UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

GRADUAÇÃO

GLERISTON CARDOSO FÉLIX

DISCRIMINAÇÃO ALGORÍTMICA E O DIREITO À EXPLICAÇÃO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

FORTALEZA

2021

GLERISTON CARDOSO FÉLIX

DISCRIMINAÇÃO ALGORÍTMICA E O DIREITO À EXPLICAÇÃO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Monografia submetida à Coordenação do Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito. Área de concentração: Direito Civil.

Orientador: Prof. Dr. William Paiva Marques Júnior.

FORTALEZA

2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

F36d Félix, Gleriston Cardoso.
Discriminação algorítmica e o direito à explicação na lei geral de proteção de dados pessoais / Gleriston Cardoso Félix. – 2021.
64 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2021.
Orientação: Prof. Dr. William Paiva Marques Júnior.

1. decisões automatizadas. 2. discriminação algorítmica. 3. inteligência artificial. 4. proteção de dados. 5. profiling. I. Título.

CDD 340

GLERISTON CARDOSO FÉLIX

DISCRIMINAÇÃO ALGORÍTMICA E O DIREITO À EXPLICAÇÃO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Monografia submetida à Coordenação do Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito. Área de concentração: Direito Civil.

Aprovada em: __/__/____.

BANCA EXAMINADORA

_____
Prof. Dr. William Paiva Marques Júnior (Orientador)
Universidade Federal do Ceará (UFC)

_____
Profª. Msc. Fernanda Cláudia Araújo da Silva
Universidade Federal do Ceará (UFC)

_____
Mestranda Nathália Lima Pereira
Universidade Federal do Ceará (UFC)

A minha mãe, Maria Cardoso Félix (Leoniza), que sempre me apoiou e incentivou nos estudos. Também me ensinou a preciosa lição de manter a calma e a paciência em todos nos momentos difíceis da vida.

AGRADECIMENTOS

À Jeová Deus, que no seu grandioso poder nos concedeu algo tão perfeito e incrível como o cérebro cuja capacidade de processamento é espantosa.

Aos meus pais, pela dádiva da vida e o ensinamento de que o trabalho honesto e a perseverança podem ser recompensadores. Especialmente a minha mãe que sempre foi base sólida em nossa família e por seu exemplo mostrou que a paciência é a chave para uma boa convivência com todos.

Aos meus irmãos, especialmente a minha irmã Gleice Kelly, pelo apoio e o incentivo a continuar no curso de Direito.

Aos amigos que a Faculdade de Direito que de diversas maneiras contribuíram para o meu progresso no curso e que me ensinaram que compartilhar o conhecimento pode ser algo transformador na vida de uma pessoa.

Ao professor orientador, William Paiva Marques Júnior, pelo apoio e interesse no tema demonstrados desde o início do trabalho e pela orientação, paciência e apoio para o desenvolvimento deste trabalho.

À professora Fernanda Cláudia Araújo da Silva e a mestranda Nathália Lima Pereira por aceitarem o convite para participarem da banca examinadora.

Agradeço também o trabalho e esforço de todos os servidores e professores da Universidade Federal do Ceará que, de alguma forma, contribuíram para esta ocasião.

Agradeço em especial aos meus amigos do DONFP (eterno Serviço Norte de Medição, Controle e Proteção – SNCP) da Chesf (Companhia Hidroelétrica do São Francisco), sem os quais não conseguiria chegar até esse momento. Muito obrigado pela ajuda e apoio no decorrer desses anos.

“Algumas vezes, mudanças históricas gigantescas são simbolizadas por mudanças minúsculas no comportamento cotidiano.” (Alvin Toffler, 2012, p. 266).

RESUMO

O atual cenário de desenvolvimento das tecnologias de informação e comunicação difundiu o uso de dispositivos eletrônicos móveis que estão coletando constantemente dados e distribuindo os dados pessoais de seus titulares na internet. Com isso formou-se um oceano de dados que podem ser coletados, organizados em categorias ou perfis, tratados e por fim novas informações são criadas com base nesses dados primários. Logo, podemos receber serviços ou produtos mais personalizados que giram a roda da economia compartilhada. Contudo, além das benesses ora listadas, não passam despercebidos os possíveis riscos do uso indevido de dados pessoais. Considerando que entre as tecnologias para esse tratamento estão algoritmos de inteligência artificial, *Big Data* e técnicas de perfilamento (*profiling*), surge para o Direito brasileiro novas situações relacionadas entre a defesa de direitos fundamentais e a inovação tecnológica. Este trabalho tem por objetivo entender como os algoritmos de IA e técnicas de perfilização podem cometer discriminações por meio de decisões automatizadas e como a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) em seu artigo 20 pode defender os titulares de dados por garantir o direito à explicação e à revisão de decisões exclusivamente automatizadas que afetem os interesses desses titulares. Para isso abordam-se os fatores que ensejaram na indústria 4.0 e como a legislação da União Europeia evoluiu para a criação do Regulamento Geral de Proteção de Dados. Depois, verifica-se como o arcabouço jurídico brasileiro possui alguns institutos de proteção de dados anteriores a vigência da LGPD. Por fim, este trabalho analisa alguns exemplos de discriminações cometidas por algoritmos e demonstra como a LGPD traz institutos de defesa ao direito à explicação e à revisão de decisões exclusivamente automatizadas como ferramentas para o combate contra discriminação algorítmica. Com fins de atingir a pretensão ora listada, utilizou-se metodologia de pesquisa básica e compilação exploratória com abordagem qualitativa, efetuando-se pesquisa documental (artigos de lei e outros atos normativos). Também foi realizada pesquisa bibliográfica e revisão de literatura (artigos, doutrinas e revistas especializadas).

Palavras-chave: decisões automatizadas; discriminação algorítmica; inteligência artificial; proteção de dados; *profiling*.

ABSTRACT

The current scenario of development of information and communication technologies has spread the use of mobile electronic devices that are constantly collecting data and distributing the personal data of their holders on the internet. With this, an ocean of data was formed that can be collected, organized into categories or profiles, processed and finally new information is created based on this primary data. Therefore, we may receive more personalized services or products that turn the wheel of the shared economy. However, in addition to the benefits listed here, the possible risks of misuse of personal data do not go unnoticed. Considering that among the technologies for this treatment are artificial intelligence algorithms, Big Data and profiling techniques, new situations arise for Brazilian law related to the defense of fundamental rights and technological innovation. This work aims to understand how AI algorithms and profiling techniques can discriminate through automated decisions and how Law No. 13.709/2018 (General Law for the Protection of Personal Data) in its article 20 can defend data subjects by guaranteeing the right to explanation and review of exclusively automated decisions that affect the interests of these holders. For this, we sought to compile the factors that led to industry 4.0 and how the legislation of the European Union evolved towards the creation of the General Data Protection Regulation. Finally, it is verified how the Brazilian legal framework has some data protection institutes prior to the validity of the LGPD. Finally, this work analyzes some examples of discrimination committed by algorithms and demonstrates how the LGPD institutes defending the right to explanation and review of exclusively automated decisions as tools for combating algorithmic discrimination. In order to achieve the claim listed herein, basic research methodology and exploratory compilation with a qualitative approach were used, carrying out documentary research (articles of law and other normative acts). Bibliographic research and literature review (articles, doctrines and specialized journals) were also carried out.

Keywords: automated decisions; algorithmic discrimination; artificial intelligence; data protection; *profiling*.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
Art.	Artigo
Arts.	Artigos
CC/02	Código Civil de 2002
CDC	Código de Defesa do Consumidor
CI	Circuito Integrado
CPP	Código de Processo Penal
CRFB/88	Constituição da República Federativa do Brasil de 1998
GDPR	*General Data Protection Regulation*
IA	Inteligência Artificial
IoT	*Internet of Things*
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
RGPD	Regulamento Geral de Proteção de Dados
SGT13	Subgrupo de Trabalho número 13
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
UE	União Europeia
WWW	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

A adaptação do ser humano ao ambiente que o rodeia é uma das razões para o desenvolvimento e a inovação tecnológica. Verifica-se que da análise do caminhar da humanidade entre uma sociedade agrícola, passando pela pujança da era industrial e chegando a veloz sociedade da informação, mudanças trazidas por cada nova tecnologia transformou a forma como percebe-se o mundo e a maneira como as pessoas se relacionam entre si. De modo que o Direito não pode ficar alheio aos impactos gerados por essas mudanças. Embora este não seja tão rápido na regulação das transformações ocasionadas por uma nova tecnologia, ele precisa entrar em cena para garantir que exista um equilíbrio entre a defesa à direitos básicos e fundamentais da pessoa humana ou da coletividade e o progresso econômico e tecnológico.

Como exemplo destaque-se o campo das tecnologias de informação e telecomunicação. Com o aumento da eficiência do processamento de dados e a diminuição dos custos de produção e operação das redes de telecomunicações, criou-se um estado de constante conectividade entre as pessoas e um grande fluxo de dados em tempo real. Hoje, com a expansão do acesso à Internet e a possibilidade de que até as “coisas” (diversos dispositivos eletrônicos: relógios, geladeiras etc.) se conectem com o mundo, a circulação de dados aumentou de forma exponencial.

Esse incremento nos usos de dados ascende como poderosa força motriz que influencia na produtividade dos negócios, na melhora da qualidade de vida e da riqueza mundial. O que por sua vez atrai a atenção do mundo jurídico na regulação dessas novas relações entre o homem e a tecnologia. Além dos benefícios é necessário vigiarmos os perigos inerentes a essas tecnologias, dentre alguns considere-se: o aumento da vigilância, o risco à privacidade e outros danos à personalidade humana como a discriminação algorítmica.

O foco desta pesquisa concentra-se nos dados pessoais. Busca-se entender como o uso desses dados associados com as tecnologias de coleta e tratamento deles, como o *Big Data* e *Profiling* associados com a Inteligência Artificial, podem implicar em lesões ao corpo digital de um indivíduo e suas repercussões no mundo real. O objetivo desta pesquisa é apontar que embora o aumento na utilização dos algoritmos utilizados por computadores promova avanços

significativos no desenvolvimento da sociedade humana, os riscos que eles podem produzir merecem apreciação pelo Direito com a finalidade de que os danos provocados pelos algoritmos possam ser evitados ou que seus efeitos sejam reduzidos.

Para isso, procura-se compreender conceitos como tecnologias de inteligência artificial (IA), perfilização (*profiling*), internet das coisas (*Internet of Things – IoT*) e *Big Data* relacionam-se entre si e geram repercussões na vida das pessoas.

Depois observa-se como a gênese dos debates de proteção de dados em legislações em outros países ensejaram na construção da regulação europeia. Em seguida uma análise da legislação setorial brasileira pontua quais institutos podem ser usados para aspectos pontuais da proteção de dados e como é fundamental a criação de uma Lei Geral de Proteção de Dados que estabeleça bases sólidas para o desenvolvimento de uma cultura de segurança dos dados pessoais e proteção aos interesses do titular desses dados.

Por fim, aponta-se os usos das decisões automatizadas realizadas por algoritmos de inteligência artificial e os riscos da opacidade algorítmica. Diante de algo que para muitos é uma verdadeira caixa-preta como é o funcionamento de uma IA, caso ela tome uma decisão discriminatória que afete interesses da personalidade de uma pessoa, como esta poderá utilizar a Lei Geral de Proteção de Dados Pessoais para solicitar que haja uma revisão da decisão ou uma explicação sobre como essa decisão da IA foi tomada? Esta pesquisa tem como finalidade responder esse questionamento em seu último capítulo.

Para atingir esse fim, no decorrer desta obra utilizou-se metodologia de pesquisa básica e compilação exploratória com abordagem qualitativa, efetuando-se pesquisa documental (artigos de lei e outros atos normativos). Também foi realizada pesquisa bibliográfica e revisão de literatura (artigos, doutrinas e revistas especializadas).

2 A EVOLUÇÃO DA SOCIEDADE DA INFORMAÇÃO NO QUE TANGE À COLETA E AO TRATAMENTO DE DADOS PESSOAIS

Mudanças disruptivas na forma como a sociedade humana se relaciona entre si e com o planeta Terra são amostras de como o ser-humano possui uma notável capacidade de aprender com o ambiente ao seu redor e de usar este aprendizado como ferramenta para criar riquezas e comodidades em seu estilo de vida.

Dentre essas mudanças revolucionárias Alvin Toffler[1] destaca três grandes ondas sucessivas que abalariam as estruturas das civilizações humanas e que proporcionariam insumos para os seguidos avanços tecnológicos que ensejariam em uma sociedade banhada por informações sobre os mais variados assuntos do conhecimento humano e que seria notadamente marcada por meios de comunicações praticamente instantâneos.

A primeira grande onda revolucionária apontada por Toffler[2] foi a revolução agrícola. Esta permitiu que os seres humanos saíssem da condição de pequenos grupos nômades de coletores-caçadores para grupos sedentários maiores organizados em estruturas que seriam embriões das futuras cidades e detentores do conhecimento do cultivo da terra e da domesticação de animais, processo esse iniciado há cerca de 10.000 anos.

A segunda onda foi caracterizada por uma série de revoluções industriais que se iniciaram em meados do século XVIII e atingiram seu ápice na metade da década de 1950. Tais revoluções causaram grandes transformações nos sistemas de transportes por meio das ferrovias e das máquinas a vapor. Em seguida o uso da eletricidade com sistemas de linha de montagem nas indústrias permitiu a produção de bens econômicos em grande escala.

Com os avanços no campo da eletrônica e o advento da informática nasce a terceira onda. Esta possibilitaria a quebra de barreira entre produtores e consumidores e retornaria para o cenário econômico a figura do “prossumidor”.[3] Este deixaria de ser um mero espectador do processo produtivo e começaria a participar na criação, teste e aprimoramento de novos produtos, inclusive em mercados

---

[1] TOFFLER, Alvin. **A terceira onda.** 31. Ed. Rio de Janeiro: Record, 2012, p. 24 - 28.
[2] Ibidem, p. 24 - 28.
[3] TOFFLER. Alvin. Op. Cit., p. 270 - 288.

geograficamente distantes de sua moradia uma vez que os avanços nas telecomunicações possibilitariam um fluxo de informações mais rápido e barato.

Ainda no que tange à Revolução Industrial destaque-se que com a invenção do transistor[4] em 1947 pelos laboratórios Bell e o desenvolvimento do primeiro circuito integrado[5] (CI) pela Texas Instruments em 1958 iniciou-se a era dos componentes eletrônicos em estado sólido[6]. Logo, a partir de 1960 o processo de miniaturização de semicondutores e componentes eletrônicos favoreceu o surgimento da computação pessoal.

Segundo Patrícia Peck Pinheiro[7]:

> Os anos 1970 viram o advento do microprocessador, minúscula partícula de silício que centraliza o processamento em um computador e onde eram condensadas centenas de transistores, os elementos que faziam os computadores ocupar grandes espaços, consumir grande quantidade de energia e estar em constante manutenção. As centenas de transistores tornaram-se milhares, dezenas de milhares e, em nossa época, centenas de milhares, fazendo dos microcomputadores pessoais, que utilizamos em nossas casas e escritórios, engenhos com capacidade de processamento superior à das grandes universidades, laboratórios e empresas de trinta anos atrás.

Portanto, entre 1960 e 1980 a redução de custos de processamento de dados e o avanço na tecnologia de rede de computadores[8] possibilitou a construção da espinha dorsal do que seria a Internet na década de 1990. Esta evoluiu da oferta de simples recursos como o correio eletrônico, envio de arquivos simples e pequenos, acesso a *World Wide Web* (WWW) por meio de conexões discadas em via linhas telefônicas fixas residenciais para serviços de transmissão de áudio e vídeo em alta definição de imagem que exigem alta largura de banda proporcionada pela tecnologia de cabos de fibras ópticas e satélites.[9]

Todos esses avanços da tecnologia humana permitiram a criação do que Schwab denomina de quarta revolução industrial ou "indústria 4.0".[10] A aludida revolução que começou a partir dos anos 2000 foi impulsionada pelo aprimoramento

---

[4] "Pequeno dispositivo semicondutor usado para controlar o fluxo de eletricidade em um equipamento eletrônico." Conceito tirado em: HOUAISS, Antônio; VILLAR, Mauro d Salles. **Dicionário Houaiss da língua portuguesa**. 1.ed., Rio de Janeiro: Objetiva, 2009, p.1868.

[5] "Dispositivo que incorpora numa unidade de pequenas dimensões todos os componentes de um circuito eletrônico completo, desenhado para executar uma ou mais funções determinadas." Conceito tirado em: Ibidem, p.471.

[6] BOYLESTAD, Robert L. **Introdução à análise de circuitos**. 10. Ed., São Paulo: Pearson Prentice Hall, 2004, p.5.

[7] PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed., São Paulo: Saraiva Educação, 2021, p. 55.

[8] CASTELLS, Manoel. **A sociedade em rede**. 6. ed., São Paulo: Paz e Terra, 2002, p. 70 - 81.

[9] PINHEIRO, Patrícia Peck. Op. cit., p. 56 - 58.

[10] SCHWAB, Klaus. **A quarta revolução industrial.** 1. ed., São Paulo: Edipro, 2016, p. 15, 16.

das redes de telecomunicações e protocolos de comunicação de dados, criação de programas de computadores mais robustos, evolução de equipamentos eletrônicos com sistemas embarcados mais inteligentes e baratos, e avanços no campo da robótica, inteligência artificial e no desenvolvimento de sensores que permitem um tsunami de dados coletados em máquinas, animais e humanos para os mais diversos propósitos.

Em um contexto de permanente conectividade e aprimoramento de algoritmos e softwares o Conselho da Agenda Global do Fórum Econômico Mundial sobre o futuro do Software e da Sociedade publicou em setembro de 2015 o relatório de pesquisa Mudança Profunda – Pontos de Inflexão Tecnológicos e Impactos Sociais[11]. Neste relatório são apontadas tecnologias que impactarão consideravelmente as relações econômicas e sociais tais como: tecnologias implantáveis; maior presença no mundo digital proporcionadas pelo aumento do acesso à Internet e às redes sociais; tecnologias vestíveis (*wearables*); computação ubíqua; armazenamento de dados para todos (por meio do *cloud computing*); internet das coisas (IoT); *Big data*; Inteligência Artificial (IA), *Blockchain* etc[12]. As referidas tecnologias aumentarão exponencialmente a produção e o fluxo de dados em face de sua permeabilidade na vida das pessoas.

As supracitadas inovações tecnológicas permitirão que a sociedade humana adentre em um admirável mundo novo de comodidades em seu cotidiano e com o aumento da produtividade gerando consideráveis ganhos econômicos. Em face desse contexto os dados gerados por tais tecnologias passam a ocupar lugar de destaque no ordenamento jurídico. Pois, o uso adequado deles permite o desenvolvimento de novas modalidades de serviços e negócios, a melhoria na qualidade de vida e o livre fluxo de informações, entre outras vantagens. Contudo, o uso indevido desses dados trará como consequências negativas o aumento de vigilância indevida sobre as pessoas, o roubo de identidade, os riscos à privacidade, a manipulação do comportamento e outros efeitos danosos contra a pessoa humana.

Logo, diante desses possíveis cenários nascem questionamentos que serão

---

[11] SCHWAB, Klaus. Ibidem, p. 115 - 154.

[12] Fórum Econômico Mundial. **Deep Shift – Technology Tipping Points and Societal Impact**, Survey Report, Global Agenda Council on the Future of Software Societal Impact, 2015. Disponível em: <http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf>. Acesso em 24 de junho de 2021.

trazidos para análise do Direito. Como encontrar um ponto de equilíbrio entre a liberdade dessas aplicações tecnológicas, o incentivo a inovação e a regulação da proteção a direito fundamentais e a dignidade da pessoa humana protegidos pela Constituição Federal de 1988? Quais instrumentos trazem uma proteção para o titular dos dados pessoais quando se considera o ordenamento jurídico brasileiro?

Conforme destaca Bruno Ricardo Bioni[13] "[...] a informação é o elemento nuclear para o desenvolvimento da economia". Para a obtenção da informação como elemento estratégico para a tomada de decisão são necessários que os dados disponíveis no mundo virtual sejam coletados, ordenados e tratados. Logo, os dados gerados por nossa sociedade da informação viraram um insumo poderoso para a sociedade da informação, assim como o advento da eletricidade foi para a sociedade industrial[14].

Os dados digitais passaram a ser tratados como uma poderosa *commodity* sendo descritos como o novo petróleo de nossa sociedade. Contudo, conforme Wolfgang Hoffmann-Riem passa apontar existem similaridades e diferenças entre o petróleo bruto e dados digitais.[15]

Ao passo que o petróleo leva um grande período para a sua formação em face do acúmulo de matéria orgânica em bacias sedimentares, os dados digitais são gerados instantemente e possuem praticamente uma produção ilimitada uma vez que novas tecnologias e hábitos sociais promovem a expansão do estoque de dados. O petróleo exige o emprego de recursos caros de perfuração do solo para ser encontrado enquanto os processos de coleta, transporte e armazenamento de dados são mais rápidos, baratos e acessíveis. Outro ponto notável sobre os dados é que eles podem ser facilmente copiados e duplicados, diferente de outros ativos econômicos como por exemplo um carro que precisaria passar por uma linha de produção para que uma cópia fosse replicada ao passo que um registro contendo os dados de projeto do carro podem ser transferidos em segundos.[16] Assim como o petróleo pode passar pelo processo de refinamento para que novas aplicações e usos dele possam ser criadas, os dados brutos também podem ser "refinados".

---

[13] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed., Rio de Janeiro: Forense, 2020, p.4.
[14] Ibidem, p.5.
[15] HOFFMAN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital:** desafios para o direito. Tradução de Ítalo Fuhrmann. Rio de Janeiro: Forense, 2021. p. 19.
[16] BARBIERI, Carlos. **Governança de Dados:** Práticas, Conceitos e Novos Caminhos. Rio de Janeiro: Atlas Book, 2019, p. 7.

Segundo Hoffmann-Riem[17] sobre o tratamento de dados:

> Em todos os lugares há pequenas, mas também grandes, "refinarias" de dados, inclusive nas mãos de empresas particularmente poderosas, como Google, Facebook, Microsoft ou Amazon, bem como empresas de nuvem de dados especiais, como a Agência Nacional de Segurança dos EUA (NSA) ou outros serviços secretos. O processamento de dados cria mais conhecimento que transmite poder, não apenas nos mercados econômicos, mas pelo menos potencialmente em quase todas as áreas de ação social.

O supracitado autor ainda destaca que assim como o refino de petróleo pode resultar em derivados de qualidade superior, novas tecnologias como a inteligência artificial, por exemplo, podem ser empregadas na coleta e tratamento de dados gerando novos produtos com vantagens superiores aos simples dados brutos.

2.1 Uso da IA no tratamento de dados pessoais

Referente à IA Jonh McCathy, considerado um dos pioneiros no campo da IA[18], a define como "a ciência e a engenharia de criar máquinas inteligentes, especialmente programas de computador inteligentes"[19]. Já Hoffmann-Riem aborda a IA como "[...] esforço de reproduzir digitalmente estruturas de decisão semelhantes às humanas".[20] Dentre as possibilidades de uso da IA, McCathy cita: videogames, reconhecimento de áudio e linguagem humana, reconhecimento de imagens tridimensionais, sistemas especializados e sistemas de classificação de dados para a tomada de decisões.[21]

Stephen Hawking vislumbrava que o poder computacional poderia atingir "uma complexidade semelhante à do cérebro humano" [22] e de que nos próximos vinte anos o custo de computadores com tal inteligência seria cerca de U$ 1.000,00 dólares. Hawking também anteviu a possibilidade de uma integração entre humanos e máquina por meios de implantes neurais que diminuiriam o abismo entre as áreas da biologia e eletrônica[23]. Conforme aponta Schwab a IA já permeia o nosso

---

[17] HOFFMAN-RIEM, Wolfgang. Op. cit., p.20.
[18] NORVING, Peter; RUSSELL, Stuart. **Artificial Intelligence A Modern Aproach**. 3 ed. New Jersey: Pearson, 2010, p. 17.
[19] MCCARTHY, Jonh**. What is Artificial Intelligence?** Tradução livre: *It is the science and engineering of making intelligent machines, especially intelligent computer programs.* Disponível em: <http://jmc.stanford.edu/articles/whatisai/whatisai.pdf>. Acesso em 26 de junho de 2021.
[20] HOFFMAN-RIEM, Wolfgang. Op. cit., p.19.
[21] MCCARTHY, Jonh**.** Op. cit. p. 10, 11.
[22] HAWKING, Stephen. **O universo em uma casca de noz**. Tradução de Cássio de Arantes Leite. Rio de Janeiro: Intrínseca, 2016, p. 175.
[23] HAWKING, Stephen. Ibidem, p. 178.

cotidiano através de carros autônomos[24], softwares de tradução como o Google Tradutor[25] e assistentes virtuais como a Siri[26] da Apple ou a Alexa[27] da Amazon. Os grandes avanços que permitiram os usos acima citados da IA decorrem do "[...] aumento exponencial da capacidade de processamento e pela disponibilidade de grandes quantidades de dados".[28] À medida em que os algoritmos ou softwares de IA avançam, tornam-se cada vez mais inteligentes, precisam de insumos (*inputs* ou entradas de dados) que alimentem a inteligência artificial para que esta continue aprimorando-se. Os dados pessoais expostos no mundo virtual alimentam esses processos de IA.

Conjuntamente com o crescimento do uso de inteligência artificial outras técnicas foram desenvolvidas no campo da computação para uso com a IA e requerem grandes quantidades de dados. Pode-se destacar o *Machine Learning* (aprendizado de máquina) que conforme Eduardo Magrani pode ser descrito a capacidade dos sistemas de IA "[...] de adquirir seus próprios conhecimentos, extraindo padrões de dados brutos"[29]. Por fim, conforme aborda Felipe Medon[30] o *machine learning*:

> Pode ser compreendido como o conjunto de técnicas de Inteligência Artificial dotadas da capacidade de acumular experiências e conhecimento a partir de uma base de dados (previamente fornecidos ou buscado pela IA), sendo, por conseguinte capaz de decidir e se orientar com base na experiência acumulada, chegando não raro, a resultados sequer previstos por seus programadores/desenvolvedores.

Sucintamente, Aurélien Géron define que "[...] Aprendizado de Máquina é a ciência (e a arte) da programação de computadores para que eles possam aprender com os dados".[31] Desta feita o aprendizado de máquina tornaria possível

---

[24] BORGES, Rafaela. Carro Autônomo: Montadoras e empresas de tecnologia disputam corrida para dispensar o motorista. <https://www.uol.com.br/carros/reportagens-especiais/transporte-do-futuro---carro-autonomo/#cover> Acesso em 29 de junho de 2021.
[25] Disponível em: <https://translate.google.com.br/?hl=pt-BR> Acesso em 29 de junho de 2021.
[26] Para saber mais sobre as funcionalidades da Siri: <https://www.apple.com/br/siri/> Acesso em 29 de junho de 2021.
[27] Para saber mais sobre as funcionalidades da Alexa: <https://www.amazon.com.br/b?ie=UTF8&node=19949683011> Acesso em 29 de junho de 2021.
[28] SCHWAB, Klaus. Op. cit. p. 19.
[29] MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019, p. 148.
[30] MEDON, Filipe. **Inteligência Artificial e Responsabilidade Civil: autonomia, risco e solidariedade**. Salvador: Editora JusPodivm, 2020, p. 97.
[31] GÉRON, Aurélien. **Mãos à Obra Aprendizado de Máquina com Scikit-Learn & TensorFlow:** Conceitos, Ferramentas e Técnicas Para a Construção de Sistemas Inteligentes. traduzido por Rafael Contatori. - Rio de Janeiro: Alta Books, 2019, p. 4.

que sistemas computacionais desenvolvessem a capacidade de aprender a aprender com base em suas próprias experiências. Como resultados dessa técnica temos “[...] as recomendações personalizadas na Netflix e outros sites de busca”.[32]

2.2 Uso da IoT e técnicas de coleta e processamento de dados: *profiling* e *data mining*

Além da IA e *machine learning*, destaque-se hoje o uso de uma diversidade de dispositivos eletrônicos inteligentes conectados à internet. Desde televisores, relógios, telefones, tablets, aspiradores de pó, geladeiras, ares-condicionados e muitos outros. Tal fenômeno gerou o que se chama de internet das coisas (*Internet of Things* – IoT).

O termo *Internet of Things* surgiu em 1998 e é atribuído a Kevin Ashton. Baseia-se em uma arquitetura de dispositivos ou objetos que utilizam a Internet para a troca de informações ou serviços, buscando reduzir a barreira entre o mundo físico e virtual.[33]

Já Tarcísio Teixeira e Vinicius Cheliga definem a internet das coisas como “[...] objetos que se conectam à internet portando sensores inteligentes e software capaz de transmitir esses dados para a rede”.[34]

Sobre o mesmo conceito Douglas Alfieri entende que a IoT constitui um conjunto de “objetos inteligentes” que utilizam sua conexão com a internet para a coleta das informações dos usuários e a transmissão delas com a finalidade de que o usuário receba um serviço mais personalizado e tenha uma participação mais ativa na produção de informações que redefinirão a adaptabilidade do dispositivo às necessidades do usuário.[35]

Por fim, Eduardo Magrani aborda que embora não exista uma unanimidade sobre o conceito da IoT podemos compreendê-la como:

---

[32] COSTA, Alessandra Cristina da. Inteligência Artificial no Empreendedorismo. In: TEIXEIRA, Tarcíso; LOPES, Alan Moreira; TAKADA, Thalles (Coord). **Manual Jurídico da Inovação e das Startups**. Salvador: Editora JusPodivm, 2020, p. 41.
[33] WEBER, Rolf; WEBER, Romana. **Internet of Things**. Springer, 2010, p. 1.
[34] CHELIGA, Vinicius; TEIXEIRA, Tarcísio. **Inteligência Artificial: aspectos jurídicos**. 3 ed. rev. e atual., Salvador: Editora JusPodivm, 2021, p. 76.
[35] ALFIERI, Douglas Guergolette. Internet das Coisas: Aspectos Jurídicos. In: TEIXEIRA, Tarcíso; LOPES, Alan Moreira; TAKADA, Thalles (Coord). **Manual Jurídico da Inovação e das Startups**. Salvador: Editora JusPodivm, 2020, p.54.

> De maneira geral, pode ser entendido como um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. O que todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade.[36]

Considerando nesse contexto que as grandes empresas de tecnologia como Microsoft, Google, Amazon etc. continuam a investir na IoT[37] gerando cada vez mais pessoas conectadas ofertando dados pessoais na internet, surge o fenômeno da "datificação"[38]: quando alguém praticamente transforma os seus feitos e sua vida em dados. Isso permite que até objetos que antes estavam fora das "redes" possam gerar um clima de onipresença no mundo virtual.

Contudo, apesar das comodidades que um ambiente integrado à internet possa nos trazer como mais acesso à informação ou ganho de tempo em face da automatização de atividades rotineiras, essas "coisas" passaram a constituir um apêndice ou extensão da pessoa humana e mais dados ou informações sobre nós estão disponíveis para terceiros. Logo, novos cenários desafiam o Direito seja: (I) no que tange à proteção à privacidade do usuário uma vez que ele passa a está em constante estado de vigilância e seus hábitos, preferências e opiniões estão debaixo de constante monitoramento; (II) perda de oportunidades em face de discriminação de dados ou algorítmica ocasionada pelo fenômeno do perfilamento (*profilling*) ou (III) danos oriundos de um tratamento inadequado de dados pessoais do usuário desses objetos integrados à internet.

Outro fator que poderá gerar repercussões jurídicas é o direito de resposta a decisões automatizadas uma vez que as técnicas de perfilamento estão categorizando as pessoas com base nos dados pessoais das mesmas e esta ação gera efeitos importantes nas "oportunidades sociais"[39] dessas pessoas que estão inseridas em um sistema econômico orientado por tratamento de dados. Este tratamento é utilizado em processos seletivos na área de recursos humanos, na concessão de crédito (ranking de crédito ou *credit score*), na definição de quanto uma pessoa pagará para contratar um seguro automotivo etc.

Portanto, como ensina Danilo Doneda, as questões citadas relacionadas a

---

[36] MAGRANI, Eduardo. **A internet das coisas.** Rio de Janeiro: FGV Editora, 2018, p. 20.
[37] ALFIERI, Douglas Guergolette. Op. cit., p.55.
[38] BIONI, Bruno R. Op. cit. p. 85.
[39] BIONI, Bruno R. Op. cit. p. 88.

rapidez e a potência da tecnologia e até mesmo referentes a qualidade da ubiquidade dela precisam ser enfrentadas pelo jurista enquanto este promove "[...] a segurança necessária para que haja previsibilidade e seguranças devidas para a viabilidade das estruturas econômicas"[40]. Logo, semelhantemente como as mudanças alistadas nas páginas iniciais deste capítulo impactaram a sociedade e o direito, as novas mudanças promovidas pela quarta revolução industrial terão que ser cuidadas pelos juristas atuais.

No campo do tratamento de dados o supracitado autor destaca a técnica de perfilamento ou *profiling*. Esta técnica usa dados ou informações de uma pessoa e por meio de "[...] métodos estatísticos e técnicas de inteligência artificial"[41] é possível refinar uma informação e obter uma série de outras informações sobre uma pessoa ou um grupo delas. A consequência seria a graduação de probabilidades que estimem uma tendência de comportamento ou tomadas de decisão da pessoa ou grupo de quem se coletou aqueles dados.

Este perfil seria um reflexo de um corpo eletrônico que seria um contraponto da pessoa natural. Embora hoje muitos obtenham benefício com o processo de *profiling* como, por exemplo, descontos em determinados produtos ou ofertas em lugares próximos por onde a pessoa esteja transitando é necessário verificar os efeitos colaterais do perfilamento de dados. Doneda aponta para o risco de que esse perfil eletrônico seja a única forma que a respectiva pessoa natural seja vista no mundo digital e que tal confusão de corpos somados às previsões estatísticas de algoritmos de IA gerem uma redução da liberdade de escolha do indivíduo.[42]

Por fim destaque-se a técnica de coleta de dados chamada *data mining* (mineração de dados) que favoreceu a implementação de grandes sistemas de coleta e tratamento de dados. Conforme ensina Doneda[43], esta técnica:

> [...] consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos. Assim, a partir de uma grande quantidade de informação em estado bruto e não classificada, torna-se possível identificar informações de potencial interesse.

---

[40] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 64.
[41] DONEDA, Danilo. Ibidem, p. 151.
[42] DONEDA, Danilo. Ibidem, p. 152.
[43] DONEDA, Danilo. Ibidem, p. 154.

Portanto, embora o *profiling* e o *data mining* sejam apenas algumas técnicas dentre muitas que associadas a algoritmos de IA e *machine learning* gerem vantagens econômicas para os detentores, coletores e processadores de dados pessoais, Doneda alerta para o perigo de que "[...] elas podem provocar um distanciamento entre a informação conscientemente fornecida pela pessoa e a utilidade na qual é transformada."[44]

Stefano Rodotà aborda que embora as tendências de perfilização tragam eficiência para as atividades do poder público e da iniciativa privada na solução de problemas de nossa sociedade, há efeitos destas tecnologias sobre as minorias sociais. Rodotà passa a citar o seguinte exemplo: imagine um bairro onde a maioria das pessoas que moram ali possuem apenas um gosto literário. Por motivos econômicos serão estimuladas as vendas de publicações inerentes a apenas aos interesses daquela maioria naquele momento específico. Com isso pessoas que possuam interesses literários divergentes da maioria serão penalizadas uma vez que o perfil de gosto literário daquele bairro estará cristalizado em uma temática específica. Por fim, tanto grupos minoritários perderão o acesso a livros que lhes interessam quanto a maioria das pessoas ali perderão a oportunidade de desenvolvimento da capacidade de percepção de gostos que poderiam lhes ser benéficos, porém estão fora do perfil traçado pelo processo de *profiling*.[45]

2.3 O *Big Data* como elemento transformador no uso de dados pessoais

Por fim, os termos *Big Data* e *Big Data Analytics* assumiram grande importância na contemporaneidade pois conforme aponta Ana Frazão esses fenômenos proporcionaram que o ciclo de tratamento de dados fosse aprimorado pelo aumento de sua eficiência uma vez que se percebeu notória melhoria nas atividades de "garimpo" de dados, classificação, organização em informações e posterior acesso a essas últimas. Esses processos ganharam:

> [...] mais veracidade, velocidade, variedade e volume. Mais do que isso, o Big Data e o Big Data Analytics permitiram que, a partir da coleta e do registro de dados, fossem a eles atribuídas utilizações e aplicações que não seriam sequer imagináveis há pouco tempo e que, na ausência de uma regulação adequada, passaram a realizadas sem limites e com resultados

[44] DONEDA, Danilo. Op. cit., p. 157.
[45] RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 82.

> que podem se projetar para sempre.[46]

Destaque-se ainda sobre a expressão *Big Data* o entendimento de William Paiva Marques Júnior[47]:

> [...] afirma-se que o *big data* refere-se à prática de analisar um grande fluxo de dados na internet. Resta indubitável que esta atividade é de grande relevância para o Direito, especialmente para o Direito Civil e o Direito Constitucional, quando se colocam em debate suas relações com os direitos de personalidade e com os direitos fundamentais, respectivamente.

Assevera o autor que no atual estado de aumento do número de dispositivos e usuários da internet o Brasil se tornará um dos possíveis epicentros de violações a direitos de personalidade como o direito à privacidade, por meio de violações de dados pessoais. Outro direito que está sob forte ataque é o direito à honra. Um exemplo desta lesão traduz-se pela conduta vil de usuários, que usam a capa do anonimato proporcionado pela rede mundial de computadores e por plataformas digitais que abrigam redes sociais, para o cometimento de crimes que incluem a criação perfis falsos e desta feita passam a macular a imagem e honra de terceiros através de ofensas e notícias falsas sobre estes.[48]

Ainda sobre o presente tema Wolfgang Hoffmann-Riem ensina que o termo *Big Data* pode ser referenciado como o cenário de utilização dos recursos digitais "[...] para lidar com grandes e diversas quantidades de dados e às várias possibilidades de combinação, avaliação e processamento desses dados por autoridades privadas e públicas em diferentes contextos."[49] Além dos quatro "V"s supracitados na lição da Ana Frazão (veracidade, velocidade, variedade e volume), Hoffmann-Riem aponta um quinto "V" que seria de "valor agregado" uma vez que os benefícios produzidos pelo *Big Data* poderiam integrar um sólido modelo de negócios e atividades que pode-se verificar nos mais diversos usos. Por exemplo, na modelagem comportamental de indivíduos e massas populacionais, no desenvolvimento de assistentes virtuais como a Alexa da Amazon ou em sistemas

---

[46] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção Pessoais e suas Repercussões no Direito Brasileiro**, 2. ed. São Paulo, Revista dos Tribunais, 2020, p. 25.

[47] MARQUES JÚNIOR, William Paiva. Obstáculos impostos à efetividade do direito personalíssimo à privacidade na Era do Big Data: uma problemática da sociedade contemporânea. In: Larissa Maria de Moraes Leal; Roberto Senise Lisboa. (Org.). **Direito Civil Contemporâneo II.** 01ed. Florianópolis: CONPEDI, 2018, v. 01, p. 34.

[48] MARQUES JÚNIOR, William Paiva. Ibidem, p.35, 36.

[49] HOFFMAN-RIEM, Wolfgang. Op. cit., p.16.

de vigilância, mobilidade urbana etc.[50]

Considerando a associação da IA com *Big Data*, Hoffmann-Riem acrescenta que dessa junção tem-se a figura do *Big Data Analytics*. Neste os dados podem ser empregados em uma análise descritiva, preventiva e prescritiva.

Enquanto a análise descritiva "peneira" e organizar os dados com a finalidade de avaliar a informação produzida (o emprego do *Big Data* em processos de *Data Mining* e em sistemas que registram e classificam sistematicamente dados), a análise preditiva busca utilizar técnicas estatísticas para correlacionar dados e extrair disto qual a probabilidade de um determinado evento acontecer. Com esta análise pretende-se prever padrões de comportamento humano que poderão ser utilizados na definição de "preferências e desejos do consumidor (Predicitve Consumer Interest)" ou para desenvolvimento de propaganda personalizada baseada em neuromarkentig.[51]

Outro uso da análise preditiva é em aplicações de policiamento preditivo (*Predictive Policing*). Este instituto, segundo Hoffmann-Riem[52]:

> Refere-se à avaliação de dados pessoais ou estatísticas disponíveis publicamente, perfis de vítimas etc., com o objetivo de identificar a probabilidade de crimes em locais específicos, em ocasiões específicas ou para grupos específicos de infratores. Na medida em que serve para prevenir o crime por dissuasão, é um controle indireto do comportamento dos infratores potenciais. Na medida em que os resultados analíticos e prognósticos servem como base para as táticas e estratégias de trabalho da polícia criminal, os algoritmos também influenciam indiretamente o comportamento das autoridades públicas, por exemplo, no planejamento e implementação operacional.

Diante desse cenário em que tecnologias algorítmicas como o *Big Data Analytics* podem "prever o futuro" por meio da análise comportamental baseada em dados pessoais será que o contexto de prevenção de crimes retratado pelo filme *Minority Report* – A Nova Lei (2002)[53] poderia tornar-se realidade daqui a 33 anos? Ou estaria posta uma realidade em que a vivência humana seria determinada pelas máquinas de IA como a apresentada no filme *Matrix* (1999)[54]? Considerando que esses cenários distópicos ainda habitam no cinema, Hoffmam-Riem aponta que apesar das benesses oferecidas pelo uso integrado do *Big Data* com a IA, estas

[50] HOFFMAN-RIEM, Wolfgang. Op. cit., p.17.
[51] HOFFMAN-RIEM, Wolfgang. Op. cit., p.18.
[52] HOFFMAN-RIEM, Wolfgang. Op. cit., p.66.
[53] Disponível em: <https://pt.wikipedia.org/wiki/Minority_Report_(filme)>. Acesso em 26/08/2021.
[54] Disponível em: <https://pt.wikipedia.org/wiki/Matrix>. Acesso em 26/08/2021.

tecnologias podem gerar riscos consideráveis para importantes “[...] bens jurídicos individuais e coletivos”[55]. Entre esses bens podem-se destacar “[...] não só o direito de exercer a liberdade, mas também a proteção contra as consequências do uso da liberdade por outros.”[56] Como exemplo destas lesões ao direito público, inclusive a democracia por meio de manipulação das informações obtidas no mundo digital, temos as ações de coleta indevida de dados pessoais de mais de 87 milhões de usuários do Facebook feita pela empresa britânica Cambrigde Analytica.[57] Estes dados foram utilizados para influenciar a campanha presidencial norte-americana de 2016.

Por fim, a análise prescritiva usa as técnicas das duas análises supracitadas e possui a finalidade de recomendar ao seu usuário que ações este deve tomar para alcançar um determinado objetivo. Por exemplo: a seleção personalizada em preços ou estratégias e táticas para influenciar atitudes e comportamentos, incluindo a influência na formação da opinião pública

Percebe-se que, em face dos riscos à própria identidade, as aludidas técnicas podem levar pessoas a adotarem comportamentos que se adequem a um perfil ideal determinado, por exemplo, por uma plataforma digital sob pena de sofrerem discriminação na rede ou perderem oportunidades. Também há o risco de que essas plataformas digitais levem as pessoas a tomarem decisões baseadas em informações manipuladas, viciando sua vontade e trazendo-lhes prejuízos que poderão ir desde um superendividamento a uma fratura na credibilidade de um sistema democrático de um país. Portanto, a importância da tutela jurídica dos dados pessoais na proteção aos direitos de personalidade ficou mais evidente em uma sociedade da informação movida a dados.

Conforme disciplina Bruno Bioni, no tocante à proteção dos dados pessoais, esta necessita de um escudo normativo próprio pois os bens jurídicos protegidos vão além de meros dados pessoais que deveriam remanescer na propriedade de seu titular amparada pela privacidade, “[...] mas encarada como um novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não

[55] HOFFMAN-RIEM, Wolfgang. Op. cit., p.19.
[56] HOFFMAN-RIEM, Wolfgang. Op. cit., p.41.
[57] Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/2019/01/09/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook.ghtml>. Acesso em 26/08/2021.

discriminação".[58]

Deste apanhado geral de conceitos revela-se a necessidade de um marco regulatório geral que estabeleça diretrizes claras para que haja tanto a proteção da pessoa natural no que diz respeito a sua privacidade e a segurança de seus dados quanto proteção a inovação tecnológica e sua viabilidade econômica.

Neste contexto, cabe destacar a importância que a Regulamento Geral de Proteção de Dados (RGPD ou GDPR - *General Data Protection Regulation* – EU 679/2016) exerce na União Europeia e demais países que desejam manter relações comerciais com ela, bem como a influência que essa norma exerceu no Brasil na criação da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018). Nos próximos capítulos é realizado uma análise da evolução histórica das normas de proteção de dados na Europa que culminou na vigência da GDPR. Depois analisa-se os dispositivos legislativos no ordenamento jurídico brasileiro que garantem de forma setorial certo nível de proteção de dados. Em seguida observa-se como a LGPD visa regular a indústria de dados como fins de evitar os aspectos danosos das técnicas de *profiling* e da discriminação algorítmica automatizada.

[58] BIONI, Bruno R. Op. cit. p. 90.

3 NECESSIDADE DE UMA LEGISLAÇÃO ESPECÍFICA PARA A PROTEÇÃO DE DADOS PESSOAIS

Danilo Doneda considera que o novo cenário jurídico oriundo das relações entre o ser-humano e a tecnologia criam regulamentos com o fim de ajustar o direito vigente "[...] à realidade da arquitetura social".[59] Portanto, considerando os efeitos citados no capítulo anterior sobre as consequências do avanço tecnológico na sociedade da informação, faz-se necessário que o jurista considere essas novas variáveis no processo de atualização de novos institutos de regulação da tecnologia com a finalidade de promover uma harmonia entre a proteção à direitos da pessoa humana e a iniciativa tecnológica.[60]

Entre os direitos da personalidade que precisam de proteção em face de nossa economia movida a dados destaca-se o direito à privacidade, à intimidade e à autodeterminação informativa. Embora nossa sociedade não seja a descrita por George Orwell em sua distopia "1984", onde o "Big Brother" podia observar constantemente as ações dos habitantes de Oceânia por meio da "teletela" e desta maneira sujeitá-los a uma vigilância constante[61], hoje os vários dispositivos que são utilizados com acesso à Internet passaram a ser usados como ferramentas de vigilância. Este monitoramento é possível por meio da coleta de dados pessoais ou pela invasão aos dispositivos conectados à internet por terceiros mal-intencionados que obtêm acesso ao microfone e câmera desses dispositivos, por exemplo. Conforme comenta Davis Lyon somos cotidianamente "[...] checados, monitorados, testados, avaliados, apreciados e julgados. [...] À medida que os detalhes de nossa vida diária se tornam mais transparentes às organizações de vigilância, suas próprias atividades são cada vez mais difíceis de discernir."[62]

Portanto, com a finalidade de proteger o usuário de atitudes abusivas por parte dos detentores dos recursos de informação e comunicação que as normas de proteção de dados pessoais começaram a ser desenvolvidas. Como exemplo destaque-se a GDPR na Comunidade Europeia e a LGPD no Brasil.

---

[59] DONEDA, Danilo. Op. cit., p. 49.
[60] DONEDA, Danilo. Op. cit., p. 70.
[61] ORWELL, George. **1984**; Tradução de Alexander Hubner, Heloisa Jahn; São Paulo: Companhia das Letras, 2009, p. 12, 13.
[62] BAUMAN, Zygmunt; LYON, David. Vigilância Líquida. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013, p. 19.

3.1 Uma breve análise do desenvolvimento do modelo europeu de uma legislação de proteção de dados e sua influência na elaboração de uma lei geral brasileira

Destaque-se que antes desses marcos regulatórios existiram predecessores, Danilo Doneda destaca que embora a legislação de proteção de dados europeia seja referência para normas de muitos países, o devido reconhecimento aos Estados Unidos faz-se necessário uma vez que neste país ocorreu uma parte substancial dos debates que promoveriam a gênese que constituiria o arcabouço jurídico protetor dos dados pessoais. Entre os debates mencionados destacam-se instrumentos normativos que tratam da "tutela às liberdades individuais afetadas, incluindo o direito à privacidade".[63]

Como exemplo do pioneirismo norte-americano na proteção à privacidade é notório no artigo escrito por Samuel Warren e Louis Brandeis, "*The rigth to privacy*", de 1890, onde os autores abordam o direito de ser deixado só, *rigth to be let alone*, como um escudo na defesa contra a invasão à privacidade ocasionada pelas modernidades da época: fotos instantâneas e jornais impressos.[64] Embora o supracitado artigo mantenha seu valor no campo doutrinário e seja constantemente citado e lido, deve ser analisado sob o prisma de que a privacidade prolongou-se além do conceito de manter-se isolado.[65]

Segundo Rodotà[66] o conceito de privacidade passou por uma redefinição:

> Uma definição da privacidade como "direito de ser deixado só" perdeu há muito tempo seu valor genérico, ainda que continue a abranger um aspecto essencial do problema e possa (deva) ser aplicada a situações específicas. Na sociedade da informação tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas. Assim a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações.

Retornando para o cenário europeu, por exemplo, segundo Doneda a norma específica pioneira na temática da proteção de dados pessoais foi a "Lei de

---

[63] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In. Coordenadores Danilo Doneda ... [et. al.]. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p.5.
[64] WARREN, Samuel; BRANDEIS, Louis. The rigth to privacy. *Harvard Law Review*, v.4, p. 195, 1890.
[65] DONEDA, Danilo. Da privacidade à proteção..., Op. cit., p.31.
[66] RODOTÀ, Stefano. Op. Cit. p. 92.

Proteção de Dados do *Land* alemão de Hesse, de 1970".[67] Esta legislação promoveu um novo olhar sobre o direito à proteção de dados por considerar que este "[...] ia além da segurança da informação da privacidade ou do sigilo."[68]

O exemplo alemão foi sucedido por outros países que promoveram leis de proteção de dados pessoais como: a Suécia (*Datalag* – 1973)[69] e a França (*Informatique et Libertées* – 1978)[70]. Notória também a decisão do Tribunal Constitucional alemão sobre a Lei do Censo de 1982, que entendeu que a capacidade de armazenamento e processamento de dados por novas tecnologias da época poderiam interferir não somente no direito à privacidade, mas outros aspectos da personalidade da pessoa. Portanto, foi reconhecida a existência do direito à autodeterminação informacional, cuja finalidade era permitir que o titular dos dados pessoais protegesse os aspectos de sua personalidade representados por esses dados[71] e esse titular tivesse poder decisório sobre a aquisição e utilização desses dados por terceiros.[72]

Por fim, em 1995, com a finalidade de integrar o sistema legislativo que trata da proteção de dados a União Europeia (UE) utiliza a Diretiva 95/46/CE[73]. Entre os destaques desta norma destaque-se que ela abordava sobre os deveres e direitos dos titulares de dados e orientações para que os países membros da UE adaptassem seus respectivos ordenamentos jurídicos internos. Também destacava a exigência de que fosse criado um órgão estatal que cuidasse da supervisão e aplicação da legislação de proteção de dados de seu respectivo país.[74]

Segundo aponta Doneda[75] a diretiva foi destaque pela preocupação com:

> [...] o tráfego de informações entre fronteiras: prevê-se o livre fluxo de dados entre as fronteiras dos estados-membros; já o fluxo para outros países é regulado pelo *princípio da equivalência*, pelo qual é cerceada a transmissão para países que não possuam um nível de proteção de dados pessoais considerado adequado, de acordo com os padrões da diretiva.

---

[67] DONEDA, Danilo. Tratado de proteção... Op. cit., p.3.
[68] DONEDA, Danilo. Tratado de proteção... Op. cit., p.8.
[69] Disponível em: < https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289>. Acesso em 25/07/2021.
[70] Disponível em: < https://www.cnil.fr/fr/la-loi-informatique-et-libertes>. Acesso em 25/07/2021.
[71] DONEDA, Danilo. Tratado de proteção... Op. cit., p.9.
[72] VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: **Comentários ao GDPR**. Viviane Nóbrega Maldonado; Renato Ópice Blum (Coord). 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 34.
[73] Disponível em: < https://eur-lex.europa.eu/eli/dir/1995/46/oj?locale=pt>. Acesso em 25/07/2021.
[74] TEIXEIRA, Tarcísio; ARMAELIN, Ruth Maria Guerreiro da Fonseca**. Lei geral de proteção de dados pessoais: comentada artigo por artigo.** Salvador: Editora JusPodivm, 2019, p. 19.
[75] DONEDA, Danilo. Da privacidade à proteção... Op. cit., p. 199.

Contudo, a Diretiva 95/46/CE foi revogada pela *General Data Protection Regulation* (GDPR ou RGPD – Regulamento Geral de Proteção de Dados) em 25 de maio de 2018 conforme determinado pelo artigo 99º desta. Este Regulamento aplica-se de forma uniforme nos países membro da UE e na Noruega, Islândia e Liechtenstein. O que é considerado um progresso em relação à Diretiva 95/46/CE uma vez que esta delegava que cada país membro desenvolvesse lei própria sobre o tema, o que gerava uma dificuldade de integração executiva entre muitos normativos.[76] Portanto, com a aplicação imediata da GDPR e a não dependência de adaptações por parte dos países em suas normas internas buscou-se promover entre os países segurança jurídica, uma equalização no nível de proteção de dados e facilitar a regulamentação do livre fluxo de dados.[77] Outros destaques trazidos pela GDPR são a definição legal das condições lícitas de tratamento de dados pessoais e a introdução de multas mais altas conforme está descrito em seu artigo 83.[78]

A GDPR em seu capítulo 5 estabelece que antes da transferência de dados para países terceiros sejam avaliadas se estes possuem legislações de proteção de dados semelhantes à GDPR. Embora o Brasil já possuísse uma legislação setorial que abordassem em alguns aspectos à proteção de dados, o normativo europeu acelerou a necessidade da criação de uma Lei Geral de Proteção de Dados Pessoais brasileira. Segundo Doneda, a vigente LGPD começou a ser originada no campo de debates internos dos membros do Mercosul por meio do Subgrupo de Trabalho de número 13 (SGT13) quando em 2004 a Argentina sugeriu criação de norma comum aos países do bloco referente à proteção de dados pessoais.[79]

Embora o trabalho elaborado no âmbito do Mercosul não tenha gerado uma norma geral para o bloco, o referido debate estabeleceu os fundamentos[80] que integraram a discussão do tema no Congresso Nacional e por fim em 14 de agosto de 2018 foi promulgada a Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais – LGPD).

---

[76] LIMA, Caio César Carvalho. Objeto, aplicação territorial e aplicação material. In: **Comentários ao GDPR**. Viviane Nóbrega Maldonado; Renato Ópice Blum (Coord). 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 22.
[77] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca**.** Lei geral de proteção... Op. cit, p. 20.
[78] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Lei geral de proteção... Op. cit, p. 21.
[79] DONEDA, Danilo. Tratado de proteção..., Op. cit., p.15.
[80] DONEDA, Danilo. Tratado de proteção..., Op. cit., p.16.

3.2 Uma análise da legislação setorial de proteção de dados pessoais

Ressalte-se que, antes de uma lei que unificasse a temática em tela, existiam ferramentas que forneciam garantias de proteção de dados pessoais, porém essas garantias encontravam-se em diplomas diversos. Como exemplo temos a Constituição Federal de 1988 em seu artigo 5º ao tratar de direitos e garantias fundamentais. Merecem destaques os seus incisos: X (ao determinar reparação aos danos que violem a intimidade, a privacidade, a honra e a imagem das pessoas); XI (reafirmando o direito à privacidade no âmbito da casa do indivíduo); XII (estabelecendo que a proteção e privacidade das correspondências e comunicações telemáticas, inclusive os dados, são considerados invioláveis e determina quais as hipóteses que excetuam essas inviolabilidades); LXXII (ao permitir que a pessoa tenha o acesso e a correção dos seus dados pessoais em instituições públicas por meio do remédio constitucional *habeas data*).

Referente a este último dispositivo Doneda aponta algumas críticas. Por exemplo, considera-se o "[...] fato de que a ação teve pouca repercussão prática nos tribunais; além de outras mais, que sublinham o fato de que a regulamentação advinda em 1997 não resolveu muitos dos problemas que minam sua efetividade."[81] Continuando sua lição ele nos apresenta o risco de que este remédio venha a perder sua função pretendida pelo constituinte e sofra o efeito colateral de virar um placebo em nosso ordenamento jurídico. Esta condição pode ser depreendida de que a vigência da Lei nº 9.507/1997, que passou a normatizar o rito do processo de habeas data, não encontrou efeito combativo frente aos óbices criados pelo crescente fluxo "[...] de dados pessoais na Sociedade da Informação."[82]

Outro exemplo pode ser encontrado no atual Código de Processo Penal (CPP) em seu artigo 201, § 6º onde o segredo de justiça determinado pelo juiz com fins de proteger a intimidade e privacidade do ofendido incluía até os dados deste. Na área cível entra em destaque os institutos dispostos no artigo 20 do Código Civil que trata do direito à imagem como "[...] o controle que cada pessoa detém sobre a sua representação externa, abrangendo qualquer tipo de reprodução de sua imagem

[81] DONEDA, Danilo. Da privacidade ... p. 287.
[82] DONEDA, Danilo. Tratado de proteção..., Op. cit., p.13.

ou de sua voz”[83], e no artigo 21 que discorre sobre o direito à privacidade. Contudo, referente a este último artigo Anderson Schreiber critica a restrição que o legislador ordinário fez ao condicionar o direito à privacidade como inviolabilidade da vida privada. Perdeu-se a oportunidade de expandir a proteção do objeto desse direito para inclui explicitamente nos direitos de personalidade “[...] a faculdade de exercer controle sobre o uso, a circulação e o armazenamento dos seus próprios dados pessoais.”[84]

O Código de Defesa do Consumidor (CDC), Lei nº 8.078/1990, destaca em seu artigo 43 e subsequentes parágrafos o direito de o consumidor ter ciência sobre o uso de seus dados em cadastros ou bancos de dados, ter acesso a esses dados e não encontrar barreiras para retificá-los. Danilo Doneda ensina que esse artigo “[...] estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em “bancos de dados e cadastros”.”[85] Ele aponta que o CDC consagra princípios relacionados à proteção de dados no âmbito das relações de consumo. Como exemplo:

> [...] entende-se a existência do princípio da finalidade, por intermédio da aplicação da cláusula da boa-fé objetiva e da própria garantia constitucional da privacidade, pelo qual os dados fornecidos pelo consumidor deverão ser utilizados somente para fins que motivaram a sua coleta – o que pode servir como fundamentação para o reconhecimento de um princípio de vedação da coleta de dados sensíveis e da comercialização de bancos de dados de consumidores.[86]

Conforme aponta Bioni, o alcance do supracitado artigo vai além de informações constantes em bancos de dados de sistemas de proteção ao crédito, mas que o intuito “[...] do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor.”[87] Por fim, o supracitado autor conclui:

> Tais direitos (acesso, retificação e cancelamento) e princípios (transparência, qualidade [exatidão] e limitação temporal) gravitam em torno da figura do consumidor, para que ele, na condição de titular dos dados pessoais, exerça controle sobre suas informações pessoais. Em suma, o Código de Defesa de Consumidor buscou conferir a autodeterminação informacional, o que perpassa desde regras para garantir a exatidão dos

---

[83] SCHREIBER, Anderson. **Código civil comentado – doutrina e jurisprudência**. Anderson Schreiber ... [et al.]. – Rio de Janeiro: Forense, 2019, p. 19.
[84] SCHREIBER, Anderson. Op. cit, p. 24.
[85] DONEDA, Danilo. Da privacidade ... p. 265.
[86] DONEDA, Danilo. Da privacidade ... p. 266.
[87] BIONI, Bruno R. Op. cit. p. 121.

> dados até limitações temporais para o seu armazenamento.[88]

Continuando na seara da proteção ao crédito a Lei nº 12.414/2011, Lei do Cadastro Positivo, buscou regulamentar a criação de banco de dados relativos às transações financeiras e histórico do uso de crédito de pessoas naturais e jurídicas com fins de atribuir a estes um perfil financeiro de capacidade de adimplência dessas pessoas. Pode-se tirar esta conclusão sobre o alcance da lei supracitada com base em seus artigos 1º ao 5º, onde são estabelecidos conceitos que denotam o que seria o "cadastro positivo", quais direitos e deveres daqueles que constroem ou acessam o banco de dados e daqueles que possuem informações nesses bancos. Conforme aponta Bioni: "[...] Essa nova peça legislativa setorial acabou por trazer, de forma original e mais sistematizada, a orientação de que o titular dos dados pessoais deve ter o direito de gerenciá-los."[89] Danilo Doneda destaca o pioneirismo deste diploma normativo no Brasil em refletir aqui elementos pertencentes aos sistemas de proteção de dados de outros lugares. Em sua visão Doneda percebe que apesar das inovações trazidas pela lei supracitada, esta não impulsionou o desenvolvimento de uma cultura de proteção de dados na área jurisprudencial:

> É possível observar a presença de conceitos como o de dados sensíveis e outros, bem como de alguns dos princípios mais importantes de proteção de dados, entre os quais os da finalidade, transparência, minimização e segurança, entre outros. No entanto, por conta de a utilização dos serviços de cadastro positivo ter sido aquém da esperada, sua presença na jurisprudência e também sua importância para a formação de uma cultura jurídica de proteção de dados não se demonstraram determinantes.[90]

Ainda no contexto de inovação da Lei do Cadastro Positivo, Marco Aurélio Bellizze Oliveira e Isabela Maria Pereira Lopes destacam a ênfase desta lei para a manutenção da qualidade de informações pessoais armazenadas em bancos de dados conforme observa-se em seu artigo 3º e a responsabilidade civil objetiva e solidária pelos danos causados ao detentor dos dados pessoais conforme determina o artigo 16 da lei em análise. Outros pontos destacados pelos autores são: a maior rigidez estabelecida para o tratamento de dados que devem ficar restritos ao processo de análise da capacidade creditícia e a possibilidade de o titular dos dados ter uma nova análise de decisões que se baseiam apenas em técnicas de

---

[88] BIONI, Bruno R. Op. cit. p. 122.
[89] BIONI, Bruno R. Op. cit. p. 123.
[90] DONEDA, Danilo. Tratado de proteção..., Op. cit., p.15.

automação desses dados.[91]

Outro diploma legislativo que merece análise é a Lei de Acesso à Informação (LAI), Lei nº 12.527/2011, cuja finalidade é garantir que o direito à transparência enumerado na Constituição Federal no artigo 5º, inciso XXXIII seja assegurado para todos. Em seu artigo 31 a LAI lança as bases do conceito de informação pessoal e busca ser o fiel da balança entre a transparência que as informações precisam no cuidado com a coisa pública e a proteção dessas informações no que se referem a dados pessoais e que estejam sob tutela do poder estatal.[92] Notório também que:

> [...] além do reforço ao equilíbrio entre acesso, qualidade da informação, proteção à privacidade e sigilo, é a diversificação de categorias – ultrassecreta, secreta e reservada -, além do detalhamento dos critérios para classificação das informações. A lei dedicou, ainda, uma seção especial para tratar das informações privadas, conferindo a elas um tempo de sigilo máximo de cem anos, que é bastante superior às demais categorias.[93]

O § 3º do supracitado artigo estabelece em que situações esta proteção secular pode ser descortinada. Por exemplo observa-se esta possibilidade poderá ser empregada para fins de: tratamento médico diante da incapacidade natural ou legal do paciente; uso de dados pessoais em estudo estatísticos ou pesquisas científicas em que exista o interesse público ou geral, contudo é proibido que esses dados possibilitem a identificação de seus titulares; e outras situações em que permeiam o interesse público como a promoção dos direitos humanos ou o cumprimento de uma ordem judicial. Estas situações de exceção podem ser também encontradas nas hipóteses de bases legais permitidas pela LGPD em seu artigo 7º.

Merece destaque o Marco Civil da Internet (MCI), Lei nº 12.965/2014, que disciplina sobre a regulação no campo da internet no Brasil e em seu artigo 3º incisos II e III ao estabelecer os princípios da proteção da privacidade e dados pessoais. O MCI inaugurou uma legislação pátria específica para proteger garantias do usuário nas diversas interações promovidas por meio da internet. Em seu artigo 7º que trata sobre os direitos do usuário são notórios os incisos: VII - que traz a vedação a divulgação de dados pessoais a terceiros estabelecendo que esses

---

[91] OLIVEIRA, Marcos Aurélio Belizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In. FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção Pessoais e suas Repercussões no Direito Brasileiro**, 2. ed. São Paulo, Revista dos Tribunais, 2020, p. 69.
[92] DONEDA, Danilo. Tratado de proteção... Op. Cit., p.15.
[93] OLIVEIRA, Marcos Aurélio Belizze; LOPES, Isabela Maria Pereira. Op. cit. p. 65.

dados poderiam ser divulgados por consentimento expresso e informado do usuário; VIII – ao especificar para quais finalidades os dados pessoais do usuário do serviço de internet poderiam ser coletados e tratados; IX – ao enfatizar como deveria ser registrado o consentimento do usuário; e X – ao determinar quais hipóteses de exclusão dos dados pessoais, inclusive a pedido do titular deles. Ainda é relevante considerar o artigo 16, inciso II que veda o armazenamento dos dados pessoais para fins que excedam o pactuado através do que foi consentido pelo usuário.

Sobre as inovações do Marco Civil da Internet Bruno Bioni[94] ensina que:

> Pela combinatória de tais dispositivos, verifica-se a autodeterminação informacional o parâmetro normativo eleito pelo MCI para a proteção de dados pessoais. Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação.

Conforme aponta Ana Frazão[95], no final de 2019, decisões judiciais indicam o uso de dispositivos de proteção de dados possibilitados pelo MCI e CDC. Como exemplo ela menciona Recurso Especial Nº 1.758.799 - MG Rel. MINISTRA NANCY ANDRIGHI, onde a 3ª Turma do STJ concordou que o consumidor que esteja inserido em banco de dados sem a ciência ou consentimento daquele, possui direito à reparação de dano moral *in re ipsa*. Esta presunção de dano é decorrente da violação do direito de informação do consumidor.

> **RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS.COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15**. [...] 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011 – dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele.
> 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas.
> 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para

[94] BIONI, Bruno R. Op. cit. p. 126.
[95] Disponível em <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/protecao-de-dados-e-expectativas-para-2020-12022020>. Acesso em 16/08/2021.

> este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade.
> 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais
> 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais.
> 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos.
> 11. Hipótese em que se configura o dano moral in re ipsa.[96]

Outro caso notório é o relatado pela Nota Técnica n.º 32/2019/CGCTSA/DPDC/SENACON/MJ.[97] O caso em tela trata-se de ação do Ministério da Justiça (MJ) por meio de processo administrativo instaurado pelo Departamento de Proteção e Defesa do Consumidor na preservação dos direitos do consumidor e usuários da rede social Facebook. As investigações foram iniciadas depois de possível violação de dados pessoais referente ao supracitado caso da empresa Cambridge Analytica. Durante o processo investigatório foram encontradas violações aos dispositivos constantes no Marco Civil da Internet (arts. 2º, inc. II e III, e 7º, incs. VI, VII, VIII, IX e XIII) e no Código de Defesa do Consumidor (art. 4º, caput, I, III e IV; 6º, II, III, IV e VI, art. 18, art. 31; art. 37 e art. 39). A referida violação de dados foi constatada diante da possibilidade de compartilhamento indevido de dados de terceiros mediante consentimento que se utiliza do método *opt-out*, o que exige ação do usuário para impedir que aconteça um compartilhamento de dados de terceiros de forma automática. Mesmo que tal consentimento estivesse escrito nos termos de utilização da supracitada rede social, foi constatada falta de transparência no processo de transferência de dados pessoais que atingiram, segundo próprio Facebook, pouco mais de 400.000 brasileiros. Estes tiveram seus dados pessoais expostos e estavam à disposição de terceiros. Foi constatado que os

---

[96] REsp 1.758.799/MG, Relatora: Min Nancy Andrighi, julgamento em: 12/11/2019. Fonte: DJe 19/11/2019.

[97] Disponível em: < https://www.defesadoconsumidor.gov.br/images/Nota_T%C3%A9cnica_32-2019.pdf> Acesso realizado em 28/08/2021.

usuários/consumidores do Facebook não tinham o pleno conhecimento de que seus dados poderiam ser utilizados em técnicas semelhantes às empregadas pela Cambridge Analytica para captação de dados pessoais e posterior criação de perfis de usuários que posteriormente foram utilizados para influenciar processos eleitorais de grande porte em outros países, por exemplo Brexit, no Reino Unido, e a eleição presidencial americana de 2016. Portanto, a forma de consentimento alegada pela defesa do Facebook tinha caráter genérico e maculava a finalidade que embasava a permissão inicial concedida pelo titular de dados, isto feriu o que fora definido pelo MCI que exige que o consentimento seja livre, expresso e informado. Deste modo, ficou claro que esta violação lesionava direitos de personalidade, por exemplo: direitos à privacidade. Embora a coleta tenha acontecido por meio de aplicativo de terceiros o Facebook é responsável por monitorar o fluxo de dados pessoais. Sobre a forma de solicitar o consentimento de seus usuários o DPDC observa que:

> Ainda, é importante deixar claro que, o caráter "genérico" do consentimento obtido pela plataforma Facebook em face de seus usuários não pode ser visto como um "cheque em branco" para que esses dados sejam disponibilizados a quem quer que seja e, no caso dos autos, o comportamento das Representadas não estava em consonância com a declaração de vontade dos consumidores (notadamente aqueles que não aderiram ao aplicativo thisisyourdigitallife), violando, dentre outros, o art. 112 do Código Civil (que também é aplicável ao presente caso, em harmonia com o CDC), acima transcrito. As Representadas também não se desincumbiram de demonstrar que tais dados não foram eliminados e nem foram compartilhados com os responsáveis pela Cambridge Analytica, conforme visto acima. Por fim, é importante esclarecer que são as Representadas que – no âmbito do modelo de opt-out adotado – dispõem de maior capacidade de monitorar os desenvolvedores de aplicativos que operam na plataforma Facebook do que os próprios consumidores.
> Tendo em vista o que foi colocado ao longo da presente Nota, notadamente a implicação de um dever maior de cuidado que deve ser imposto à plataforma Facebook na guarda das informações disponibilizadas pelos seus usuários, verifica-se à ocorrência de prática abusiva. Com efeito, (apesar de todas as contradições das Representadas quanto a extensão dos fatos apurados), resta evidente que dados dos cerca de quatrocentos e quarenta e três mil usuários da plataforma estavam em disposição indevida pelos desenvolvedores do aplicativo thisisyourdigitallife para finalidades, no mínimo, questionáveis, e sem que as Representadas conseguissem demonstrar eventual fato modificativo de que tal número foi efetivamente menor. Neste particular, é importante destacar que é incontroverso nos autos que tal aplicativo atuou em violação aos termos de uso da plataforma Facebook. Em sendo assim, é inevitável que dados de usuários brasileiros foram parar em mãos erradas e ficaram, no mínimo, submetidos a risco concreto (e não meramente abstrato) de serem tratados para finalidades não consentidas.[98]

Ao final da recomendação foi proposta uma multa à empresa em questão

[98] BRASIL. Nota Técnica n.º 32/2019/CGCTSA/DPDC/SENACON/MJ, p. 19.

de R$ 6.600.000,00.[99]

Em sua análise, Ana Frazão observa que embora a LGPD não estivesse disponível para sua aplicação aos casos supracitados, o STJ e o MJ utilizaram a legislação disponível para determinar um quadro protetivo aos dados pessoais com institutos que posteriormente seriam chancelados pela vigência do texto da LGPD.

Embora existissem antes da LGPD ferramentas distribuídas na legislação brasileira que permitissem a proteção dos dados pessoais, elas eram insuficientes diante das exigências que a GDPR implementa sobre a transferência de dados para países com nível de proteção equivalente a norma europeia. Portanto, a Lei nº 13.709/2018 foi um marco no ordenamento jurídico pátrio porque consolidou em uma lei geral considerável conjunto de institutos de proteção do titular de dados pessoais. Considerada necessária a construção da lei supracitada em face do contexto atual de "datificação" do ser-humano, a LGPD coloca o Brasil no rol de países que possuem legislação de segurança de dados semelhante à GDPR.

A LGPD visa defender o titular dos dados. Contudo, para que ela atinja essa finalidade é primordial que também proteja o ciclo de vida desses dados. Isso inclui desde sua concepção, por exemplo, por meio de coleta de dados ou informações por meio de uma *smartband*, *smartphone* ou meio físico como arquivos em papel, até o seu tratamento (por exemplo por algum método de *profiling*) até o fim de vida dos dados (o que poderia incluir o completo apagamento ou destruição de dados daquela pessoa em um banco de dados).

Um breve registro deve ser feito de que no imaginário de muitos haja uma estrita relação entre dados pessoais e arquivos digitais. Entretanto, da leitura da art. 1º da lei a proteção de dados pessoais vai além do mundo virtual e alcança qualquer registro, inclusive os físicos em papel. Deste entendimento corroboram Patrícia Pinheiro[100] e Tarcísio Teixeira[101]. Este último juntamente com Ruth Armelin entende que entre os dados a que a lei em comento se refere são:

> [...] tão somente aqueles inerentes à pessoa, tais como nome, endereço, e-mail, sexo, profissão ou aqueles que possam levar à identificação da pessoa, tais como IP (*Internet Protocol*; em português, Protocolo de

[99] Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/2019/12/30/ministerio-da-justica-multa-facebook-em-r-66-milhoes-em-apuracao-sobre-compartilhamento-de-dados.ghtml >. Acesso realizado em 28/08/2021.
[100] PINHEIRO, Patrícia Peck. **Proteção de dados Pessoais: comentários à Lei n. 13.709/2018 (LGPD).** 3 ed., São Paulo: Saraiva Educação, 2021, p.92.
[101] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca**.** Op. Cit, p.28.

> Internet), dados estatísticos e quaisquer outros dados que, de alguma forma, levem à identificação de um único indivíduo.[102]

Entre os destaques legislativos trazidos pela LGPD, Bruno Bioni[103] ensina que embora o consentimento do titular ainda seja uma das bases de tratamentos de dados pessoais mais utilizadas, o art. 7º da lei expandiu o número de hipóteses de bases colocando-as em mesmo nível hierárquico conforme pode-se perceber abaixo:

> 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 terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, 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. (Grifou-se)

Além das inovações ora apontadas é importante mensurar o impacto do âmbito jurídico a proteção que a LGPD exerce sobre decisões automatizadas. Como exemplo considere o disposto no art. 20:

> 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.

Sobre esse artigo a defesa de sua pertinência no corpo do novel diploma legislativo decorre da intensificação dos processos de automação na coleta e tratamento de dados pessoais, o sistema de avaliação de crédito (*credit score*) é um

---

[102] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca**.** Op. cit, p.27.
[103] BIONI, Bruno R. Op. cit. p. 127.

exemplo. Esse artigo permite que o titular de dados exerça a defesa de sua personalidade e o que estiver a ela ligado quando passa a assegurar o direito de revisão de decisões tomadas única e apenas de forma automatizada, como por exemplo por meio de algoritmos ou robôs de inteligência artificial. Considerando que se vive em um contexto de uma proliferação de robôs na tomada de decisões referente a análise de grandes volumes de dados: "[...] Não é porque foi um robô que tomou a decisão que o direito à transparência e ao livre acesso será tolhido do usuário, respeitados, evidentemente, os segredos comercial e industrial."[104]

Continuando seus ensinamentos, Teixeira e Armelin[105] defendem que:

> A inclusão deste artigo pelo legislador revela a sua preocupação com o limite da influência da decisão de uma máquina sobre a vida das pessoas, considerando-se que muitas vezes a análise de dados se dará de forma automatizada, sem a interferência de uma pessoa natural, o que pode levar a premissas errôneas e consequente discriminações e abusos por parte do agente de tratamento.

Sobre a abrangência da atuação do art. 20 na LGPD, Patrícia Peck[106] entende que:

> Este é um artigo mais polêmico, visto que envolve as situações de uso de métodos automatizados de análise de dados, como ocorre, por exemplo, em processos de seleção (análise de volume de informações de perfis de candidatos) e também na concessão de crédito (na análise de *score*). Claramente, devido ao volume, uso de robôs é uma forma de melhoria da análise (aplicação de métodos de *analytics* com *big data*).

Na mesma obra, Peck passa a esclarecer que não existe no texto do supracitado artigo a obrigatoriedade de que essa revisão da decisão seja realizada exclusivamente por uma pessoa natural. Isso porque o legislador entendeu pela possibilidade de que essa revisão seja executa pela própria IA que decidiu anteriormente. Contudo, uma pessoa natural poderia esclarecer o funcionamento do processo de decisão da IA, respeitados o direito livre dos contratos entre as partes e o segredo comercial e industrial.

---

[104] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca**.** Op. cit, p.86.
[105] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca**.** Op. cit, p.87.
[106] PINHEIRO, Patrícia Peck. Proteção de dados Pessoais..., Op. cit., p.129.

4 DISCRIMINAÇÃO ALGORÍTMICA E A PROTEÇÃO TRAZIDA PELA LGPD

O tratamento automatizado de dados já permeia várias camadas da sociedade humana. Como exemplos pode-se destacar: "[..] A próxima música preferida, a publicação na rede social que será curtida, o melhor itinerário no trânsito agora e a escolha sobre as condições de renovação de um contrato".[107] Ainda conforme aponta Felipe Medon[108]:

> Da seleção para uma vaga de emprego, à concessão de crédito, passando pela abordagem policial nas ruas: o processo decisório por trás dessas ações será eminentemente fundado em algoritmos comandados por Inteligência Artificial. Mas os algoritmos podem falhar. E causar danos.

Essas ações ora descritas são realizadas por algoritmos e uma das suas principais finalidades é utilizar a probabilidade estatística para fazer previsões mais próximas de tornarem-se uma realidade. De acordo com a lição conjunta de Laura Schertel Mendes, Marcela Mattiuzzo e Mônica Tiemy Fujimoto[109]:

> Embora algoritmos não possam fornecer respostas precisas a todas as questões, eles podem analisar os dados fornecidos (inputs) e oferecer "palpites" coerentes. Quanto maior a quantidade e qualidade dos dados disponibilizados ao algoritmo, maior a chance de o resultado estar próximo do real.

Considerando os efeitos do avanço tecnológico em nossas vidas, conforme aumenta a participação da IA e especificamente a sua área do *machine learning* (aprendizado de máquina), onde os próprios algoritmos estão capazes de escrever seus próprios algoritmos de aprendizagem para que os humanos não precisem mais escrever cada detalhe do código fonte de certo programa de computador, os computadores agora conseguem chegar a solução desejada conforme os dados (*inputs*) e o resultado que se deseja.[110] Portanto, faz-se mister que junto com as benesses dessas aplicações também sejam considerados quais riscos podem afetar as pessoas e como os mesmos podem ser reparados ou

---

[107] SOUZA, Carlos Afonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. In: **Tratado de proteção de dados pessoais.** DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz. (coord.), 1. ed., Rio de Janeiro: Forense, 2021, p. 243.
[108] MEDON, Filipe. Op. cit., p. 220.
[109] MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da lei geral de proteção de dados. In: **Tratado de proteção de dados pessoais.** DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz. (coord.), 1. ed., Rio de Janeiro: Forense, 2021, p. 423.
[110] MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO. Ibidem, p. 424.

minorados.[111] Conforme observado adiante, uma questão importante nessa seara é a obscuridade ou opacidade algorítmica frente aos processos automatizados decisórios.

A importância de um diploma normativo geral que busque proporcionar o equilíbrio entre a proteção de dados e o avanço da tecnologia é fundamental para que a sociedade não seja consumida pela caixa de pandora criada pelos supracitados algoritmos de IA e pelas técnicas de *Big Data*. Conforme ensina Frank Pasquale esses algoritmos não são transparentes para seus usuários. Considerados verdadeiras caixas pretas (*blackboxes*), eles são determinados por fórmulas complexas concebidas por um forte aparato de cientistas e engenheiros e defendidas por um exército de advogados.[112] Sobre o processo de construção desses algoritmos Pasquale também observa que existem possibilidades de que eles possam causar danos:

> Algoritmos não são imunes ao problema fundamental da discriminação, e que suposições infundadas e negativas se solidificam em preconceito. Eles são programado por seres humanos, cujos valores estão embutidos em seu software. E muitas vezes eles (algoritmos) frequentemente utilizam dados que estão viciados demais com o preconceito humano.[113] (Tradução Livre).

Umas das principais promessas concernentes a decisões tomadas por algoritmos é de que eles são mais objetivos em seu processo de escolha da decisão e que estão livre de vieses característicos das decisões efetuadas por seres humanos. Entretanto, há registros de que a imparcialidade algorítmica pode ser comprometida por: dados enviesados ou viciados que alimentam os algoritmos; ou pelo tipo de método usado na decisão automatizada que cria um efeito discriminatório não intencional.[114]

---

[111] DUARTE, Fernando. Nove algoritmos que podem estar tomando decisões sobre sua vida – sem você saber. Disponível em: <https://www.bbc.com/portuguese/geral-42908496>. Acesso em: 05/09/2021.

[112] PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015, p. 6.

[113] *Algorithms are not imune from the fundamental problem of discrimination, in which negative and baseless assumptions congeal into prejudice. They are programmed by human beings, whose values are embedded into their software. And they must often use data laced with all-too human prejudice.* (PASQUALE, Frank. Ibidem, p. 38.)

[114] DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso; ANDRADE, Noberto Nunes Gomes de. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar**, Fortaleza, v.23, n.4, 2018, p.5.

4.1 Os casos COMPAS e Decolar.com: efeitos da discriminação algorítmica por métodos de perfilização

Sobre a questão da opacidade e efeito discriminatório referente ao processo de decisão automatizada de algoritmos e como esses sistemas de IA podem gerar danos graves, destaque-se o caso *State v Loomis*[115] que aconteceu no estado de Wisconsin, Estados Unidos da América. Neste caso o sistema de análise matemática COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) fora utilizado para análise de reincidência em crimes. Ele utilizava um questionário respondido pelo réu onde essas respostas alimentariam o algoritmo matemático. Como resultado este determinaria uma pontuação que corresponderia ao grau de reincidência em crimes do referido réu, ajudando o juízo a "[...] decidir se a pessoa vai ser solta com pagamento de fiança, se deve ser mandada para a prisão ou receber outro tipo de sentença e - se já estiver na cadeia - se tem direito a liberdade condicional."[116]

Embora a finalidade desse sistema seja reduzir a subjetividade das decisões judiciais por livrá-las de vieses racistas ou preconceituosos, relevante é a observação de Filipe Medon:

> O grande problema é que o COMPAS pode acabar dando pontuações consideravelmente maiores para infratores pertencentes a minorias étnicas, revelando um preconceito oculto no algoritmo, cujo funcionamento não é revelado por motivos de segredo comercial.
> [...] Instada a se manifestar, a Suprema Corte de Wisconsin autorizou, em 2016, que o COMPAS continuasse sendo utilizado para ajudar os juízes nas sentenças, mas a Corte expressou hesitação quanto ao futuro, tendo em vista as limitações técnicas do algoritmo. Com efeito, acabou deliberando por algumas restrições, sendo a principal delas o fato de que o propósito original do COMPAS não deve ser sentenciar, mas atuar como ferramenta de assistência para a análise de um indivíduo.[117]

Um exemplo local de discriminação algorítmica é o caso da empresa Decolar.com que praticou ações caracterizadas como *geo princing* e *geo blocking*. Essas práticas "[...] consistem em discriminações injustificadas feitas a consumidores por critérios geográficos para efeitos de diferenciação do preço das acomodações (*geo princing*) e para a negativa de oferta de vagas (*geo blocking*)."[118] A supracitada empresa foi multada em R$ 7.500.000,00 pelo Departamento de

---

[115] Disponível em: <https://harvardlawreview.org/2017/03/state-v-loomis/>. Acesso em: 03/09/2021.
[116] Disponível em: < https://www.bbc.com/portuguese/brasil-37677421>. Acesso em: 03/09/2021.
[117] MEDON, Filipe. Op. cit. p. 226, 227.
[118] MEDON, Filipe. Op. cit. p. 253.

Proteção e Defesa do Consumidor que apurou "[...] discriminação da empresa com consumidores por conta da etnia e localização geográfica, o que configura prática abusiva, além de verdadeiro desequilíbrio no mercado e nas relações de consumo."[119] Conforme apontado pela investigação a Decolar.com:

> [...] estaria oferecendo reservas a preços diferentes, a depender da localização do consumidor, identificado por intermédio do Internet Protocol – IP (identificação única para cada aparelho com acesso a Internet, conectado a uma rede), prática conhecida como geo pricing. Além disso, a Decolar estaria também ocultando a disponibilidade de acomodações a consumidores brasileiros, em favor de consumidores estrangeiros, conduta denominada geo blocking. Ambas as práticas discriminam consumidores em razão da localização geográfica destes.
> 3. Com vistas a comprovar o alegado, a empresa Booking colacionou aos autos pesquisa de simulação simultânea de reserva de hospedagem no site da empresa Decolar, por meio de computadores localizados nas cidades de São Paulo (Brasil) e Buenos Aires (Argentina), na qual foram registrados valores diferentes para as mesmas reservas (i.e., acomodações iguais, na mesma data), os preços alcançaram a margem de até 29% a mais para os consumidores brasileiros".
> [...] 4. Outrossim, foi constatada a indisponibilidade de algumas acomodações para o notário de São Paulo, enquanto que, em Buenos Aires, ao mesmo tempo, a mesma acomodação era mostrada como disponível. A pesquisa foi realizada nas datas entre 26 de abril e 4 de maio de 2016.[120]

Fica evidente que estas práticas violam o "[...] artigo 39 do CDC nos seus incisos II, V, IX e X, bem como o artigo 9º, §2º, incisos II e IV do Marco Civil da Internet e o artigo 6º da LGPD, que traz o princípio da não discriminação."[121] Este princípio encontra-se enunciado no inciso IX do referido artigo da LGPD que diz: "[...] não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos."[122] Felipe Medon aponta ainda que a questão discriminatória referente a utilização de algoritmos no site da referida empresa resta-se comprovada pela presunção do "[...] suposto maior poder de compra de um estrangeiro".[123]

Esta prática também é chamada de *weblining*. Conforme podemos ver em sua definição abaixo essa atitude:

---

[119] Disponível em: < https://www.justica.gov.br/news/collective-nitf-content-51>. Acesso em: 05/09/2021.
[120] Nota Técnica n.º 92/2018/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/SENACON/MJ. Disponível em: < https://www.cmlagoasanta.mg.gov.br/abrir_arquivo.aspx/PRATICAS_ABUSIVAS_DECOLARCOM?cdLocal=2&arquivo=%7BBCA8E2AD-DBCA-866A-C8AA-BDC2BDEC3DAD%7D.pdf>. Acesso em: 05/09/2021.
[121] MEDON, Filipe. Op. cit. p. 254.
[122] BRASIL. Lei 13.709/2018.
[123] MEDON, Filipe. Op. cit. p. 254.

> [...] que tem origem nas antigas práticas de seguradoras, que desenhavam linhas vermelhas - *redlining* - nos mapas das cidades para negar o acesso ao contrato de seguro, cancelá-lo ou vedar sua renovação em regiões de alto risco. De igual forma, indenizações eram calculadas considerando diferenças étnicas. O *redlining é* considerado ilegal em mais de quarenta Estados norte-americanos. O *weblining* é a nova versão da técnica discriminatória, aplicada no ciberespaço, à luz das técnicas de geolocalização, criando perfis especializados, no sentido de negar acesso a determinados bens e serviços ou diferenciar preços a moradores de determinadas regiões de acordo com sua condição financeira ou determinada etnia.[124]

Por fim destaque-se o útil ensinamento de Bruno Bioni[125] que demostra o quanto essas práticas como a demostrada no caso Decolar.com podem ser danosas para o indivíduo:

> [...] Essas são amostras de que a categorização da pessoa, a partir de seus dados pessoais, pode repercutir nas suas *oportunidades sociais*, no contexto de uma sociedade e uma economia movida por dados.
> Por exemplo, o próprio ato de consumo pode ser modelado com base no histórico de compras. Por meio dele, cria-se um perfil do consumidor para direcionar preços de acordo com a sua respectiva capacidade econômica (*price-discrimination*).
> É a prática conhecida como *profiling*, em que os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. Tudo é calibrado com base nesses estereótipos; inclusive o próprio conteúdo acessado na Internet.

Outro fator que deve ser levado em consideração é que os dados de geolocalização (seja o monitoramento do IP ou pela utilização de sistemas de satélites como o GPS) quando cruzados com dados pessoais podem gerar novas informações que por sua vez poderão ser categorizadas como dados pessoais sensíveis. Por exemplo, uma plataforma digital ao coletar dados de localização que indiquem a frequência e periodicidade com que uma pessoa visita determinado endereço tem a possibilidade de indicar que essa pessoa realiza um tratamento médico ou participa de uma prática religiosa.[126] Logo, é importante que seja oportunizado ao titular de dados a possibilidade de que ele não revele sua localização geográfica. Caso esta informação seja imprescindível para o

---

[124] COLOMBO, Cristiano; NETO, Eugênio Facchini. Decisões automatizadas em matéria de perfis e riscos algorítmicos. In. MARTINS, Guilherme Magalhães; ROSENVALD, Nelson; (Coord.). **Responsabilidade civil e novas tecnologias**. Indaiatuba, SP: Editora Foco, 2020, p. 170.
[125] BIONI, Bruno R. Op. cit. p. 88.
[126] COLOMBO, Cristiano; GOULART, Guilherme Damásio. Ética algorítmica e proteção de dados pessoais sensíveis: classificação de dados de geolocalização em aplicativos de combate à pandemia e hipóteses de tratamento. In. BARBOSA, Mafalda Miranda; NETTO, Felipe Braga; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência Artificial:** diálogos entre Brasil e Europa. Indaiatuba, SP; Editora Foco, 2021, p. 277.

funcionamento da aplicação ou serviço digital o usuário deverá ser explicitamente comunicado que a informação de geolocalização será coletada e para qual finalidade esta será empregada. Esta ciência ao usuário é importante para que haja um consentimento livre e esclarecido do titular de dados pessoais e assim este tenha condições de decidir se usará aquela aplicação.

Portanto, em virtude desses eventos a legislação setorial vista no capítulo 3 desta pesquisa somará esforços com a LGPD como ferramentas robustas para prevenção e reparação aos danos causados por essas tecnologias. Esta última norma, por exemplo, contém dois importantes direitos que serão analisados em seguida: o primeiro é o direito à explicação, direito este concernente à condição do titular dos dados obter explicações claras, necessárias e compreensíveis que o permitam entender o funcionamento da lógica e a condições de tratamento de seus dados para determinada finalidade ou resposta automatizada. O segundo é o direito à revisão de todas as decisões totalmente automatizadas relativas ao uso de dados pessoais conforme previsto no art. 20.

4.2 O direito à explicação e à revisão de decisões automatizadas

Considerando o contexto das situações ocasionadas acima pela atuação de algoritmos, IA, técnicas de perfilização, *Big Data* e o uso dos rastros digitais da pessoa natural, Ana Frazão[127] levanta o debate sobre a questão da transparência e *accountability* dessas tecnologias:

> Ora, para que se pudesse ter um mínimo de confiança e tranquilidade em relação a tais processos, seria necessário haver algum tipo de controle tanto sobre (i) a qualidade dos dados, a fim de se saber se atendem aos requisitos de veracidade, exatidão, precisão, acurácia e sobretudo adequação e pertinência diante dos fins que justificam a sua utilização, quanto sobre (ii) a qualidade do processamento de dados, para se saber se, mesmo a partir de dados de qualidade, a programação utilizada para o seu tratamento é idônea para assegurar resultados confiáveis.

Portanto, urge a utilização de mecanismos de transparência e *accountability* para que o mundo dominado por algoritmos possa tornar-se o minimamente compreensível para aqueles que são afetados pelas decisões algorítmicas. Apesar de que há uma limitação para o entendimento da técnicas de construção e funcionamento de algoritmos ou desenvolvimento dos softwares que

[127] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais ..., Op. cit. p. 38.

personificam esses algoritmos, seja por exigir das pessoas conhecimentos técnicos especializados relacionados as ciências ou engenharias de hardware/software ou dados ou seja porque esses produtos tecnológicos muitas vezes estão sob a guarda do sigilo comercial/industrial, é preciso que a sociedade inicie os primeiros passos na buscar para reduzir a opacidade algorítmica. Na visão de Ana Frazão[128]:

> A grande discussão, portanto, é saber, entre o que não é conhecido, o que pode e deve ser conhecido, como pressuposto mínimo da proteção de direitos individuais e da própria democracia. Somente assim será possível avaliar minimamente os riscos das crescentes categorizações e perfilizações, inclusive para o fim de delimitar que listas ou categorias não deveriam ser nem mesmo criadas.

No contexto brasileiro Renato Leite Monteiro nos ensina que o direito à explicação é oriundo do direito à transparência delineado pela LGPD em seu art. 6º, inciso VI: "[...] transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial."[129] Ele ainda observa, referente ao direito à explicação e à transparência, que antes da aprovação da LGPD, "[...] tais direitos só eram garantidos em decisões automatizadas relativas à concessão de crédito, modelagem e cálculo de risco de crédito."[130] Logo, na visão de Renato Monteiro outra violações a direitos relacionados à explicação sobre o tratamento automatizado de dados pessoais encontrariam óbice para saneamento utilizado a legislação vigente, como por exemplo: o direito à saúde ser ameaçado quando os dados genéticos (considerados pela LGPD como dados pessoais sensíveis conforme disposto em seu art. 5º, inc. II) de uma pessoa fossem usados por um algoritmo de seguro de saúde para cálculo de probabilidade do segurado vir a contrair doença que necessite de tratamento de alto custo e desta feita o contrato de seguro fosse rejeitado ou extremamente majorado pela seguradora.[131] Uma vez que a proteção setorial trazida pelo CDC e a Lei do Cadastro Positivo não seriam suficientes para a situação supracitada. Logo verifica-se a urgência de uma Lei geral de abrangência nacional relativa à proteção de dados que possa expandir o rol de proteções contra o mal uso de dados nos mais variados contextos da vida em

---

[128] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais ..., Op. cit. p. 42.
[129] BRASIL. Lei 13.709/2018.
[130] MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? In: **Instituto Igarapé**, artigo estratégico 39, 2018, p. 5. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf> Acesso: 04/09/2021.
[131] MONTEIRO, Renato Leite. Op. cit, p. 3.

sociedade, lei esta que se entremearia em diversas searas aprimorando garantias como o direito à explicação e à revisão de decisões algorítmicas.[132]

Entre uma das obrigações do controlador de dados consta no §1º do art. 20 que este deve "[...] 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."[133] Sobre a forma prática de garantir a execução desse parágrafo, Renato Monteiro[134] pondera:

> Caso o responsável pelo processamento dos dados se recuse a fornecer os dados pessoais utilizados na decisão automatizada e a explicar os critérios e/ou a lógica subjacente dos algoritmos que controlam o processo de tomada de decisão, a Lei prevê que poderá ser requisitado à futura Autoridade Nacional de Proteção de Dados (ANPD) que seja realizada, após processo administrativo em que deve ser garantido a ampla defesa e o contraditório, auditoria nos sistemas da entidade. Esse procedimento visa verificar, principalmente, a existência de aspectos discriminatórios, tais como o uso de dados pessoais sensíveis ou que excedam a finalidade pretendida. Todavia, aferir eventuais discriminações pode ser um trabalho extremamente técnico, devido à complexidade dos algoritmos, o que demonstra a necessidade de a ANPD ter um corpo de profissionais altamente especializado e preparado. Portanto, a LGPD amplia essas vedações no uso de dados para além das relações de consumo, para incluir outros usos de dados pessoais.

Sob ótica semelhante, Felipe Medon[135] compartilha o papel que poderá ser desempenhado pela ANPD no que tange a dificuldade prática de exigir transparência total de um algoritmo que está acobertado pelo segredo comercial ou a sua livre disponibilidade de como ele funciona para o público poderia inviabilizar o processo de inovação tecnológica ou deixar o algoritmo vulnerável a manipulações de terceiros:

> Em vez de transparência quanto aos algoritmos, a melhor saída seria acabar com a opacidade dos dados, que deveriam sofrer interferência. Dito de maneira diversa, dever-se-ia procurar que os dados utilizados para treinar um algoritmo fossem avaliados previamente, sendo, por vezes, apropriado compartilhar detalhes de inputs e outputs com um terceiro e idôneo, que pudesse revisar a justiça do algoritmo responsável pela tomada de decisões. No Brasil, talvez não fosse equivocado pensar que a Autoridade Nacional de Proteção de Dados pudesse desempenhar algum papel nesse contexto, uma vez que o parágrafo segundo do artigo 20 da LGPD já prevê que a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, nos casos em que não se forneça ao titular de dados as informações

[132] MONTEIRO, Renato Leite. Op. cit, p. 9.
[133] BRASIL. Lei nº 13.709/2018.
[134] MONTEIRO, Renato Leite. Op. cit., p. 10.
[135] MEDON, Filipe. Op. cit. p. 296.

> solicitadas em razão da necessidade de preservação do segredo comercial industrial.

Entre os comandos previstos na LGPD no art. 20, §1º visando estabelecer o direto à explicação e à revisão de decisões tomadas exclusivamente por processos automatizados, temos o papel da Agência Nacional de Proteção de Dados (ANPD) conforme descrito na parte final do §2º do art. 20: "[...] a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais."

Referente ao entendimento do art. 20, A. Barreto Menezes Cordeiro[136] leciona que o termo "decisão" pode ser conceituado da seguinte forma:

> Por decisão entende-se um ato, numa aceção não jurídica, que incida sobre um caso concreto e produza efeitos jurídicos relativamente a um ou mais titulares de dados específicos, quer seja a aceitação ou a recusa de um pedido, a sua caracterização, catalogação, atribuição de uma classificação, definição de perfil ou qualquer outra medida análoga produtora de um efetivo resultado.

Segundo os ensinamentos de Cristiano Colombo e Eugênio Facchini Neto[137] a definição do que seria uma decisão exclusivamente automatizada pode ser descrita como um processo de decisão sem intervenção humana que gera uma resposta ao usuário sem a participação humana na análise ou revisão da referida decisão. Eles passam a mostrar que o início do processo de perfilização (*profiling*) ocorre com a participação dos dados dos próprios usuários de determinados sistemas de informação ou serviços que fornecem esses dados conscientemente ou não. Sobre alguns exemplos de como ocorre essa captação de dados com a finalidade de alimentar o funcionamento de perfilização destaque-se:

> Especialmente através da atribuição de uma nota (*rating*), com a distribuição de estrelas ou escolha de símbolos de sentimentos (*emoticons*) (embora sem a exclusão do uso da escrita alfabética em espaços apropriados para a redação de textos), os internautas externalizam opiniões e recomendações, gerando *inputs*, sob a forma de feedback para a comunidade. Os textos escritos são submetidos ao "Processamento da Linguagem Natural" (PLN, ou NLP, *Natural Language Processing*), a fim de identificar palavras ou frases como positivas, negativas ou neutras, permitindo classificar o sentimento ligado ao subscritor da mensagem. Os conteúdos gerados pelos usuários (user-generated-contents-UGCs) passam a ser inputs aos algoritmos que buscam a granularidade dos sentimentos,

---

[136] CORDEIRO, A. Barreto Menezes. Decisões individuais automatizadas à luz do RGPD e da LGPD. In: BARBOSA, Mafalda Miranda; NETTO, Felipe Braga; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência Artificial:** diálogos entre Brasil e Europa. Indaiatuba, SP; Editora Foco, 2021, p. 266.

[137] COLOMBO, Cristiano; NETO, Eugênio Facchini. Op. cit., p. 165.

> projetando interesses, tendências e intenções, a partir da construção de perfis dos seus consumidores.

Por fim, Medon[138] defende que o direito à explicação embora estivesse inscrito no CDC e na Lei do Cadastro Positivo, agora encontra melhor guarida no art. 20, §1º da LGPD. Semelhante pensamento é defendido por Renato Monteiro[139]:

> Em síntese, a LGPD garante aos indivíduos o direito a ter acesso a informações sobre que tipos de dados pessoais seus são utilizados para alimentar algoritmos responsáveis por decisões automatizadas. Caso o processo automatizado tenha por finalidade formar perfis comportamentais ou se valha de um perfil comportamental para tomar uma decisão subsequente essa previsão também incluirá o acesso aos dados anonimizados utilizados para enriquecer tais perfis. Esse direito ainda inclui a possibilidade de conhecer os critérios utilizados para tomar a decisão automatizada e de solicitar a revisão da decisão por um ser humano quando esta afetar os interesses dos titulares.
> Pela Lei, os direitos à explicação e à revisão de decisões automatizadas podem ser usufruídos em qualquer tipo de tratamento de dados pessoais, independente do setor ou mercado. Isto confere ao titular dos dados pessoais ferramentas importantes para coibir abusos e práticas discriminatórias no uso dos seus dados. Tais direitos devem contribuir diretamente para uma mudança na forma como produtos, serviços e processos são desenvolvidos, devido às obrigações de informar e explicar atribuídas aos agentes de tratamento. Estes terão que pensar, desde a concepção, como garantir os direitos previstos na LGPD. Espera-se que isso diminua a obscuridade e a opacidade dos algoritmos.

Continuando no campo das decisões automatizadas é interessante que no texto original da LGPD havia a previsão de que no exercício do direito de revisão a pessoa afetada pudesse solicitar que essa revisão fosse realizada por outra pessoa natural:

> Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.[140]

A Medida Provisória nº 869/2018, entretanto, retirou esta referência de revisão "por pessoa natural" do caput do art. 20. Embora o Congresso Nacional tenha emendado o referido artigo por incluir o §3º com o seguinte texto:

> A revisão de que trata o caput deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que

---

[138] MEDON, Filipe. Op. cit. p. 297.
[139] MONTEIRO, Renato Leite. Op. cit., p. 11.
[140] Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html> Acesso em: 06/09/2021.

> levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados."[141]

Contudo, durante a conversão da supracitada MP na Lei nº 13.853/2019 o Presidente da República vetou o supracitado parágrafo sob o seguinte motivo:

> "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."

Portanto, embora essas mudanças no corpo legislativo retirem à obrigação de que a revisão da decisão automatizada seja executada por pessoa natural, o texto vigente da lei já propicia um adequado nível de proteção contra a discriminação algorítmica e uma garantia do direito à explicação.

Conforme aponta a doutrina sobre o uso de uma revisão humana de decisões efetuadas exclusivamente por algoritmos recebe-se grata lição referente ao protagonismo do tratador de dados em prover meios que possibilitem a participação humana no exercício do supracitado direito e o papel da Autoridade Nacional de Proteção de Dados na regulação deste tema:

> A redação atual da lei não demanda revisão por pessoa natural. No entanto, deve-se entender que, para garantir o pleno exercício do direito de revisão, este deve ser efetivo e permitir que se possa chegar a conclusões diferentes das apresentadas pela decisão automatizada original. Desse modo, deve-se considerar que a revisão para uma pessoa natural é uma prática recomendável, sempre e quando seja possível e pertinente para os fins aqui debatidos.
> A LGPD, então, criou um direito de revisão e nada no texto impede que seja estabelecido que a revisão com intervenção humana seja o padrão a ser utilizado em casos concretos. Justamente o contrário, nos casos em que caiba, o arcabouço geral de proteção da lei parece acomodar a visão de que a inserção de humanos na revisão pode tornar o processo mais plural e acessível. A intervenção humana reforçaria, assim, a confiança do usuário, que tenderia a acreditar ainda mais no processo, aumentando a percepção de transparência.
> Igualmente, nada impede que a ANPD teça recomendações específicas sobre como deve se dar a revisão. O simples fato de não ser determinada legalmente a intervenção humana na revisão não impede que a autoridade de proteção estabeleça casos em que, para dar vazão aos objetivos gerais da lei e melhor concretude a seus princípios, dita intervenção (por pessoa natural) seja recomendada. Nesse sentido, a prática das organizações,

[141] Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm> Acesso em: 06/09/2021.

> somada a atuação da ANPD, determinará o grau de participação humana na revisão de decisões automatizadas.[142]

Nesta última hipótese a ANPD faria uso de suas atribuições elencadas no art. 55-J para usar auditorias como mecanismo de controle e fiscalização na consecução do cumprimento do direito à explicação e à revisão conforme estão descritos nos incisos abaixo:

> Art. 55-J. Compete à ANPD:
> [...] IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> [...] XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

Conforme leciona Pedro Rubim Borges Fortes[143] as novas discussões suscitadas pelo avanço das tecnologias de informação e o tratamento de dados e a vigência dos dispositivos regulatórios listados no art. 55-J da LGPD demostram que o Estado possui uma responsabilidade algorítmica na defesa do interesse público que pode ser lesionado por decisões automatizadas ou pelo uso indevido de dados pessoais. Sobre como deve ser exercida essa responsabilidade pelo ente estatal o referido autor ensina:

> No âmbito da responsabilidade civil, o estado deve proteger os direitos dos usuários nas sociedades digitais, sendo necessária a intervenção institucional para tutelar direitos coletivos. O Estado deve agir como regulador, ator, legislador, de maneira a reequilibrar as assimetrias de poder e de informação entre as empresas e seus usuários para impedir efeitos negativos e lesivos. Atualmente, os processos informatizados a partir da coleta e processamento de grande volume de dados impõem uma mineração de dados e o uso da tecnologia de informação como fonte de riqueza e como um novo capital a ser acumulado, coordenado e distribuído. Nesse contexto, cabe ao poder público investigar, analisar e controlar as fórmulas matemáticas dos algoritmos, exercendo o devido controle normativo de seus efeitos de acumulação, coordenação e distribuição de dados. Em que pese o foco prioritário da literatura acadêmica contemporânea sobre a proteção do direito à privacidade dos usuários da internet, a responsabilidade algorítmica do estado exige um desenvolvimento muito mais amplo da capacidade de atuação e controle estatal.
> [...] Com essas fórmulas matemáticas são desenvolvidas através de vultosos investimentos em tecnologia da informação e possuem um caráter

[142] SOUZA, Carlos Afonso; PERRONE, Christian; MAGRANI, Eduardo. Op. cit., p. 267.
[143] FORTES, Pedro Rubim Borges. Responsabilidade algorítmica do Estado. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson; (Coord.). **Responsabilidade civil e novas tecnologias**. Indaiatuba, SP: Editora Foco, 2020, p. 436, 437.

> de propriedade industrial, o poder público enfrentará resistência quanto a ter acesso aos algoritmos com alegações de que se tratam de um bem privado e que a empresa precisa manter o segredo do negócio. Contudo, o Estado deve ser capaz de simultaneamente ter assegurado o seu acesso aos algoritmos e preservar o sigilo quanto aos detalhes de sua fórmula e ao segredo industrial respectivo. Desafio semelhante decorre do fato de que uma auditoria de algoritmos exige não apenas a análise da fórmula matemática, mas não raro a verificação do processamento de dados em situação real para se aferir como ocorre o tratamento e eventual manipulação da massa de dados dos usuários, especialmente se for empregada a tecnologia de aprendizado de máquina em que o processamento dos dados opera inclusive com base em operações que não foram previamente programadas pelos desenvolvedores humanos do software.

Na visão de Nuria López o art. 20 vai além de proporcionar o direito à explicação e à revisão. Esse artigo traz o dever de que tratador de dados detecte e corrija os vieses discriminatórios de seus algoritmos.[144]

Diante das dificuldades impostas pela opacidade algorítmica como as complexas técnicas de desenvolvimento do algoritmo de IA e as proteções legais que recaem sobre esses softwares, López[145] defende que outra abordagem diferente da questão legal para resolução de problemas relacionados aos viesses algorítmicos pode ser o desenvolvimento de uma cultura de boas práticas internas nas empresas desenvolvedoras desses algoritmos. Ela entende que a adoção de ferramentas de governança ética na criação do projeto e implementação da IA que trata de decisões automatizadas pode contribuir para o fortalecimento dessa cultura, por exemplo:

> Um instrumento prático para essa governança é o AIIA – *Artificial Intelligence Impact Assessment* (que em português poderia ser, para manter a nomenclatura da LGPD, um "relatório de impacto da inteligência artificial"). Ele é majoritariamente um *assessment* sobre ética e tecnologia – e é por essa razão que eticistas passam a ocupar lugares em tantas empresas de tecnologia e de consultoria no exterior.
> A dificuldade na elaboração de um AIIA reside no equilíbrio de ser específico o bastante para endereçar as questões pertinentes ao algoritmo em questão, pois não há um modelo que sirva a todos, e geral (não genérico) o bastante para visualizar o contexto geral de impacto da inteligência artificial. Alguns *assessments* existentes endereçam especificamente riscos de vieses discriminatórios já conhecidos como de idade, sexo ou raça ou etnia. O risco é de olhar para trás para aprender com as discriminações passadas e não ver adiante os riscos que novas tecnologias podem trazer. Por isso, questões mais abrangentes, desde que assertivas, permitem um desenvolvimento mais eficiente (e ético) da inteligência artificial.

---

[144] LÓPEZ, Nuria. Um direito, um dever: guia para o art. 20 da LGPD. In: **Proteção de dados: desafios e soluções na adequação à lei**. Alessandra Borelli Vieira ... [et al.]; org. Renato Muller da Silva Opice Blum. 2 ed., Rio de Janeiro: Forense, 2021, p. 189.
[145] LÓPEZ, Nuria. Um direito, um dever: guia para o art. 20 da LGPD. Op. cit., p. 193.

Como modelo desse tipo de prática é mencionada a iniciativa do governo canadense[146] que em sua ferramenta de análise de impactos causados por algoritmos de IA utiliza um questionário que determina o nível de impacto de sistemas de decisões automatizadas. Esse questionário visa ajudar órgãos do governo a aprimorar o gerenciamento dos riscos causados pelas decisões automatizadas utilizando fatores como o design do sistema de IA, o algoritmo, o tipo de tomada de decisão, os impactos nos usuários e os dados que serão utilizados.

[146] Disponível em: < https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> Acesso em 10/09/2021.

5 CONSIDERAÇÕES FINAIS

A evolução histórica das tecnologias de informação e comunicação permitiram a criação de um oceano de dados. Observa-se que o avanço da eletrônica na miniaturização dos componentes eletrônicos possibilitou o desenvolvimento da computação pessoal e aprimoramentos das redes de telecomunicações. Posteriormente, o barateamento dos custos de armazenamento e processamento de dados em conjunto com a expansão da rede mundial de computadores (Internet) impulsionou o nascimento da quarta revolução industrial. Esta por sua vez propiciou ferramentas e produtos que incrementam o uso de dados pessoais em nosso sistema econômico: dispositivos eletrônicos vestíveis conectados à Internet, computação em nuvem, redes de dados com alta largura de banda, videochamadas em tempo real etc.

Esse dilúvio de dados pessoais oriundos dos usos dessas tecnologias possui grande potencial econômico. Como exemplo do aproveitamento desses dados pode-se citar a categorização ou perfilamento dos gostos pessoais de determinado indivíduo. Este processo pode ser utilizado para que determinada empresa de publicidade lhe envie propaganda personalizadas. Outro exemplo é o uso de dados pessoais sensíveis provenientes de um *smartwatch* para que determinado aplicativo de *smartphone* faça uma análise desses dados e retorne para o usuário recomendações de cuidados com a saúde. Para que os exemplos citados ocorram faz-se necessário o uso de algoritmos de inteligência artificial na coleta e análise da grande quantidade de dados gerada em um ambiente de economia movida a dados. O uso da IA (algoritmos) e *profiling* (técnicas de perfilização) para coletar e tratar esses dados representam grande avanço no campo computacional e geram novas aplicações úteis como tradutores virtuais e softwares de reconhecimento de imagens.

Uma das formas de inteligência artificial que possibilitam essas atividades é o aprendizado de máquina (*machine learning*). Esta técnica permite que a IA implemente soluções com base em sua experiência anterior de trabalho, gerando novo conhecimento que é utilizado na próxima atividade que a IA executará. Desta forma não é necessário que o programador da IA escreva em seu algoritmo, ou código de programação, todos os passos necessários para se atingir determinado fim. A IA receber um conjunto básico de comandos e a partir de seu funcionamento e

uma carga de dados para alimentar essa inteligência, ela adquire a capacidade de aprender por si mesma.

Contudo, além dos benefícios trazidos pela IA, existem efeitos colaterais. Entre eles destaca-se a possibilidade de manipulação do comportamento humano por meio de publicidade direcionada. Isto pode levar desde o superendividamento de um indivíduo à manipulação de um processo eleitoral como o exemplo do caso relacionado a empresa Cambridge Analytica em 2016. Outro exemplo destacado neste trabalho é a perda de oportunidades relacionados a discriminação algorítmica em face de perfilização.

Como técnicas de *profiling*, algoritmos de IA e o *Big Data* usam métodos estatísticos para determinar uma probabilidade de certo evento ocorrer e para tanto utilizam os dados pessoais fornecidos por seus titulares, há a possibilidade de que uma correlação estatística atribua certo valor ou rótulo indevido a alguém, privando-o de certa oportunidade uma vez que aquela pessoa não encontra-se na mesma categoria dos que estão mais adequados a receber a referida oportunidade (seja propaganda, desconto, vaga de emprego, melhor nota de crédito etc.).

Portanto, diante da possibilidade de abusos cometidos por essas técnicas, surgiu a preocupação de uma regulação normativa de proteção de dados. Considerando os exemplos apresentados no capítulo três deste trabalho percebe-se que o cenário de proteção de dados mudou de uma preocupação apenas com a privacidade para uma cultura de proteção ao corpo eletrônico de uma pessoa representada no mundo virtual. Percebe-se pelo desenvolvimento de uma cultura de proteção aos dados pessoais criada em solo europeu que se originou pela criação de leis diferentes em países diversos da União Europeia e atingiu o presente ápice pela entrada em vigor da GDRP (*General Data Protection Regulation*).

O Regulamento Geral Europeu de Proteção de Dados exerceu grande influência para que no Brasil existisse uma norma geral relacionada a temática de proteção de dados pessoais. Embora no ordenamento jurídico pátrio existam normas que garantam certa medida de proteção de dados pessoais, estas proteções são setoriais como observa-se as garantias encontradas no CDC, na LAI, no Marco Civil da Internet e na Lei do Cadastro Positivo.

Essas leis trazem dispositivos que são chancelados pela LGPD como por exemplo: a hipótese do livre consentimento esclarecido do titular de dados para que estes sejam coletados ou tratados; o direito ao acesso e à correção de dados

incorretos em bancos de dados; o princípio da finalidade específica para os usos de dados pessoais etc.

No entanto, além da exigência da RGPD que condicionou o fluxo de dados pessoais da EU para países que adotassem legislação de proteção de dados com nível semelhante ao europeu, deve-se considerar que o avanço tecnológico criou situações no cotidiano que ensejaram a urgência de uma lei geral de proteção de dados. Entre essas situações destaque-se o risco algorítmico de discriminações ocasionadas por decisões automatizadas.

Considerando os riscos ora apontados, a LGPD contém em seu texto no art. 20 o direito à explicação e à revisão de decisões automatizadas. Esse direito passou a ser mais bem amparado pela nova lei. Embora busque-se atingir com os algoritmos decisões livre de vieses discriminatórios inerentes ao ser humano, verifica-se que este fim não é conseguido. Isso decorre da possibilidade dos próprios algoritmos de IA cometerem discriminações: seja porque os próprios dados que alimentam esses algoritmos estejam contaminados ou viciados com informações discriminatórias ou em virtude da possibilidade de que o próprio software onde funciona a IA contenha os vieses de seu programador ou seu criador. Como exemplos foram apontados os casos: COMPAS nos Estados Unidos e as situações de *geo princing* e *geo blocking* cometidas pela empresa Decolar.com no Brasil.

Neste último caso, para que problemas relacionados a mal uso de dados pessoais e da geolocalização sejam dirimidos, é interessante que os desenvolvedores de aplicações que utilizam esses dados tornem explícita ao usuário a opção de não fornecer a sua geolocalização. Contudo, se esta informação for necessária para o funcionamento da aplicação ou plataforma virtual, o tratador de dados deverá tornar claro esta condição e informar para o titular de dados quais dados serão utilizados e para que finalidade, incluindo informações sobre sua localização geográfica, com a finalidade de permitir ao usuário decidir se fará uso dessa aplicação.

Entende-se que os seguintes óbices foram encontrados para o pleno exercício do direito à explicação e à revisão de decisões automatizadas: a opacidade algorítmica e o segredo industrial e comercial. Portanto, para que tais barreiras sejam contornadas o último capítulo deste trabalho apresentou o relevante papel que a Agência Nacional de Proteção de Dados (ANPD) deverá desempenhar

no processo de regulação do cenário de proteção de dados por meio das auditorias em algoritmos de IA.

Considerando que esses algoritmos possuem natureza complexa cujo conhecimento para a sua análise é detido por especialistas na área das Ciências da Informação e possivelmente pela organização desenvolvedora desse software, e levando em conta que esses algoritmos estão protegidos pelas normas de proteção comercial ou industrial, a ANPD recebeu função importante para fazer a análise da justiça algorítmica dessas aplicações de IA. Essa atuação é importante para que seja garantido ao titular de dados pessoais uma explicação coerente e válida referente às decisões exclusivamente automatizadas que afetem seus interesses.

No que pese a falta da obrigatoriedade legislativa da revisão de decisão automatizada por pessoa natural, além da possibilidade de atuação da ANPD por meio de processo administrativo como forma de prevenção ou redução de danos ocasionados pelo risco algorítmico, outra abordagem que pode suprir a ausência legislativa supracitada é o desenvolvimento por parte dos tratadores de dados pessoais de uma cultura de prevenção aos riscos causados por algoritmos de IA. Um exemplo de boa prática é o uso de relatórios específicos de impactos causados por esses algoritmos que indiquem os riscos de vieses discriminatórios.

REFERÊNCIAS

ALFIERI, Douglas Guergolette. Internet das Coisas: Aspectos Jurídicos. In: TEIXEIRA, Tarcíso; LOPES, Alan Moreira; TAKADA, Thalles (Coord). **Manual Jurídico da Inovação e das Startups**. Salvador: Editora JusPodivm, 2020.

BARBIERI, Carlos. **Governança de dados: práticas, conceitos e novos caminhos.** 1. ed., Rio de Janeiro: Atlas Books, 2019.

BARBOSA, Mafalda Miranda; NETTO, Felipe Braga; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência Artificial:** diálogos entre Brasil e Europa. Indaiatuba, SP; Editora Foco, 2021.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida.** Tradução de Carlos Alberto Medeiros. 1. ed., Rio de Janeiro: Zahar, 2013. Título Original: Liquid surveillance: a conversation.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed., Rio de Janeiro: Forense, 2020.

BOYLESTAD, Robert L. **Introdução à análise de circuitos**. 10. Ed., São Paulo: Pearson Prentice Hall, 2004.

BORGES, Rafaela. Carro Autônomo: Montadoras e empresas de tecnologia disputam corrida para dispensar o motorista. Disponível em: <https://www.uol.com.br/carros/reportagens-especiais/transporte-do-futuro---carro-autonomo/#cover> Acesso em 29 de junho de 2021

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20/08/2021.

BRASIL, Lei nº 12.965, **Marco Civil da Internet**, Brasília, 23 de abril de 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm > Acesso em 18/08/2021.

BRASIL, Lei nº 13.709, **Lei Geral de Proteção de Dados**, Brasília, 14 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm > Acesso em: 15/07/2021.

CASTELLS, Manuel. **A sociedade em rede.** Tradução de Roneide Venancio Majer.8. ed. Paz e Terra.

CHELIGA, Vinicius; TEIXEIRA, Tarcísio. **Inteligência Artificial: aspectos jurídicos.** 3. ed. rev. e atual, Salvador: Editora JusPodivm, 2021.

COLOMBO, Cristiano; NETO, Eugênio Facchini. Decisões automatizadas em matéria de perfis e riscos algorítmicos. In. MARTINS, Guilherme Magalhães; ROSENVALD, Nelson; (Coord.). **Responsabilidade civil e novas tecnologias**.

Indaiatuba, SP: Editora Foco, 2020.

COLOMBO, Cristiano; GOULART, Guilherme Damásio. Ética algorítmica e proteção de dados pessoais sensíveis: classificação de dados de geolocalização em aplicativos de combate à pandemia e hipóteses de tratamento. In. BARBOSA, Mafalda Miranda; NETTO, Felipe Braga; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência Artificial:** diálogos entre Brasil e Europa. Indaiatuba, SP; Editora Foco, 2021.

CORDEIRO, A. Barreto Menezes. Decisões individuais automatizadas à luz do RGPD e da LGPD. In: BARBOSA, Mafalda Miranda; NETTO, Felipe Braga; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura. **Direito Digital e Inteligência Artificial:** diálogos entre Brasil e Europa. Indaiatuba, SP; Editora Foco, 2021.

COSTA, Alessandra Cristina da. Inteligência Artificial no Empreendedorismo. In: TEIXEIRA, Tarcíso; LOPES, Alan Moreira; TAKADA, Thalles (Coord). **Manual Jurídico da Inovação e das Startups**. Salvador: Editora JusPodivm, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados.** 2. ed., São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In. Coordenadores Danilo Doneda ... [et. al.]. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo; MENDES, Laura Schertel; SOUZA, Carlos Affonso; ANDRADE, Noberto Nunes Gomes de. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Revista Pensar**, Fortaleza, v.23, n.4, 2018.

DUARTE, Fernando. Nove algoritmos que podem estar tomando decisões sobre sua vida – sem você saber. Disponível em: <https://www.bbc.com/portuguese/geral-42908496>. Acesso em: 05/09/2021.

Fórum Econômico Mundial. **Deep Shift – Technology Tipping Points and Societal Impact, Survey Report, Global Agenda Council on the Future of Software Societal Impact**, 2015. Disponível em: <http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf>. Acesso em 24 de junho de 2021.

FORTES, Pedro Rubim Borges. Responsabilidade algorítmica do Estado. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson; (Coord.). **Responsabilidade civil e novas tecnologias**. Indaiatuba, SP: Editora Foco, 2020.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção Pessoais e suas Repercussões no Direito Brasileiro**, 2. ed. São Paulo, Revista dos Tribunais, 2020.

FRAZÃO, Ana. **Proteção de dados e expectativas para 2020**. Disponível em <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/protecao-de-dados-e-expectativas-para-2020-12022020>. Acesso em 16/08/2021.

GÉRON, Aurélien. **Mãos à Obra Aprendizado de Máquina com Scikit-Learn & TensorFlow:** Conceitos, Ferramentas e Técnicas Para a Construção de Sistemas Inteligentes. traduzido por Rafael Contatori. - Rio de Janeiro: Alta Books, 2019.

HAWKING, Stephen. **O universo em uma casca de noz**. Tradução de Cássio de Arantes Leite. Rio de Janeiro: Intrínseca, 2016.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito.** Tradução de Ítalo Fuhrmann. 1. ed., Rio de Janeiro: Forense, 2021.

HOUAISS, Antônio; VILLAR, Mauro d Salles. **Dicionário Houaiss da língua portuguesa**. 1.ed., Rio de Janeiro: Objetiva, 2009.

LIMA, Caio César Carvalho. Objeto, aplicação territorial e aplicação material. In: **Comentários ao GDPR**. Viviane Nóbrega Maldonado; Renato Ópice Blum (Coord). 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

LÓPEZ, Nuria. Um direito, um dever: guia para o art. 20 da LGPD. In: **Proteção de dados: desafios e soluções na adequação à lei**. Alessandra Borelli Vieira ... [et al.]; org. Renato Muller da Silva Opice Blum. 2 ed., Rio de Janeiro: Forense, 2021.

MAGRANI, Eduardo. **A internet das coisas.** Rio de Janeiro: FGV Editora, 2018.

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

MARQUES JÚNIOR, William Paiva. Obstáculos impostos à efetividade do direito personalíssimo à privacidade na Era do Big Data: uma problemática da sociedade contemporânea. In: Larissa Maria de Moraes Leal; Roberto Senise Lisboa. (Org.). **Direito Civil Contemporâneo II.** 01ed.Florianópolis: CONPEDI, 2018, v. 01.

MARTINS, Guilherme Magalhães; ROSENVALD, Nelson; (Coord.). **Responsabilidade civil e novas tecnologias**. Indaiatuba, SP: Editora Foco, 2020.

MCCARTHY, Jonh**. What is Artificial Intelligence?** Disponível em: <http://jmc.stanford.edu/articles/whatisai/whatisai.pdf>. Acesso em 26 de junho de 2021.

MEDON, Filipe. **Inteligência artificial e responsabilidade civil: autonomia, riscos e solidariedade.** 1. ed., Salvador: Editora JusPodivm, 2020.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? In: **Instituto Igarapé**, artigo estratégico 39, 2018.

NORVING, Peter; RUSSELL, Stuart. **Artificial Intelligence A Modern Aproach**. 3 ed. New Jersey: Pearson, 2010.

OLIVEIRA, Marcos Aurélio Belizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In. FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção Pessoais e suas Repercussões no Direito Brasileiro**, 2. ed. São Paulo, Revista dos Tribunais, 2020.

ORWELL, George. **1984**; Tradução de Alexander Hubner, Heloisa Jahn; São Paulo: Companhia das Letras, 2009.

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

PINHEIRO, Patricia Peck. **Direito Digital**. 7. Ed. São Paulo. Saraiva Educação, 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados Pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 3 ed., São Paulo: Saraiva Educação, 2021.

RODOTÀ, Stefano. **A Vida na Sociedade de Vigilância**. A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016.

SCHREIBER, Anderson. **Código civil comentado – doutrina e jurisprudência**. Anderson Schreiber ... [et al.]. – Rio de Janeiro: Forense, 2019.

SOUZA, Carlos Afonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. In: **Tratado de proteção de dados pessoais.** DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz. (coord.), 1. ed., Rio de Janeiro: Forense, 2021

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca**. Lei geral de proteção de dados pessoais: comentada artigo por artigo.** Salvador: Editora JusPodivm, 2019.

TOFFLER, Alvin. **A terceira onda.** 31. Ed. Rio de Janeiro: Record, 2012.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da lei geral de proteção de dados. In: **Tratado de proteção de dados pessoais.** DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz. (coord.), 1. ed., Rio de Janeiro: Forense, 2021

VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: **Comentários ao GDPR: Regulamento geral de proteção de dados da União Europeia.** Viviane Nóbrega Maldonado; Renato Ópice Blum (Coord). 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

VIEIRA, Alessandra Borelli ... [et al.]; org. Renato Muller da Silva Opice Blum. **Proteção de dados: desafios e soluções na adequação à lei**. 2 ed., Rio de Janeiro: Forense, 2021.

WARREN, Samuel; BRANDEIS, Louis. The rigth to privacy. **Harvard Law Review**, v.4, 1890.

WEBER, Rolf; WEBER, Romana. **Internet of Things**. Springer, 2010.