelhas em forma de alça, arcos superciliares proeminentes, pele mais escura, baixa sensibilidade a dor, o uso de tatuagens, etc.” Há uma associação a povos considerados inferiores, sendo eles negros, ciganos e selvagens americanos. Temos um forte viés de raça, trazendo à tona a premissa de que esse grupo minorizado estava mais propenso a delinquir.

Tal pensamento lombrosiano encontrou ressonância em terras brasileiras com Raymundo Nina Rodrigues, que defendia a relativização da responsabilidade penal para as raças inferiores, leia-se negros, índios e mestiços, atribuindo-lhes um comportamento criminoso e insano, devendo ser considerado o quesito raça na formulação das normas jurídicas, havendo inclusive, a necessidade de criação de códigos penais diferentes, aplicados conforme a raça (VAZ; RAMOS, 2021, p. 157 – 158).

Pode-se pensar que esses são pensamentos ultrapassados, do já longínquo século XIX, que agora em pleno século XXI tais abordagens não encontram mais guarida no nosso atual patamar de desenvolvimento, mas infelizmente a realidade não se apresenta desta forma.

A inteligência artificial deu um novo fôlego para essa linha de pensamento, havendo estudos que buscam identificar padrões faciais, de expressão, de movimentação corporal. Um estudo chinês de 2016 buscou por padrões em rostos de criminosos em uma base com 2 mil fotos. As críticas que foram lançadas contra o projeto foram refutadas pelos pesquisadores alegando que o aprendizado de máquina é neutro e que o estudo pode ter sido o primeiro sem qualquer interferência de vieses subjetivos dos observadores humanos (SILVA, 2022, p. 131).

Na Inglaterra e em Israel existem casos de empresas que tem como proposito determinar, no caso inglês, o estado mental e as intenções de uma

pessoa através das expressões faciais, posturas, gestos e movimentos. Já no caso israelense, a *startup* propunha-se através do reconhecimento facial e aprendizado de máquina classificar as faces em “potenciais pesquisadores, ‘QI alto’, pedófilos, jogadores de pôquer, terroristas ou criminosos do colarinho branco” (SILVA, 2022, p. 131 - 132).

Então dada uma imagem, uma foto, os modelos propostos seriam capazes de definir que aquela pessoa é um pedófilo, um terrorista, saber as intenções que ela possui, usando para isso o aprendizado de máquina. Como visto anteriormente, esses modelos são treinados, a massa de dados de entrada para treinamento tem um elevado peso para o direcionamento dos resultados, além das pessoas envolvidas na construção do modelo. Por todo o expresso até aqui, fica difícil concluir que a tecnologia de inteligência artificial e o aprendizado de máquina são neutros e que seus resultados seriam desprovidos da subjetividade e dos vieses humanos. A tecnologia não é neutra, ela acaba por refletir os valores, os interesses daqueles que estão construindo a solução, sendo moldada pelas mesmas estruturas que existem na sociedade, estruturas de desigualdade (ACHIUME, 2020, p. 4).

Para Silva (2022, p. 183) esse olhar de neutralidade faz parte da dupla opacidade, onde grupos hegemônicos apresentam a visão de neutralidade e também dissipam o debate sobre o racismo e assim mantém a hegemonia, as vantagens que estruturalmente acabam usufruindo.

## CONSIDERAÇÕES FINAIS

Em números recentes somos em torno de 8 bilhões de seres humanos na face da terra. São 8 bilhões de homens, mulheres e crianças, são 8 bilhões de pessoas brancas, negras, pardas, indígenas, asiáticas, PCDs, heterossexuais, LGBTQIA+, magras, gordas, altas, baixas, professantes ou não de diferentes religiões. A humanidade é diversificada, com diferentes valores, formas de ver o mundo e assim caminhamos rumo ao futuro, observando acertos e barbaridades cometidas no passado, perpetuadas ou não no presente e à espera de qual futuro?

Procurando pelo outro significado de humanidade temos que é um "sentimento de bondade, benevolência, em relação aos semelhantes, ou de compaixão, piedade, em relação aos desfavorecidos", mas infelizmente existem diferentes episódios em que o significado não se transpôs para a realidade e a prática não imitou a teoria. É de simples observação que há discrepâncias de tratamento, de rendimentos financeiros e de oportunidades – inclusive de vida ou de morte - entre pessoas brancas e negras, homens e mulheres e outras interseccionalidades. O homem padrão das estatísticas repressoras do estado, tem cor definida, assim como a cor que acompanha o servir e o limpar, sem qualquer demérito destas atividades tão importantes e dignas, mas por que não se veem pessoas loiras de olhos azuis limpando banheiros na mesma proporção que as vemos sendo servidas? é mais que coincidência, destino ou sorte, é uma construção que vem de muito tempo atrás e permanece atual, está enraizada, é estrutural e estruturante das relações.

Discriminação, preconceito e tantos 'ismos', como o racismo, que é objeto deste trabalho, estão presentes nos números, estatísticas, dos estudos que aqui foram utilizados para demonstrar as discrepâncias e o assunto é urgente, pois é muito mais que números, possuem nome, idade, sonhos, família, pai, mãe, filho, filha, marido, esposa, são pessoas, uma das 8 bilhões que compõem, como você e eu, a humanidade, mas que por algum critério, são diminuídas, desprivilegiadas, tolhidas e no contexto digital, mais integrado, com mais informação, essa realidade se perpetua, trazendo visões de outrora para esse mundo novo do digital, da conexão.

Como desenvolvido no decorrer deste trabalho, vivemos hoje em uma Sociedade da Informação e nesta sociedade os dados possuem grande importância, um grande valor, assim como a terra, a eletricidade, a máquina a vapor foram agentes transformadores em outros momentos da humanidade, os dados são hoje aquilo que move a Sociedade da Informação. O cruzamento dos dados, gerando informações e *insights* permitem que novos negócios surjam, necessidades sejam criadas, atuando de forma direta sobre as pessoas, conhecendo seus gostos, seus direcionamentos e atendendo-as.

Nesse contexto entram leis que buscam organizar o tratamento dos dados pessoais, e no contexto brasileiro temos a lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD) que traz o titular ao centro, dando-lhe direitos e trazendo responsabilidades para aqueles que efetuem os tratamentos de dados pessoais, seja determinando estes tratamentos, os controladores, quanto executando esses tratamentos, os operadores, que passam a precisar observar e se preocupar com princípios, bases legais, direitos, dentre outros aspectos. Se antes se utilizava dados à revelia do titular e da forma como bem aprouvesse, agora um processo de governança precisa ser adotado, trazendo controle e transparência sobre o que é feito com os dados pessoais, permitindo ao titular conhecer e fazer uso de seus direitos perante o controlador. Essa é uma importante evolução jurídica, onde em um mundo digital, desconhecido em seus meandros por grande parcela da sociedade, termos leis que tragam princípios, regras, direitos e a previsão fiscalizatória, com suas devidas sanções pelo descumprimento, é necessário para organizar esse mundo digital.

Dentro desse escopo destacam-se os dados pessoais sensíveis que, como pode ser verificado, são dados que podem trazer impacto aos direitos e garantias dos titulares, para a LGPD são dados de “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;”. Há uma maior preocupação por parte do legislador no uso desses dados pessoais, necessitando uma maior atenção em seu uso. Observar a história permite enxergarmos perseguições e mortes que ocorreram, como por exemplo, judeus, ciganos, pessoas com deficiência, comunistas em campos de concentração da

Alemanha nazista. Lembrar disso é importante para não repetir, mas os tratamentos desses dados não desembocam apenas ao resultado morte, a discriminação pode trazer a falta de direitos, dificuldades na busca de um emprego, ser “confundido” como alguém que pode trazer perigo à sociedade, trazendo impacto na vida e no desenvolvimento das pessoas.

Vale destacar o princípio da não discriminação presente na LGPD, sendo um dos dez princípios que a lei esculpe e que norteiam o tratamento dos dados pessoais e dados pessoais sensíveis. Em uma sociedade da informação, o tratamento dos dados repercute na vida das pessoas e na sociedade em geral, desde as decisões em uma eleição que pode ser direcionada com o uso dos aprendizados gerados a partir dos dados obtidos pela pegadas digitais das pessoas, até mesmo a decisão de dar ou não crédito, a oportunidade ou não para uma vaga de trabalho, para entrar ou não em um país, seja para trabalhar ou passear. O digital se faz totalmente real na vida de cada um de nós.

Por todo o exposto, temos casos e mais casos de discriminação, onde o foco deste trabalho deteve-se sobre o prisma do racismo, atitude que vem há séculos sendo perpetuada na sociedade brasileira, e não só nela, gerando abismos de oportunidades, exclusão e tratamentos totalmente diversos, num imaginário de que um pobre e preto tem maior tendência a ser um perigo para a sociedade, apesar dos agentes parte dos constantes escândalos desta republica terem características totalmente diferentes, e causando efeitos danosos a uma coletividade quando não utiliza a rés pública da forma mais eficiente e eficaz em pró da sociedade.

Temos um racismo estrutural, entranhado na nossa sociedade e dado que as máquinas aprendem através dos dados que nós seres humanos geramos e introduzimos para que essas aprendam, o racismo estrutural tende a ser otimizado por máquinas rápidas e super eficazes em encontrar e perpetuar padrões, onde alguns exemplos foram dados durante este trabalho, casos recentes e em grandes organizações.

Torna-se assim imprescindível um trabalho rigoroso sobre o desenvolvimento de soluções em inteligência artificial e para o contexto deste

trabalho de visão computacional, trazendo governança ao processo, analisando os riscos que o uso dos modelos pode gerar para o público alvo e sendo esses riscos capazes de trazer impacto aos direitos e garantias, devem ser cuidados com rigor. A qualidade dos dados de entrada é fator preponderante do sucesso de um modelo ético, o universo de dados que compõe a massa de dados de treinamento devem trazer as diferentes características que o público alvo possuí, existem diferenças entre pretos, negros, orientais, por exemplo, e tais diferenças precisam ser ensinadas para os modelos, a fim de que estes identifiquem diferentes tonalidades de pele, diferentes tipos de penteados, desenhos de olhos, nariz, boca, dentre outros pontos avaliados. Um modelo que não tenha aprendido poderá gerar análises errôneas com potencial efeito sobre àqueles que são submetidos a esta análise, como por exemplo, ser identificado com um procurado pela justiça. O olhar no final não deve ser na tecnologia e sim nas pessoas e pelas pessoas, sendo a tecnologia o instrumento, o meio para a realização de uma atividade de forma otimizada.

Trazer novamente à tona ideias que liguem características físicas e potencialidade delitiva é algo grotesco, ideias como essa deveriam estar sepultadas a mais de século e não serem ressuscitadas com o uso da tecnologia. Os vieses estão presentes no desenvolvimento das soluções, estão nos dados que temos disponível para ensinar os modelos, está na visão de quem desenvolve os modelos, de quem acompanha a produção do serviço, acreditar que por ser uma máquina que afere um resultado, esse está livre dos vieses preconceituosos, livre de erros, é uma falácia perigosa.

O intuito deste trabalho não é demonizar a tecnologia da inteligência artificial e nesta, mais precisamente do reconhecimento facial. O reconhecimento facial é um importante instrumento para diminuir a probabilidade de fraudes em uma sociedade cada vez mais conectada, digital. O trabalho buscou trazer elementos que buscam dar segurança aos titulares que passam e passarão por processos de modelos algorítmicos, diminuindo os riscos para estes com governança, uso de boas práticas no desenvolvimento e testes, atenção ao público alvo e a representatividade deste nos treinamentos do modelos, dentre outros aspectos aqui abordados. Com isso mitigamos riscos e com acompanhamento, fiscalização e responsabilização, manter o funcionamento

desses modelos de forma segura às pessoas. Sigamos acompanhando como sociedade e atuando para a garantia dos direitos e garantias fundamentais de todas as pessoas, independente de quem seja, para a humanidade.

## REFERÊNCIAS

ACHIUME, E. Tendayi. **Racial Discrimination and Emerging Digital Technologies:** A Human Rights Analysis. United Nations General Assembly, 2020. Disponível em: https://digitallibrary.un.org/record/3879751. Acesso em: 11/11/2022.

ALMEIDA, Silvio Luiz de. **Racismo estrutural**. São Paulo: Pólen, 2019.

AMNESTY INTERNATIONAL; ACCESS NOW. **The Toronto Declaration (2018)**. Disponível em: https://www.torontodeclaration.org/declaration-text/english/ Acesso em: 28 out. 2022.

ANDERSEN, Lindsey. **Human Rights in the Age of Artificial Intelligence**. New York: AccessNow, 2018.

ANDREJEVIC, Mark; SELWYN, Neil. **Facial Recognition**. Edição do Kindle. Cambridge: Polity Press, 2022.

ANPD. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesde Tratamento_Final.pdf. Acesso em 15 abr. 2022.

ANPD. **Guia Orientativo** – Tratamento de Dados Pessoais pelo Poder Público. v. 1, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf Acesso em 15 abr. 2022.

ANUNCIAÇÃO, Diana; TRAD, Leny Alves Bonfim; FERREIRA, Tiago. "Mão na cabeça!": abordagem policial, racismo e violência estrutural entre jovens negros de três capitais do Nordeste. **Saúde e Sociedade**. 2020, v. 29, n. 1. Disponível em: https://www.scielo.br/j/sausoc/a/ctHxJZn497TXLJBhpSB8GRn/?lang=pt Acesso em: 22 abr. 2022.

BARRETO JUNIOR, Irineu Francisco; VENTURI JUNIOR, Gustavo. Inteligência Artificial e seus efeitos na Sociedade da Informação. *In:* LISBOA, Roberto Senise (Org.). **O Direito na Sociedade da Informação.** São Paulo: Almedina, 2020, v. 4.

BIONI, Bruno Ricardo; LUCIANO, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada? *In:* FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade.** 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 15 out. 2022.

BRASIL. Lei 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de

pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm Acesso em: 17 abr. 2022.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 23 jun. 2021.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1 Acesso em: 20 out. 2022.

BRUZZONE, Andrés. **Ciberpopulismo:** política e democracia no mundo digital. São Paulo: Contexto, 2021.

BUOLAMWINI, Joy Adowaa. **Gender Shades:** Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers. 2017. Supervisor: Ethan Zuckerman. Degree of Master of Science at the Massachusetts Institute of Technology.

BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por “legítimo interesse do controlador”: primeiras questões e apontamentos. *In*: FRAZÃO, Ana; OLIVIA, Milena Donato; TEPEDINO, Gustavo (Coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

CASTELLS, Manuel. **A Era da Informação:** economia, sociedade e cultura. 22. ed. São Paulo: Paz e Terra, v. I, 2020.

CARRERA, Fernanda. Algoritmização de estereótipos raciais em bancos de imagens: a persistência dos padrões coloniais Jezebel, Mammy e Sapphire para mulheres negras. **Palabra Clave**, v. 24, n. 3, p. e2433, 2021. Disponível em: https://palabraclave.unisabana.edu.co/index.php/palabraclave/article/view/14967. Acesso em: 26 maio 2022.

CAVOUKIAN, Ann. **Privacy by Design** - The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. 2010. Disponível: https://iap.org/resources/article/privacy-by-design-the-7-foundational-principles/; Acesso: 28 out. 2022.

CORMEN, Thomas. Desmistificando Algoritmos. Rio de Janeiro: Elsevier, 2014.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. O Uso de Tecnologias de Reconhecimento Facial em Sistemas de Vigilância e suas Implicações No Direito À Privacidade. **Revista de Direito, Governança e Novas Tecnologias**. Belém, v. 5, n. 2, p. 01-21, jul./dez., 2019.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: **Tratado de proteção de dados pessoais**. DONEDA, Danilo et al. (Coord.). Rio de Janeiro: Forense, 2021.

EUROPEAN PARLIAMENT. **Briefing EU Legislation in Progress** – Artificial intelligence act. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf Acesso em 28 out. 2022.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. Princípios que Regem o Tratamento de Dados no Brasil. *In*: **Comentários à Lei Geral de Proteção de Dados**. LEI n. 13.709/2018, Com alteração da Lei n. 13.853/2021. LIMA, Cíntia Rosa Pereira de (Coord.). São Paulo: Almedina, 2020.

GARCIA, Ana Cristina Bicharra. Ética e Inteligência Artificial. **Computação Brasil – Revista da Sociedade Brasileira de Computação**. Porto Alegre, n. 43, p. 14-22, novembro, 2020.

INFORMATION COMMISSIONER'S OFFICE. **Information Commissioner's Opinion: The use of live facial recognition technology in public places**. 2021. Disponível em: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf. Acesso em: 24 abr. 2022.

KAISER, Brittany. **Manipulados**: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque. 1 ed., Rio de Janeiro: Harper Collins, 2020.

KILOMBA, Grada. 1968. **Memórias da plantação:** episódios de racismo cotidiano. Rio de Janeiro: Editora Cobogó, 2019.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVIA, Milena Donato (coordenadores). 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais:** mecanismos de tutela para o livre desenvolvimento da personalidade. Orientador: Sergio Marcos Carvalho de Ávila Negri. Dissertação (Mestrado). Mestrado em Direito e Inovação. Universidade Federal de Juiz de Fora, 2019, 118 p. Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/11438 Acesso em: 16 abr. 2022.

LESLIE, David. **Understanding artificial intelligence ethics and safety**: A guide for the responsible design and implementation of AI systems in the public sector. London: The Alan Turing Institute, 2019.

LOMBROSO, Cesare. **O homem delinquente**. Tradução Sebastião José Roque. São Paulo: Ícone, 2013.

LUGER, George F. **Inteligência artificial:** estruturas e estratégias para a solução de problemas complexos. 4 ed. tradução Paulo Engel. Porto Alegre:Bookmann, 2004.

LUZ, Pedro Henrique Machado da; LOUREIRO, Maria Fernanda Battaglin. Privacidade e Proteção de Dados Pessoais: Os Novos Desafios na Sociedade em Rede. **Meritum**. Belo Horizonte, v. 13, n. 1, p. 69-86, jan./jun, 2018.

MASSENO, Manuel David. Como a União Europeia Procura Proteger os Cidadãos-Consumidores em Tempos de Big Data. **Revista Eletrônica do Curso de Direito da UFSM**. v. 14, n. 3, 2019.

MOTTA, Ivan Dias da; ABAGGE, Yasmine de Resende; KNOERR, Fernando Gustavo. A Lei Geral de Proteção de Dados: Os Dados Pessoais Podem Ser Considerados Direitos Da Personalidade? **Economic Analysis of Law Review**. v. 10, n. 2, p. 278-302, Mai-Ago, 2019.

MORAES, Izabelly Soares de; GONÇALVES, Priscila de Fátima; LEDUR, Cleverson Lopes; CÓRDOVA JUNIOR, Ramiro Sebastião; SARAIVA, Maurício de Oliveira; FRIGER, Sandra Rovena. **Introdução a Big Data e Internet das Coisas (IoT)**. Porto Alegre: SAGAH, 2018.

MOREIRA, Adilson José. **O que é discriminação?** Belo Horizonte: Letramento, 2017.

MOREIRA, Adilson José. **Tratado de Direito Antidiscriminatório**. São Paulo: Editora Contracorrente, 2020.

OLEIVEIRA, Samuel R. de. **Sorria, você está sendo filmado**: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

O'NEIL, Cathy. **Algoritmos de destruição em massa**: como o Big Data aumenta a desigualdade e ameaça à democracia. Santo André: Editora Rua do Sabão, 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 22 jun. 2020.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: **TIC Domicílios 2020**. São Paulo: Comitê Gestor da Internet no Brasil, 2021.

PARLAMENTO EUROPEU. Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da União, 2021/0106. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF Acesso em 28 out. 2022.

PELLIZZARI, Bruno Henrique Miniuchi; BARRETO JUNIOR, Irineu Francisco. Bolhas Sociais e seus Efeitos na Sociedade da Informação: Ditadura do Algoritmo e Entropia na Internet. **Revista de Direito, Governança e Novas Tecnologias**. Belém, v. 5, n. 2, p. 57-73, jul./dez., 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed, São Paulo: Saraiva Educação, 2020.

RAMOS, Silvia; SILVA, Pedro Paulo da. Dissecação do Enquadro In: **Negro trauma: racismo e abordagem policial no Rio de Janeiro**. Silvia Ramos, et al. ilustração Miguel Morgado. Rio de Janeiro: CESeC, 2022. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2022/02/CESEC_elemento-suspeito_final-3.pdf Acesso em 22 abr. 2022.

RODOTÀ, Stefano. **A vida na sociedade de vigilância** – a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROSÁRIO, Cícero Marcos Lopes do. **A proteção de dados pessoais sensíveis no Brasil**. Rio de Janeiro: Lumen Juris, 2021.

RUSSELL, Stuart Jonathan; NORVIG, Peter. **Inteligência Artificial**. 2ª ed. tradução de PubliCare Consultoria. Rio de Janeiro: Elsevier, 2004.

SARLETE, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. *In:* **Tratado de proteção de dados pessoais**. DONEDA, Danilo; et al. (coordenadores). Rio de Janeiro: Forense, 2021.

SENADO FEDERAL. Lei nº 13.853, de 8 de julho de 2019 – Veto. Mensagem Nº 288, de 8 de Julho de 2019. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2019/lei-13853-8-julho-2019-788785-veto-158685-pl.html Acesso em 29 out. 2022.

SENADO FEDERAL. Proposta de Emenda à Constituição nº 17, de 2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline Acesso em: 29 out. 2022.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 36. ed. revista e atualizada. São Paulo: Malheiros Editores, 2013.

SILVA, Lucas Gonçalves da; SANTOS, Elaine Celina Afra da Silva. O aumento das “fake news” durante a propaganda eleitoral e sua possível influência no resultado do pleito. **Revista Brasileira de Direitos e Garantias Fundamentais**, Goiânia, v. 5, n. 1, p. 1-19, jan./jun. 2019.

SILVA, Tarcízio. Linha do Tempo do Racismo Algorítmico. **Blog do Tarcízio Silva**, 2019. Disponível em: https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo. Acesso em: 30 out. 2022.

SILVA, Tarcizio da. VISÃO COMPUTACIONAL E RACISMO ALGORÍTMICO: BRANQUITUDE E OPACIDADE NO APRENDIZADO DE MÁQUINA. **Revista da Associação Brasileira de Pesquisadores/as Negros/as (ABPN)**, (S.l.), v. 12, n. 31, fev. 2020. ISSN 2177-2770. Disponível em: https://abpnrevista.org.br/index.php/site/article/view/744. Acesso em 30 out. 2022.

SILVA, Tarcízio. **Racismo algorítmico**. Edição do Kindle. São Paulo: Edições Sesc SP, 2022.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1-38, 9 mai. 2020.

TEIXEIRA, Lucas de Barros. Transparência algorítmica em soluções utilizadas por governos afora, e o contexto Brasil. **Revista de Tecnologia Aplicada (RTA)**. v. 10, n. 2, maio/ago., 2021.

UNITED KINGDON. **Guidance Data Ethics Framework** (2020). Disponível em: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020 Acessado em 25 out. 2022.

VAZ, Lívia Sant'anna; RAMOS, Chiara. **A justiça é uma mulher negra**. Belo Horizonte: Casa do Direito, 2021.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: A luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.