CENTRO UNIVERSITÁRIO AUTÔNOMO DO BRASIL
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITOS FUNDAMENTAIS E DEMOCRACIA – MESTRADO E DOUTORADO

LUCIANA WALY DE PAULO

O DIREITO FUNDAMENTAL À IGUALDADE E A DECISÃO AUTOMATIZADA NAS RELAÇÕES DE CONSUMO

CURITIBA
2023

LUCIANA WALY DE PAULO

O DIREITO FUNDAMENTAL À IGUALDADE E A DECISÃO AUTOMATIZADA NAS RELAÇÕES DE CONSUMO

Dissertação apresentada ao Programa de Pós-graduação *stricto sensu* em Direitos Fundamentais e Democracia, Centro Universitário Autônomo do Brasil, para obtenção do grau de Mestre em Direito.

Orientadora: Prof.ª Dr.ª Rita de Cassia Correa de Vasconcelos

CURITIBA

2023

LUCIANA WALY DE PAULO

O DIREITO FUNDAMENTAL À IGUALDADE E A DECISÃO AUTOMATIZADA NAS RELAÇÕES DE CONSUMO

BANCA EXAMINADORA

_____

Prof.ª Dr.ª Rita de Cássia Corrêa de Vasconcelos

_____

Prof.ª Dr.ª Jussara Maria Leal de Meirelles

_____

Prof. Dr. Marco Antonio Lima Berberi

CURITIBA

2023

Ficha catalográfica elaborada pelo Sistema Universitário de Bibliotecas (UniBrasil),
com os dados fornecidos pelo(a) autor(a)

Paulo, Luciana Waly de

O direito fundamental à igualdade e a decisão automatizada nas relações de consumo. / Luciana Waly de Paulo. -- Curitiba, 2023.

195 f.

Orientador: Profa. Dra. Rita de Cassia Correa Vasconcelos

Dissertação (Mestrado) – UniBrasil, 2023.

AGRADECIMENTOS

Sou muito grata aos meus pais por todo apoio e por estarem ao meu lado nessa caminhada. Agradeço a oportunidade de fazer parte do programa de mestrado da UniBrasil aos professores e, em especial, à professora Rita de Cassia Correa de Vasconcelos e ao professor Marco Antonio Berberi.

RESUMO

O objetivo dessa pesquisa é discutir o regime legal das decisões automatizadas pela perspectiva da Lei n. 13.709/2018 (Lei Geral de Proteção de dados Pessoais) bem como a necessidade de intervenção humana. Por isso, verifica-se se é possível dispensar a intervenção humana nas decisões automatizadas. Além disso, a decisão deve respeitar os direitos fundamentais, como a proteção dos dados pessoais e o princípio da igualdade. Deve-se ter o devido cuidado para não causar discriminações, sejam diretas ou indiretas, a uma pessoa ou a grupos de pessoas. A discussão ocorre sob a perspectiva do direito do consumidor em contratações que envolvam a pontuação de crédito e a contratação de seguros privados. Também se abordam as leis que se aplicam para essas contratações, haja vista que têm como objetivo antever o risco. O direito à igualdade e à não discriminação estão previstos na Constituição da República de 1988 e na Lei Geral de Proteção de Dados Pessoais. Trata-se de uma pesquisa bibliográfica e documental, cuja metodologia é a hipotético-dedutiva. Ao se estudar a evolução do direito à privacidade, o direito fundamental à proteção de dados pessoais e a inteligência artificial, não há uma resposta única para as decisões automatizadas e a sua revisão. Para garantir o direito à privacidade, deve-se aplicar diversas técnicas e legislações, assim como a governança, a auditoria, o devido processo informacional e o direito à explicação. Para que o exercício do direito à revisão das decisões seja garantido, necessita-se da intervenção humana, por meio de um procedimento, ainda na via extrajudicial, haja vista que as leis que tratam sobre esse tema estabelecem diversos direitos a serem observados, como o direito à informação e o de acesso aos dados pessoais, por exemplo. Também se vê o devido processo legal e o direito à explicação. Estudam-se alguns dos mecanismos possíveis de serem utilizados para evitar discriminações.

Palavras-chave: direitos fundamentais; inteligência artificial; decisão automatizada; revisão por pessoa humana.

ABSTRACT

This research aims to discuss, the legal regime of automated decision-making from the perspective of the Brazilian General Data Protection Law (Law n. 13.709/2018) and the necessity of human intervention. The main objective is to discusses the precautions which are necessary and recommended to have before and after the automated decision. And, if it is possible to not have human intervention. The decision must respect Fundamental Rights, as the Fundamental right to the protection of personal data and the right to equality. And also, to prevent discrimination against an individual, group of people who share protected characteristic, or a person, so it can be an indirectly discrimination for belonging as part of the group or as an individual. The discussion will be from the perspective of the consumers mainly about credit scoring and the pricing of private individual insurance contracts. Those types of contracts analysis the risk classification, there are specific laws that regulates these contracts. It is also discussed the prohibition of discrimination is specified in the Brazilian Federal Constitution and discriminations are also prohibit in the Brazilian General Data Protection Law based on the principle of non-discrimination. The methodology used is hypothetical-deductive, based on bibliography and documentary review. After studying the evolution of privacy, the fundamental right of data protection, and the principle of non-discrimination and the artificial intelligence there is not one exclusive answer to the automated decision. It will be necessary to apply different techniques and regulations, as governance, auditing of automated decision, information due process, the right of explanation, the right to review and the necessity of the human intervention. These rights can be applied in the extrajudicial route. Those are some of the applicable mechanisms to avoid discrimination.

KEYWORDS: fundamental rights; artificial intelligence; automated decisions; human intervention.

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados
CEP – Código de Endereçamento Postal
CDC – Código de Defesa do Consumidor
CRFB – Constituição da República Federativa do Brasil
EC – Emenda Constitucional
GDPR – *General Data Protection Regulation*
IA – Inteligência Artificial
LCP – Lei do Cadastro Positivo
LGPD – Lei Geral de Proteção de Dados Pessoais
MCI – Marco Civil da Internet
RGPD – Regulamento Geral Europeu
RIPDP – Relatório de Impacto à Proteção de Dados Pessoais
STF – Supremo Tribunal Federal
STJ – Superior Tribunal de Justiça

SUMÁRIO

INTRODUÇÃO

A inteligência artificial (IA) e as decisões automatizadas estão presentes no cotidiano das pessoas — como os tradutores simultâneos, as recomendações de filmes e de música baseadas em algoritmo, as decisões das redes socais para bloquear conteúdo inadequado — e, por isso, muitas vezes passam desapercebidas. Trata-se, ademais, de uma tecnologia que está se desenvolvendo muito rapidamente e sendo aplicada em diversos setores. Em razão disso, são testadas praticamente em tempo real.

Nesse sentido, discutem-se as decisões automatizadas e a sua revisão sob uma perspectiva constitucional e da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), assim como das legislações especiais, como a Lei n. 8.078/1990 (Código de Defesa do Consumidor – CDC) e a Lei n. 12.414/2011 (Lei do Cadastro Positivo – LCP), com o intuito de se prevenir os titulares de dados de serem afetados por decisões discriminatórias e que não respeitem o direito fundamental à igualdade e à proteção dos dados pessoais.

Para tanto, esta pesquisa, bibliográfica e documental, adota o método hipotético-dedutivo e estrutura-se em três capítulo. No primeiro, adota-se como marco teórico a doutrina de Celso Antônio Bandeira de Mello, uma vez que alguns dos focos desse capítulo são os princípios da igualdade e o da não discriminação. Desse modo, compreendem-se a criação de perfis e as decisões automatizadas como generalizações que têm potencial de causar discriminações não permitidas no ordenamento jurídico brasileiro.

O segundo capítulo, por sua vez, embasa-se na discussão promovida por Bruno Meneses Lorenzetto e Amilcar Cordeiro Teixeira Filho no texto “A inteligência artificial e o direito à explicação”. Assim, defende-se que, embora esteja diante de um problema decorrente da evolução tecnológica, o Direito deve encontrar respostas para solucioná-lo, além de enfrentar a opacidade e o enviesamento das decisões automatizadas, a fim de tutelar os direitos fundamentais. Complementando a argumentação, o capítulo também se fundamenta no livro *Nova lei do cadastro positivo*, de Leonardo Roscoe Bessa,

para tratar da questão do Cadastro Positivo e dos direitos previstos em sua legislação, pois ela traz dispositivos que protegem os dados pessoais.

Já o terceiro capítulo embasa-se no livro *Tratamento de dados pessoais e discriminação algorítmica nos seguros*, de Thiago Junqueira, que engloba os dois grandes temas do presente estudo: o enfrentamento das discriminações e as decisões automatizadas. Além disso, nesse capítulo, investiga-se a doutrina nacional sobre esses temas e alguns aspectos da legislação estrangeira, ou seja, do Regulamento (EU) 2016/679 (Regulamento Geral de Proteção de Dados da União Europeia). Desse modo, verifica-se como é possível garantir que a decisão automatizada esteja adequada e em consonância com os direitos fundamentais. Por fim, ainda se discute a necessidade de intervenção humana na revisão das decisões automatizadas.

Ademais, o estudo desenvolve-se sob a perspectiva das relações de consumo, em aspectos como a pontuação de crédito (*credit scoring*) e a fixação de prêmio de seguros conforme o potencial risco apresentado pelo contratante. De um modo geral, entende-se que a economia é baseada em dados, o chamado *big data*. Nesse contexto, os algoritmos baseiam a tomada de decisões automatizadas. Essas decisões, por sua vez, afetam diretamente os titulares de dados pessoais e, muitas vezes, devido ao enviesamento dos algoritmos e de sua opacidade, não é possível se determinar claramente como foram tomadas. Isso pode ocorrer por diversos fatores: pelo modo de coleta dos dados, pela metodologia estatística aplicada, ou ainda pelo processo de aprendizado da máquina que faz as suas próprias correlações.

No entendimento adotado neste estudo, as relações de consumo partem do pressuposto da vulnerabilidade dos consumidores, que pode ser técnica, fática, jurídica ou informacional. Além disso, o direito do consumidor também está no rol de direitos fundamentais expressos, assim como a igualdade, a proteção dos dados pessoais, o contraditório e o devido processo informacional. Dessa forma, aplica-se, nesse contexto de relações de consumo, o dispositivo constitucional que garante a aplicação imediata dos direitos fundamentais nas atividades privadas, ou seja, a eficácia horizontal desses direitos.

Retornando à explanação da estrutura geral da pesquisa, no primeiro capítulo estuda-se a evolução do direito à privacidade e a necessidade de um direito fundamental autônomo de proteção de dados pessoais, o qual foi incluído na Constituição da República de 1988 pelo artigo 5º, inciso LXXIX, em que se assegura, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Emenda Constitucional n. 115/2022). Nesse capítulo, ainda se discorre sobre as quatro gerações de leis de proteção de dados pessoais e seus respectivos contextos históricos; os direitos fundamentais que têm relação com a proteção de dados pessoais; a diferença entre dados e informações pessoais; e a distinção entre dados pessoais e dados pessoais sensíveis.

Nesse sentido, a proteção dos dados pessoais sensíveis objetiva afastar as discriminações, sejam elas ilícitas, proibidas ou abusivas. A importância desse tema surge quando se aborda o assunto dos bancos de dados e a perfilização (*profiling*), os quais são elaborados a partir de decisões automatizadas. Essas decisões, por seu turno, podem excluir pessoas do acesso a produtos e serviços, assim como criar um ciclo vicioso de discriminação.

No Capítulo 1, aborda-se os princípios da igualdade e da não discriminação, bem como os seus fundamentos na Constituição de 1988 e na Lei Geral de Proteção de Dados Pessoais. Discorre-se ainda sobre a diferença entre discriminação direta e indireta — ambas previstas na CRFB — e sobre como as leis infraconstitucionais, a doutrina e as decisões possibilitam os distintos tratamentos sobre os temas em questão.

Já no Capítulo 2, descreve-se a inteligência artificial e suas espécies. Depois, investiga-se como uma decisão automatizada pode ser tomada e pondera-se sobre a necessidade de utilização, nesse tipo de decisão, de uma enorme quantidade de dados pessoais. Vê-se também os principais conceitos sobre as espécies de IA e o termo algoritmo, e expõem-se quais regulações estão previstas no Brasil sobre a IA.

Nesse mesmo capítulo, no item 2.1, reflete-se a relação entre a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), a Lei n. 8.078/1990 (Código de Defesa do Consumidor – CDC) e a Lei n. 12.414/2011 (Lei do Cadastro Positivo). Discute-se também o conceito de banco de dados

trazido pelo CDC e a sua aplicabilidade nos dias de hoje. Além disso, estuda-se a LCP e o CDC no que diz respeito aos dispositivos aplicáveis às questões que envolvem decisões automatizadas e a revisão delas. Outros aspectos dessas leis são discutidos, como o prazo para a manutenção de dados e informações pessoais e o conceito de perfilização. Por fim, são analisados alguns exemplos práticos em que há discriminação sem haver uma justificativa pertinente.

No capítulo 3, retoma-se como foram aprovados o artigo 20 da LGPD e suas alterações, e discute-se os questionamentos feitos pela doutrina, as possíveis soluções para a decisão automatizada e sua revisão. Nesse capítulo também se reflete sobre a necessidade de intervenção humana na decisão automatizada para a sua revisão. Além disso, abordam-se os direitos previstos nas legislações vigentes (CRFB, LGPD, CDC, LCP) para a tutela do titular dos dados, e para que ele não esteja sujeito a decisões automatizadas discriminatórias e possa entender como elas foram tomadas.

Ademais, reflete-se sobre os principais pontos, dos temas em tela, discutidos pela doutrina e sobre as decisões do judiciário brasileiro para a proteção e a efetivação dos direitos fundamentais. Verifica-se, desse modo, que as garantias mais discutidas são o direito à explicação e o devido processo informacional, assim como os direitos de acesso às informações, de notificação, de retificação, o princípio da transparência, por exemplo.

Ainda no terceiro capítulo, aborda-se o papel da Autoridade Nacional de Proteção de Dados (ANPD) na regulamentação e fiscalização da proteção de dados pessoais. Além disso, discute-se como a governança dos dados pessoais pode contribuir para a qualidade das decisões automatizadas e como os titulares poderão exercer os seus direitos tendo em vista que, para isso, os agentes de tratamentos dos dados devem viabilizar e disponibilizar o conhecimento e as informações necessárias.

Sabe-se que a linguagem utilizada na inteligência artificial é matemática: são fórmulas matemáticas, estatísticas usadas para a tomada da decisão, assim como para a formação dos perfis, que costumam ser chamados de perfilização (*profiling*). A perfilização, por sua vez, trabalha com a categorização de pessoas

e grupos de pessoas, o que pode ser prejudicial, pois pode refletir discriminações históricas e limitadoras do livre desenvolvimento da personalidade.

A decisão automatizada é complexa pois envolve programas de computador, podendo apresentar opacidade e enviesamento, o que dificulta o entendimento de como a decisão foi tomada. Contudo, os problemas que afetam as pessoas são mesmo complexos, e envolvem questões jurídicas, sociais, econômicas, históricas. Por isso, tendo em vista toda a discussão proposta no estudo, conclui-se que deve ser facilitado o exercício da autodeterminação informativa pelos indivíduos e pelos grupos atingidos pela decisão automatizada.

CAPÍTULO I

1 DA PRIVACIDADE AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

A proteção de dados pessoais tem forte relação com a privacidade e com a evolução de seu direito e da sociedade. Por muito tempo, esse direito tinha como objetivo proteger o indivíduo, a vida privada e familiar e, portanto, consistia em uma proteção estática[1]. Esse aspecto da privacidade não deixou de existir, mas a vida tem se tornado cada vez mais complexa e hiperconectada, devido aos dispositivos móveis, o maior acesso à internet e à tecnologia. Nesse contexto, esse direito, além de ter um aspecto negativo, de restrição, de não intromissão, tem um aspecto positivo que possibilita a atuação do titular dos dados no sentido de protegê-los e de resguardar sua privacidade.

As primeiras legislações acerca da proteção de dados pessoais datam da década de 1970 e tinham como objetivo combater a privacidade — tratava-se de uma visão individualista para a proteção dos dados pessoais[2]. Ao longo dos anos, ampliou-se e modificou-se a aplicação dessas legislações, em virtude das mudanças sociais e da necessidade de acompanhar o desenvolvimento das tecnologias, da ampliação do acesso à internet e do aumento da utilização de banco de dados[3].

Para explicar essa evolução, utiliza-se o conceito de gerações de leis de proteção de dados pessoais, proposto por Viktor Mayer-Schönberger[4] para

---

[1] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução: Maria Celina Bodin de Moraes. Rio de Janeiro: Editora Renovar, 2008.

[2] "A Lei de Proteção de Dados do Land alemão de Hesse,1 de 1970, é identificada como o primeiro diploma normativo que trata especificamente dessa matéria, e debates que tiveram lugar na segunda metade da década de 1960 foram extremamente ricos e fundamentais para definir o perfil dessa disciplina que, de acordo com estimativas, hoje está presente de forma concreta em mais de 140 países". DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo GEN, 2020b.

[3] Banco de dados centralizados nos Estados Unidos, *Nacional Data Center,* o que levou a um debate sobre o tema no Congresso daquele país (DONEDA, 2020b).

[4] "A Lei de Proteção de Dados do Land alemão de Hesse,1 de 1970, é identificada como o primeiro diploma normativo que trata especificamente dessa matéria, e debates que tiveram lugar na segunda metade da década de 1960 foram extremamente ricos e fundamentais para definir o

compreender a proteção de dados e a sua evolução histórica que acompanha o desenvolvimento da tecnologia.

A primeira geração de leis de proteção de dados pessoais tinha como objetivo a tutela dos bancos de dados e a utilização deles pelo poder estatal, e não a privacidade das pessoas em si[5]. Além disso, também visava ao processamento eletrônico de dados realizado pelas empresas privadas[6]. Ou seja, objetivava regulamentar o uso da tecnologia pelo poder estatal e o uso dos bancos de dados[7].

A coleta de dados e informações pelos entes estatais direcionava-se ao planejamento e ao funcionamento burocrático governamental. Contudo, a população reagiu contrariamente a essas iniciativas, motivada pelo temor em relação à concentração de poder e ao controle exercido pelo poder estatal. Os Estados usavam bancos únicos, com grandes quantidades de dados (como nos Estados Unidos)[8], o que colocava a população em situação de vulnerabilidade.

Em seguida, a segunda geração de leis de proteção de dados volta-se para a tutela da privacidade e para a proteção de dados pessoais que tinham como característica a liberdade negativa (como na metade da década de 1970 na França)[9]; volta-se também para a eficácia do consentimento do cidadão. Embora a liberdade de escolha do cidadão fosse limitada, ele não aceitava a possibilidade de ser excluído socialmente[10].

Nesse contexto, as pessoas passaram a ter acesso a instrumentos para atuarem em favor de seus direitos em casos de uso indevido de seus dados pessoais[11]. O titular, então, passa a ter a possibilidade e a responsabilidade de

---

perfil dessa disciplina que, de acordo com estimativas, hoje está presente de forma concreta em mais de 140 países" (DONEDA, 2020b, p. 23).

[5] 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, 2020a.

[6] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

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

[8] MENDES, *op. cit*.

[9] DONEDA, *op. cit*.

[10] MENDES, *op. cit*.

[11] DONEDA, *op. cit*.

proteger os seus dados, e desse modo “dá-se ênfase autonomia do indivíduo em controlar o fluxo de suas informações pessoais”[12].

Na década de 1980, surgem as leis de proteção de terceira geração, que consistiam tanto na possibilidade de as pessoas fornecerem ou não os seus dados como em mecanismos para que pudessem exercer o controle sobre eles, isto é, na autodeterminação informativa[13]. Essa geração de leis tem como marco a decisão do Tribunal Constitucional Alemão que reconheceu a autodeterminação informativa, que consiste no exercício do controle dos dados e de suas informações pessoais[14]. Dessa forma:

> Nessa formulação de um direito à autodeterminação informativa, o Tribunal reconheceu uma carga participativa muito maior que a reconhecida pelas interpretações das normas de proteção de dados pessoais em períodos anteriores. A principal diferença em relação à segurança geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e transmissão e não apenas como a opção entre “tudo ou nada[15].

Por fim, a quarta geração de leis de proteção de dados pessoais são as que estão presentes nas legislações atuais e têm como característica a tutela coletiva, por conta de o exercício individual ser árduo, custoso, complexo, o que dificultava a sua proteção[16]. Além disso, houve maior proteção aos dados pessoais sensíveis que não podem ficar à mercê da atuação individual para a verificação das violações de direitos, pois, nesses casos, havia a possibilidade de as pessoas sofrerem discriminações[17].

Mesmo com a necessidade do consentimento do sujeito, que ganha maior protagonismo, como se viu, foi insuficiente. Portanto, fez-se necessária a sua adjetivação, ou seja, a qualificação do consentimento — como se encontra na própria Lei Geral de Proteção de Dados Pessoais (LGPD) — que deve ser livre, informado, inequívoco, específico[18].

---

[12] BIONI, *op. cit*., p. 111.
[13] DONEDA, 2020a.
[14] BIONI, 2020a, p. 111.
[15] MENDES, 2014, p. 41-42.
[16] DONEDA, 2020a.
[17] MENDES, 2014.
[18] BIONI, *op. cit*.

Diante disso, para garantir o direito à privacidade, é necessário, além de instrumentos para o seu exercício, uma maior proteção, visto que existem dificuldades em se saber como são coletados, onde são armazenados e como são utilizados os dados. Nesse sentido:

> Entre as técnicas utilizadas, estas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação, que não era resolvido com medidas que simplesmente reconheciam o direito à autodeterminação informativa; outra, paradoxalmente, é a própria redução do papel da decisão individual de autodeterminação informativa. Isto ocorre porque se parte do pressuposto de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, à qual não pode ser conferida exclusivamente a uma decisão individual[19].

Essas dificuldades para o exercício da autodeterminação informativa ainda continuam a existir e se agravaram atualmente com o aprimoramento da inteligência artificial.

Nessa mesma época foi formulado o *Reporting Act* (FCRA), legislação que trata dos informes de crédito e dados pessoais, em 1970, ou mesmo o *Privacy Act* de 1974.[20] Essas legislações visavam à regulamentação dos relatórios de crédito dos consumidores[21].

Na União Europeia, em 1995, adotou-se a Diretiva 95/46/CE, que trata da proteção das pessoas em relação ao tratamento de dados pessoais e de sua. Posteriormente, foi substituída em 2016 pelo Regulamento Geral de Proteção de Dados, RGPD ou GDPR (*General Data Protection Regulation*)[22].

No caso do Brasil, também se discutiu um sistema integrado de identificação civil, concebido na década de 30 e retomado e desenvolvido no início da década de 70[23]:

> [...] projeto do Registro Nacional de Pessoas Naturais (RENAPE), que previa a criação de um órgão de abrangência nacional que integraria o Registro Civil de Pessoas Naturais e a Identificação Civil, além da criação de uma base de dados. O projeto acabou arquivado em 1978,

[19] DONEDA, 2020, p. 2.
[20] *Ibidem*, p. 26.
[21] MENDES, 2014.
[22] DONEDA, 2020b.
[23] *Ibidem*.

> depois de ter suscitado um debate que deixou registros na imprensa e também de certa forma inspirando um projeto de lei, de autoria do Deputado Faria Lima, que "Cria o Registro Nacional de Banco de Dados e estabelece normas de proteção da intimidade contra o uso indevido de dados arquivados em dispositivos eletrônicos de processamento de dados[24].

Há muito tempo existe a tutela da intimidade e da vida privada no art. 5º, inciso X, da Constituição da República de 1988. Além disso, há também a proteção da privacidade nas comunicações, no inciso XII, que dispõe que

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

A visão do direito à privacidade e do direito de estar só[25] foi influenciada por um estudo de Samuel Warren e Louis Brandeis[26] de 1890. Nessa época, passou-se a utilizar máquinas fotográficas e as publicações das fotos eram feitas em jornais. Desse modo, criticou-se sobre o uso dessa tecnologia, já que violaria da privacidade das pessoas. Discute-se esse artigo e às primeiras leis de proteção de dados que surgiram são por terem como objetivo a proteção de pessoas de uma determinada camada social e por enfatizarem uma visão individualista[27]. Essa abordagem, nesse sentido, tem uma relação mais próxima com o direito à propriedade[28].

Ademais, houve no Brasil, em 2000, a discussão do Projeto Lei n. 3.360/2000, que continha seis artigos. Esse projeto tratava da privacidade de dados e da relação entre usuários, provedores e portais em redes eletrônicas[29].

---

[24] *Ibidem*, p. 30.
[25] "Mesmo um ponto de partida corriqueiro, que é a menção a um 'direito a ser deixado só', tantas vezes apontado como sendo a definição de Warren e Brandeis, não é de todo exato: em seu mencionado artigo, os autores em nenhum momento definem estritamente o *right to privacy.* A associação que geralmente é feita do artigo com o *right to be let alone* deve ser relativizada: essa é uma citação da obra do magistrado norte-americano Thomas Cooley, que os autores não chegam a afirmar que traduziria propriamente o conteúdo do direito à privacidade — ou seja, Warren e Brandeis não chegaram a trabalhar com uma perspectiva fechada de *privacy*" (DONEDA, 2020b, p. 7).
[26] DONEDA, 2020b.
[27] RODOTÀ, 2008.
[28] *Ibidem*.
[29] BRASIL. **Projeto de lei n. 3.360, de junho de 2000**. Dispõe sobre a privacidade de dados e a relação entre usuários, provedores e portais em redes eletrônicas. Brasília, DF: Câmara dos Deputados, [2000]. Disponível em:

A privacidade está protegida também como um direito da personalidade no art. 21 do Código Civil de 2002, que assegura que a vida privada da pessoa natural é inviolável. Além disso, assegura que o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a essa norma. Atualmente, a legislação civilista ainda descreve a privacidade com uma concepção individualista[30].

Os perfis criados a partir dos dados disponibilizados ou acessados projetam, de alguma maneira, uma espécie de identidade virtual da pessoa, que nem sempre será acurada. Decorre daí a preocupação com a proteção dos direitos da personalidade, pois:

> Personalidade significa as "características ou o conjunto de características que distingue uma pessoa" da outra. Com base nessa abordagem semântica, os direitos da personalidade seriam os caracteres incorpóreos e corpóreos que conformam a projeção da pessoa humana. Nome, honra, integridade física e psíquica seriam apenas alguns dentre uma série de outros atributos que dão forma a esse prolongamento[31].

Diante disso, nota-se que a proteção dos dados pessoais também tem como objetivo proteger os direitos à personalidade, à privacidade[32], ao livre desenvolvimento da personalidade, assim como à autodeterminação informativa[33].

Reconhece-se um aspecto negativo da privacidade, que é deixar o indivíduo em paz, só; ao mesmo tempo, identifica-se também um aspecto positivo, vinculado a uma maior proteção, que é o controle dos dados pessoais, feito pelo indivíduo que deve decidir como e onde os seus dados poderão ser

---

http://imagem.camara.gov.br/Imagem/d/pdf/DCD30JUN2000.pdf#page=159. Acesso em: 30 jan. 2023.

[30] DONEDA, *op. cit*.

[31] BIONI, 2020a, p. 55.

[32] *Ibidem*.

[33] SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 81-106, 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 9 fev. 2023.

utilizados e circularão[34]. Em suma, a evolução do direito à privacidade pode ser destacada da seguinte maneira:

> Seriam, assim, três as concepções sobre o direito à privacidade acima apresentadas, quais sejam, (i) o direito de ser deixado só, (ii) o direito de ter controle sobre a circulação dos dados pessoais, e (iii) o direito à liberdade das escolhas pessoais de caráter existencial[35].

Com o intuito de refinar a discussão, cumpre esclarecer que o termo "dado" refere-se a atos ou sinais que demandam interpretação, pois antecedem a uma informação, a qual pode ser expressa de diversas maneiras, como graficamente, de forma fotográfica ou sonora[36].

O dado pessoal, por sua vez, "[...] são os fatos, comunicações e ações que se referem a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável"[37]. A informação pessoal, então, revela aspectos que dizem respeito à pessoa e contém atributos de sua personalidade[38]. Além disso, quando o dado estiver anonimizado, em princípio, não será possível determinar o seu titular. Por esse motivo, podem ser utilizados para estatísticas — como é utilizado pela inteligência artificial.

Nesse sentido, a proteção de dados pessoais engloba diversos direitos fundamentais, e não se baseia mais em uma visão individualista, patrimonialista, pois:

> [...] proteção de dados pessoais é, em síntese, a proteção da pessoa humana, mormente quanto ao resguardo do livre desenvolvimento de sua personalidade e, em particular, por meio da centralidade da garantia da sua autodeterminação informacional consoante o artigo 1º da LGPD[39].

Desse modo, a privacidade consiste em um "[...] aspecto mais amplo que a intimidade, que é um conjunto das facetas da vida de uma pessoa,

---

[34] MENDES, 2014.
[35] MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. p. 173.
[36] MENDES, 2014.
[37] *Ibidem*, p. 55-56.
[38] *Ibidem*.
[39] SARLET; RUARO, 2021, p. 85.

possibilitando que se tenha um retrato de sua vida íntima e sua personalidade pessoal, familiar e social”[40].

A proteção de dados pessoais, como ensina Stefano Rodotà, tem dupla função: uma de impedir a interferência na esfera individual, e outra de controlar o fluxo desses dados e de determinar de que maneira é possível construir a esfera particular[41]. Por conseguinte, aquela visão individualista, que se reduz a um direito à privacidade, tem sido ampliada e transformada, pois, com a proteção de dados, oferecem-se mecanismos de controle pelo titular desses, assim como propicia-se que órgãos independentes, como a Autoridade de Proteção de Dados Pessoais, possam atuar na fiscalização da garantia desse direito. Deve-se levar em consideração que é impossível que o indivíduo faça sozinho essa fiscalização. Além disso, as violações a essa proteção atingem grupos de pessoas, podendo ser mais danosas ainda quando atingem grupos de pessoas que já estão em situação de vulnerabilidade.

Quando se fala em proteção de dados pessoais, a primeira preocupação que surge diz respeito à privacidade, aqui utilizada como termo amplo para abranger a intimidade, a vida privada, a imagem. Essa proteção, nesse sentido, abrange os demais direitos fundamentais e os direitos da personalidade. A Constituição da República de 1988 distingue vida privada de intimidade no art. 5º, inciso X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Contudo, parte da doutrina sustenta que não há necessidade dessa distinção. Nota-se uma tendência dos autores que estudam a LGPD em utilizar o termo “privacidade” para abranger as diversas expressões desse direito. Diante disso, parece interessante verificar se essa distinção é realmente pertinente. Essa diferenciação tem como base a teoria de círculos concêntricos

---

[40] CAMURÇA, Lia Carolina Vasconcelos; MATIAS, João Luís Nogueira. Direito à privacidade e à proteção de dados pessoais: análise das práticas obscuras de direcionamento de publicidade consoante a lei nº 13.709 de 14 de agosto de 2018. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 6-23, 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1590. Acesso em: 12 ago. 2022. p. 09.

[41] RODOTÀ, 2008.

formulada pela doutrina alemã, a qual contribui para a superação da clássica distinção entre público e privado, bem como para a superação do paradigma proprietário-econômico[42]. Nesse sentido, Luiz Fernando Moncau elucida o seguinte:

> Apesar disso, ainda hoje a teoria das esferas é reconhecida uma ferramenta útil para determinar os níveis de gravidade de uma violação a privacidade, por oferecer um parâmetro, ainda que pouco preciso, para determinar em que a personalidade de um indivíduo é afetada por intrusões ou pela divulgação de aspectos da vida privada[43].

Desse modo, para a teoria das esferas, há distinção entre os conceitos de segredo, intimidade e vida privada no que diz respeito à delimitação dos aspectos da vida de uma pessoa entre o espaço público e o privado[44].

Entretanto, Danilo Doneda[45] sustenta que não há por que diferenciar os dois termos trazidos pela Constituição da República de 1988. Primeiro, pois na CRFB foi a primeira vez que surgiu essa distinção pelo legislador brasileiro, e nem mesmo a doutrina e a jurisprudência brasileira faziam essa distinção. O segundo argumento é de que haveria muita subjetividade na distinção dos dois termos e, por isso, ela não contribuiria para a proteção do direito fundamental em si[46]. Nesse sentido, utiliza-se neste estudo o termo “privacidade”, mas reconhece-se que essa distinção pode ser útil na análise de casos concretos.

Ademais, a relevância da proteção dos dados pessoais como um direito fundamental decorre de que é possível, a partir dos dados pessoais, identificar uma pessoa. Esses dados levam a uma representação do que seria a pessoa na sociedade[47] e, por isso, podem afetá-la ou até mesmo atingir grupos de pessoas, de maneira direta ou indireta, sem que elas saibam.

---

[42] MONCAU, Luiz Fernando. **Direito ao esquecimento**: entre a liberdade de expressão, a privacidade e a proteção de dados pessoais. São Paulo: Thomson Reuters Brasil, 2020.
[43] *Ibidem*, p. 123.
[44] BIONI, 2020a.
[45] DONEDA, 2020a.
[46] *Ibidem*.
[47] MENDES, Laura Schertel. *Habeas data* e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, [*s. l.*], v. 12, n. 39, p. 185-216, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 4 maio 2022.

A privacidade tem um aspecto negativo e outro positivo. O primeiro visa à proteção do indivíduo para que não se invada essa esfera de proteção. O aspecto positivo é promocional para que a pessoa possa desenvolver-se livremente e, nessa concepção, há também um aspecto coletivo. Desse modo, elucida-se claramente:

> Nessa perspectiva, e avaliando a trajetória da matéria nas últimas décadas, revelam-se uma série de interesses a ela relacionados, não somente atinentes à reserva e ao isolamento, porém também à construção de uma esfera pessoal na qual seja possível a liberdade de escolha e, consequentemente, o desenvolvimento da personalidade[48].

A visão de que a privacidade tem uma feição relacional significa que "[...] deve determinar o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior — pela qual a pessoa determina sua inserção e de exposição"[49].

Rodotà identifica que opiniões políticas ou sindicais estão protegidas pela privacidade e fazem parte esfera pública, isto é, da identidade pública da pessoa, e não devem ser utilizadas de maneira que causem discriminações[50]. Por isso, a circulação dessas informações tem especial proteção — pelo direito à privacidade[51]. É o que autor denomina de paradoxo, de acordo com o qual essas informações devem ter maior proteção em virtude de causarem discriminações[52].

A EC n. 115/2022 ampliou os direitos fundamentais previstos no artigo 5º da CRFB e incluiu o inciso LXXIX, em que assegura "[...] nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Isso se coaduna com o fato de os dados pessoais serem tratados tanto no âmbito interno como no internacional. Embora a Lei Geral de Proteção de Dados pessoais ampare os titulares nos meios digitais, faz-se necessário uma proteção efetiva.

---

[48] *Ibidem*, p. 10.
[49] MENDES, 2019, p. 10.
[50] RODOTÀ, 2008.
[51] *Ibidem*.
[52] *Ibidem*.

Ingo Sarlet[53] considera a proteção de dados pessoais um direito humano fundamental com base na releitura dos direitos fundamentais clássicos e do direito constitucional multinível, haja vista que muitos desses dados e informações são compartilhados em âmbito internacional. Além disso:

> Seja como for, é objeto de elevado consenso que o direito à proteção de dados pessoais é, simultaneamente, um direito humano e um direito fundamental, o que, calha enfatizar, não afasta situações de tensão e conflitos normativos, de diversa natureza[54].

Faz sentido esse entendimento, ainda mais quando se tem em conta que, na maioria das situações, as tecnologias de tratamento de dados pessoais são produzidas fora do Brasil, há também muitas vezes a transferência e o compartilhamento desses dados. Nessa esteira, Dominika Iwan[55] entende que os direitos humanos são indicados para contribuir para as decisões automatizadas em âmbito internacional, por terem como características a universalidade e a indivisibilidade, e por serem aplicáveis a todos — pois a tecnologia atinge as pessoas em âmbito internacional, isto é, não há mais fronteiras[56].

Vinícius Sampaio[57], por sua vez, fundamentando-se nos art. 22 e 42 da LGPD[58], defende que a proteção de dados pessoais se trata de um direito, pois esse entendimento possibilita a defesa dos interesses e dos direitos dos titulares de dados via judicial de maneira individual ou coletiva, de acordo com a legislação pertinente, e com os instrumentos de tutela individual e coletiva.

---

[53] SARLET, Ingo W. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: BIONI, Bruno *et al.* (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo GEN, 2020.

[54] *Ibidem*, p. 44.

[55] IWAN, Dominika. Applicability of human rights control mechanisms in algorithmic decision-making cases. **Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 269-291, 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2286. Acesso em: 11 fev. 2023.

[56] IWAN, 2021.

[57] SAMPAIO, Vinícius. **Proteção de dados pessoais**: da privacidade ao interesse coletivo. Rio de Janeiro: Lumen Juris, 2020.

[58] LGPD, Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva. E, Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Nessa linha, a defesa desse direito pode ser exercida coletivamente: "[...] se os problemas relacionados ao tratamento de dados pessoais são eminentemente coletivos, talvez seja oportuno que assim também se reconheça o direito à sua proteção, como um interesse aprioristicamente"[59]. Esse posicionamento parece interessante, haja vista que as decisões automatizadas são tomadas a partir de perfis (*profiling*) criados com dados de diversas pessoas, os quais encapsulam e relacionam determinadas caraterísticas a grupos de pessoas.

Bruno Bioni[60], por sua vez, defende a proteção de dados pessoais como um novo direito da personalidade. Dessa maneira seria possível abarcar toda atividade de processamento de dados, ainda que não seja pessoal, mas que afete a vida de uma pessoa de alguma maneira. Bioni argumenta o seguinte:

> O direito à proteção de dados pessoais deve ser alocado como uma nova espécie do rol aberto de direitos da personalidade, dando elasticidade à cláusula geral da tutela humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana[61].

O próprio artigo 5º, parágrafos 2º e 3º, da CRFB permite a abertura do rol de direitos fundamentais com fundamento nos tratados internacionais, que pode decorrer também do regime e dos princípios por ela adotados. Além disso, cabe destacar que os direitos fundamentais têm aplicação imediata e abrangem as relações privadas (eficácia horizontal dos direitos fundamentais), como será visto ao longo deste estudo.

Antes de a proteção de dados pessoais ser reconhecida expressamente como um direito fundamental, muito se discutiu se ele seria implícito ou não. Anísio Gavião Filho e Luiz Fernando de Freitas[62] defendem que há uma abertura

---

[59] SAMPAIO, *op. cit*., p. 90.
[60] BIONI, 2020a.
[61] BIONI, 2020a.
[62] GAVIÃO FILHO, Anizio Pires; FREITAS, Luiz Fernando Calil de. Direitos fundamentais estatuídos não diretamente ou implícitos? **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 25, n. 3, p. 232–257, 2020. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1630. Acesso em: 12 ago. 2022.

material do catálogo de direitos fundamentais permitida pela própria Constituição e pelos tratados internacionais. Nesse sentido, quanto maior for a indeterminação da linguagem do texto constitucional, maiores serão as possibilidades de serem formulados direitos fundamentais[63].

Sarlet[64], por outro lado, assevera que deve ser vista com certa reserva a afirmação de que todo direito fundamental decorre da dignidade da pessoa humana, haja vista que a dignidade da pessoa humana, como princípio fundamental, constitui um valor-guia para os direitos fundamentais, bem como para a ordem constitucional[65].

Ademais, reconhece-se que a inteligência artificial repercute no Direito e faz com que o sistema jurídico tenha que adaptar os seus institutos processuais e principiológicos à nova realidade instituída por ela:

> Além disso, deve-se grifar a ressignificação de princípios como o da dignidade da pessoa humana e o da separação de poderes, que ganham em sentido na sociedade informacional, bem como as garantias do devido processo, da ampla defesa e do contraditório que devem ser alvo de uma releitura à luz do constitucionalismo digital. Destaca-se, nesse contexto, a necessidade de assegurar um devido processo informacional e a assim chamada separação informacional de poderes[66].

Um dos aspectos da proteção de dados pessoais é, de fato, a proteção da privacidade (intimidade, vida privada) da pessoa, contudo, há ainda outros que são abarcados pela Lei Geral de Proteção de Dados Pessoais, como a não-discriminação, a autodeterminação informativa, o direito à informação, o livre desenvolvimento da personalidade. Esses aspectos serão tratados ao longo deste estudo, porém neste primeiro capítulo o foco recai sobre o direito fundamental à proteção de dados pessoais e o princípio da igualdade.

A privacidade, como visto, evoluiu a partir de uma liberdade de proteção negativa, protegendo o indivíduo e a sua família, para então também ter um

---

[63] *Ibidem*.
[64] SARLET, Ingo W. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. rev. atual. Porto Alegre: Livraria do Advogado, 2018.
[65] *Ibidem*.
[66] SARLET, Ingo W. *et al.* **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital**. São Paulo: Saraiva, 2022. p. 11.

aspecto positivo em que a pessoa pode controlar o compartilhamento de seus dados e das suas informações. Contudo, como se verá no próximo capítulo, ao se criar perfis nos ambientes digitais, as decisões podem ser tomadas com base em informações que têm como objetivo antever potenciais riscos. Por isso, as decisões automatizadas têm potencialidade discriminatória e podem atingir determinados grupos de pessoas. Em função disso, a proteção de dados também tem uma dimensão coletiva[67]. Nesse sentido, houve uma redefinição da privacidade, como explica Rodotà:

> Partindo dessa constatação, pode-se dizer que hoje a sequência quantitativa mais relevante é "pessoa-informação-circulação-controle", e não mais apenas "pessoa-informação-sigilo", em torno da qual foi construída a noção clássica de privacidade. O titular do direito à privacidade pode exigir formas de "circulação controlada", em não somente interromper o fluxo das informações que lhe digam respeito[68].

O objetivo deste estudo não é aprofundar as discussões teóricas sobre a privacidade e o direito fundamental da proteção de dados, mas apontar a sua complexidade e refletir sobre a sua transformação diante do desenvolvimento das tecnologias, o que envolve o estudo das decisões automatizadas e do risco de discriminações indevidas.

No contexto das tecnologias digitais, a proteção de dados pessoais não tem como objetivo a proteção do dado em si, mas do seu titular, haja vista que as decisões automatizadas impactam a sua personalidade, a sua liberdade e o seu livre desenvolvimento[69].

A complexidade do direito fundamental à proteção de dados pessoais pode ser compreendida como multidimensional, por harmonizar diversos interesses e direitos, assim como possibilitar a participação do titular nos processos de coleta e tratamento de seus dados[70]. Há uma dupla proteção da pessoa: uma diz respeito à dignidade da pessoa humana, outra à das liberdades[71].

---

[67] RODOTÀ, 2008.
[68] *Ibidem*, p. 93.
[69] MENDES, 2014.
[70] *Ibidem*.
[71] *Ibidem*.

A dignidade da pessoa humana compreende a integridade física e corporal, mas também apresenta uma dimensão para garantir as condições justas e adequadas de vida de um ser humano[72]. Nesse aspecto, protege a pessoa quanto à ordem material e aos direitos sociais[73]. Logo, para que haja respeito à dignidade da pessoa humana:

> O que se percebe, em última análise, é que onde não houver respeito pela vida e pela integridade física do ser humano, em que as condições mínimas para uma existência digna não forem asseguradas, em que a intimidade do indivíduo forem objeto de ingerências indevidas, onde sua igualdade relativamente aos demais não for garantida, bem como onde não houver limitação do poder, não haverá espaço para a dignidade da pessoa humana, e esta não passará de mero objeto de arbítrio e injustiças[74].

Além disso, para Mendes[75] esse direito tem dupla dimensão, uma subjetiva e outra objetiva. A dimensão subjetiva contribui para que o sujeito possa controlar a circulação dos seus dados[76]:

> Assim, percebe-se que a regra é a autodeterminação do titular sobre os dados pessoais, salvo direitos de terceiros ou interesse público predominante, previsto em legislação. Isso enseja a necessidade de autorização legal ou consentimento do titular de dados para que a coleta, o processamento, a utilização ou a circulação de dados pessoais seja considerada legítima[77].

A dimensão objetiva, por sua vez, corresponde à proteção desse direito assegurada pelo poder estatal por meio de legislações e de meios processuais, no âmbito jurídico ou administrativo, que possibilita ao indivíduo a defesa desse direito[78].

Convém lembrar que a proteção do consumidor está entre os direitos fundamentais (CRFB, art. 5º, inciso XXXII). Dessa forma, competirá ao Estado promover, na forma da lei, a defesa do consumidor. Apesar disso, já existia a

---

[72] SARLET, 2018.
[73] *Ibidem*.
[74] *Ibidem*, p. 105-106.
[75] MENDES, *op. cit*.
[76] *Ibidem*.
[77] MENDES, 2014, p. 176.
[78] *Ibidem*.

proteção ao consumidor em relação a seus dados no art. 43, Lei n. 9.099/1990 — esse assunto será abordado com mais profundidade no Capítulo 2.

O direito fundamental do consumidor foi reconhecido pela Organização das Nações Unidas (ONU), pela Comissão de Direitos Humanos, em 1973[79]. E, em 1985, a Assembleia Geral da ONU editou a Resolução n. 39/248, na qual se estabeleceram normas internacionais de proteção ao consumidor e se ressaltou que os governos deveriam implantar políticas voltadas para a defesa do consumidor[80].

O direito do consumidor tem como objetivo disciplinar a ordem econômica. Essa necessidade surge devido às mudanças socioeconômicas nos mercados de produção, distribuição e de consumo, por conta da massificação e da despersonalização das contratações[81]. Essa proteção objetiva que o consumidor possa exercer o direito de acesso e de retificação dos seus dados pessoais[82]. Além disso, existe também a garantia do *habeas data*: trata-se de um remédio constitucional que também assegura o acesso aos dados pessoais e a retificação deles[83].

De modo geral, entende-se que o consumidor está em uma situação de vulnerabilidade, seja em razão do poder econômico ou por questões técnicas, e isso se agrava com a utilização de inteligência artificial:

> Nesse contexto, é fundamental levar-se em conta a vulnerabilidade do consumidor, tanto técnica, por possuir menos informações que o fornecedor a respeito do fluxo de seus dados, como fática, por possuir menos recursos intelectuais e econômicos para a reparação de prejuízos advindos do tratamento de dados[84].

---

[79] SCHWARTZ, Fabio. **Manual do direito do consumidor**: tópicos e controvérsias. 2. ed. Rio de Janeiro: Editora Processo, 2020.
[80] *Ibidem*.
[81] MENDES, *op. cit*.
[82] DRUMMONT, Victor. *Internet, privacidade e dados pessoais*. Rio de Janeiro: Lumen Juris, 2003.
[83] *Ibidem*.
[84] MENDES, 2014, p. 199.

Além disso, o consumidor também é vulnerável juridicamente, haja vista sua falta de conhecimento dos seus direitos e deveres inerentes à relação de consumo[85], em suma:

> [...] das condições e efeitos jurídicos da incidência da legislação e do próprio conteúdo do contrato de consumo que venha a celebrar. A doutrina considera, em paralelo, uma vulnerabilidade científica, para abranger também a ausência de conhecimentos em economia ou contabilidade pelo consumidor, e sua consequente incapacidade de compreensão das consequências da contratação sobre seu patrimônio[86].

Ademais, a vulnerabilidade fática[87] é ampla e diz respeito a situações concretas em que há interferência do poder econômico, assim como a "[..] situações concretas de reconhecimento da debilidade do consumidor a partir de qualidades subjetivas que denotem sua subordinação estrutural em relação ao fornecedor"[88].

Há uma outra categoria de vulnerabilidade, denominada de informacional. Ela está presente com mais vigor na contemporaneidade, principalmente na definição de perfis, com a presença de inteligência artificial[89]:

> As novas tecnologias da informação e o desenvolvimento da internet, com sua incorporação a produtos e serviços, dão causa a uma profunda transformação do mercado de consumo. Introduz, com isso, realidade nova para reconhecimento da vulnerabilidade do consumidor no mercado[90].

Nesse caso, na sociedade da informação, se está diante de uma assimetria informacional no momento da contratação de um serviço ou produto[91]. Portanto, a análise de qual categoria de vulnerabilidade é aplicável será feita no caso concreto[92].

---

[85] MIRAGEM, Bruno. Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo. *In*: MARQUES, Claudia L.; MIRAGEM, Bruno; MAGALHÃES, Lucia Ancona Lopez de (org.). **Direito do consumidor** – 30 anos de CDC. São Paulo: Grupo GEN, 2020.
[86] *Ibidem*, p. 246.
[87].*Ibidem*.
[88] *Ibidem*, p. 247.
[89] *Ibidem*.
[90] *Ibidem*, p. 248.
[91] MIRAGEM, 2020.
[92] *Ibidem*.

Além disso, deve-se mencionar que, entre os princípios da ordem econômica, estão a soberania nacional; a propriedade privada; a função social da propriedade; a livre concorrência; e a defesa do consumidor (CRFB, art. 170); tendo também como finalidade assegurar a todos a existência digna, conforme os ditames da justiça social.

Outra legislação que trata do tema da proteção de dados pessoais é o Marco Civil da Internet, Lei n. 12.965/2014, art. 3º, inciso III, sendo um dos seus princípios justamente a proteção de dados pessoais. Há outras legislações que tratam do assunto proteção de dados pessoais no Brasil que podem ser encontradas na Constituição da República de 1988, art. 5º, como a ação de *habeas data*, regulamentada pela Lei n. 9.507/1997. A Lei n. 12.527/2011 (Lei de Acesso à Informação) explana sobre o que se considera informação pessoal:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem [...]

A referida lei regulamenta o direito à informação previsto no art. 5º, inciso XXXIII, pois garante o direito de se receber dos órgãos públicos informações que digam respeito ao interesse particular de uma pessoa, ou ao interesse coletivo ou geral. Essas informações devem ser prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

No geral, esses são alguns dos aspectos relevantes quanto à evolução da privacidade e da proteção de dados pessoais. Esses dados, por sua vez, devem ser protegidos no contexto de utilização da inteligência artificial, pois a tecnologia pode afetar diversos direitos fundamentais ao mesmo tempo.

1.1 DADOS PESSOAIS E A INTELIGÊNCIA ARTIFICIAL

Há tempos a tecnologia está se espraiando por diversas áreas. Nesse sentido, surgiram as leis de proteção de dados pessoais, haja vista que a utilização deles pela administração pública de diversos países se tornou uma

preocupação de todos em virtude da concentração de poder decorrente das informações extraídas da vida dos seus cidadãos.

No setor financeiro, mais especificamente, os dados são utilizados para prever e minimizar riscos. O mesmo ocorre como no setor securitário, por exemplo, na contratação de planos de saúde. É evidente a utilidade dos dados, contudo, não se pode ter apenas uma visão utilitarista sobre a vida e sobre as pessoas, como se elas fossem apenas dados, objetos e potenciais consumidores ou clientes.

Shoshana Zuboff[93] explica que, na era do capitalismo de vigilância, o comportamento das pessoas é considerado um superávit comportamental. Nesse contexto, as informações sobre a vida das pessoas são extraídas pelos próprios usuários de redes sociais e aplicativos (*likes*, *emoticons*, listas). Então essas pessoas são impactadas pelo tratamento desses dados e não dispõem de recursos para defenderem-se — e na maioria das vezes nem saberão como fazer isso.

Por isso, Zuboff afirma que não há nada de neutro nessa situação, pois para se atingir os interesses da economia capitalista, faz-se necessário escalar as vendas de um produto ou serviço, atrair as pessoas. Para isso, as empresas extraem informações dos seus potenciais consumidores com o intuito de produzir produtos e serviços e, posteriormente, ofertá-los a eles[94].

A informação, por seu turno, é o resultado obtido do estado primitivo dos dados[95]. O objetivo da coleta de dados é coletar informações sobre o sujeito e, consequentemente, antever e evitar eventuais riscos em uma contratação, uma vez que a "[...] informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza"[96].

De acordo com Mendes[97], a legislação excepciona os dados anonimizados, ou seja, que se refiram a pessoas indeterminadas. Esses não estarão sujeitos à proteção de dados pessoais, pois a partir deles seria

---

[93] ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. London: Profile Books, 2019.
[94] *Ibidem*.
[95] BIONI, 2020a, p. 31.
[96] DONEDA, 2020a.
[97] MENDES, 2014.

impossível a identificação de uma pessoa. Apesar disso, deve-se ter cautela com essa afirmação, pois há meios de reverter a anonimização e se ter acesso aos dados por intermédio da tecnologia[98]. É nesse sentido que a LGPD considera que a pessoa deve ser identificada ou identificável para ter seus dados protegidos.

Os dados pessoais são divididos em dados pessoais e dados pessoais sensíveis. A ANPD contribui com a seguinte conceituação:

> O conceito de dado pessoal é amplo, sendo definido, no art. 5º, I, da LGPD, como a informação relacionada à pessoa natural identificada ou identificável. Assim, um dado é considerado pessoal quando permite a identificação, direta ou indireta, de uma pessoa natural[99].

A LGPD, por seu turno, faz a seguinte distinção entre os dados pessoais no art. 5º:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Para a maioria da doutrina, o rol de dados pessoais sensíveis é exemplificativo, pois seria impossível a listagem de todos eles. O gênero de uma pessoa, por exemplo, não consta no rol da LGPD como dado pessoal sensível, mas concretamente pode ser um dado sensível. Por isso, o conceito de dado sensível deve ser funcionalizado de acordo com a sua utilização, ou seja, deve ser considerado dentro do contexto em que se aplica:

> Daí poder se concluir que o conceito de dados sensíveis deve ser funcionalizado de acordo com o tratamento que é concedido a eles. Significa sustentar que dados sensíveis são qualificados como tais não só por conta de sua natureza intrinsecamente personalíssima, de forma apriorística, mas devido ao uso e finalidade que é concedido a esse

---

[98] *Ibidem*.

[99] ANPD. **Guia orientativo**: aplicação da lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral. Brasília, DF: Tribunal Superior Eleitoral, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf. Acesso em: 07 fev. 2023. p. 09.

> dado por meio de um tratamento que pode gerar uma potencialidade discriminatória abusiva[100].

Dessa maneira, nota-se que há dados, como gênero e idade, que têm um peso grande seja na prestação de serviços, como plano de saúde e seguros, seja no mercado de trabalho — por exemplo, em determinadas áreas, quanto mais elevada a idade de uma pessoa, menor sua chance de ser contratada. Por isso, esses dados deveriam ser considerados como sensíveis[101] na prática. Porém, se *a priori* os dados não forem considerados sensíveis, não há a necessidade de o controlador dispensar cuidados mais rigorosos sobre eles[102].

Os abusos no tratamento de dados sensíveis é um problema que atinge o princípio da igualdade quando a utilização deles for potencialmente discriminatória[103]. Por conseguinte, a análise se o dado é sensível ou não deve ser feita de maneira dinâmica[104].

Os dados pessoais sensíveis, portanto, exigem um cuidado maior no tratamento e no armazenamento, já que podem levar a discriminações. Não obstante isso, o art. 11, §1º da LGPD determina que: “Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica”. Junqueira[105] afirma que esse parágrafo do art. 11 oferece respaldo para defender que o rol de dados sensíveis não é taxativo. Por

---

[100] MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). **PUC-Rio**, [*s. l.*], jul. 2021. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 26 set. 2022. p. 03.

[101] Outro exemplo: “Questão desafiadora é a referente à provável criação, pela IA, de novas formas de discriminação que não se relacionam com categorias tradicionalmente protegidas. Tenha-se em mente o exemplo real do uso do provedor de e-mail por alguns seguradores, no Reino Unido, para a precificação do seguro”. JUNQUEIRA, Thiago. Tomada de decisões automatizadas nos seguros privados: tratamento de dados pessoais e prevenção da discriminação racial à luz da LGPD. *In*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O direito civil na era da inteligência artificial**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 14.

[102] *Ibidem*.

[103] MENDES, 2014.

[104] JUNQUEIRA, Thiago. **Tratamento de dados pessoais e discriminação algorítmica nos seguros**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020b.

[105] JUNQUEIRA, 2020a.

conseguinte, a definição de dados sensíveis previamente deve ocorrer tendo em vista um rol exemplificativo:

> Diante da nova realidade dos “perfis”, essas distinções perdem significado: seja porque dados pessoais, aparentemente não “sensíveis, podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas[106].

Diante do exposto, a definição de dado pessoal sensível não é estabelecida em abstrato, mas diante do caso concreto[107]. Deve-se levar em consideração em qual contexto esse dado será utilizado e a relação que se estabelecerá com as demais informações disponíveis pelo agente de tratamento[108], haja vista que a “[...] potencialidade que seu tratamento possa servir como instrumento de estigmatização ou discriminação, à luz da privacidade, identidade pessoal e, de modo geral, da dignidade da pessoa humana”[109]. O art. 9º da RGPD proíbe o tratamento nas seguintes hipóteses:

> É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Esse artigo da GDPR também apresenta exceções[110] quanto ao tratamento desses dados. Desse modo, trata-se de uma legislação mais detalhista quanto a esse tema.

---

[106] RODOTÀ, 2008, p. 84.
[107] KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.
[108] *Ibidem*.
[109] *Ibidem*, p. 455-456.
[110] ”2. O disposto no n.º 1 não se aplica se se verificar um dos seguintes casos: a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados; b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva

Um dos aspectos da proteção de dados sensíveis é afastar a possibilidade de discriminação. Ademais, o princípio da não discriminação está previsto no art. 6º, inciso IX, da LGPD. Para isso, faz-se necessário o princípio da isonomia material que "[...] serve a fundamentar o seu regime diferenciado"[111]. Assim, esse princípio é o guia para a utilização de dados sensíveis:

> O princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam

---

nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados; c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento; d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares; e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular; f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional; g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados; h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3; i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados- -Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional; j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.º 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados. 3. Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes. 4. Os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde".

[111] DONEDA, 2020a, p. 4.

> inequitativos. Esse princípio deve servir como base de sustentação da tutela dos dados sensíveis, especialmente quando estamos diante do exercício democrático e do acesso a direitos sociais, tais como o direito ao trabalho, à saúde e à moradia[112].

Em razão disso, os dados sensíveis da pessoa devem ser utilizados para finalidades que atendam ao seu interesse. O tratamento dos dados é norteado pelo princípio da finalidade, da necessidade e da adequação[113] — adiante se discutirá cada um desses princípios. Por isso, a utilização desse tipo de dados é mais restrita, pois, uma vez atingida a finalidade estabelecida, eles devem ser destruídos por programas desenvolvidos para isso[114].

Ademais, a proteção contra a discriminação decorrente do processamento de dados pessoais depende da proibição ou limitação da coleta e do armazenamento desses dados e informações sensíveis[115]. Por conseguinte, o princípio da isonomia é o instrumento para evitar as práticas discriminatórias[116].

Nem sempre, em um primeiro momento, um dado pode se revelar sensível, mas pode passar a ser, pois a tecnologia pode fazer correlações de dados para obter informações sobre acontecimentos e comportamentos[117].

Considera-se tratamento de dados pessoais, segundo a LGPD (art. 5º, inciso X), toda operação realizada com dados pessoais, como as que se referem a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Esboça-se um exemplo acerca do tratamento de dados. Uma rede de supermercados, nos Estados Unidos, pôde saber que uma adolescente estava grávida por meio de dados e informações que coletaram a partir de buscas feitas por ela. No entanto, imagina-se que se trata de uma filha de seus clientes, uma menor de idade, que está grávida. O supermercado, então, envia promoções específicas sobre gravidez para eles. No entanto, os próprios pais da menina

---

[112] MULHOLLAND, 2018, p. 174.
[113] RODOTÀ, 2008.
[114] *Ibidem*.
[115] MENDES, 2014.
[116] *Idem*, 2020.
[117] *Ibidem*.

não sabem da gravidez e passam a saber pelo supermercado quando vão reclamar das recomendações de produtos [118].

Os dados sensíveis são aqueles que apresentam maiores riscos e potencialidade discriminatória[119]. No entanto:

> E, ainda, cada vez mais é patente que mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos considerados sensíveis sobre a personalidade de alguém, podendo levar a práticas discriminatórias. Afirma-se, em síntese, que um dado, em si, não é perigoso ou discriminatório — mas o uso que dele se faz pode sê-lo[120].

A informação obtida por meio dos dados pessoais continua atrelada à pessoa, embora possa circular de maneira independente, pois é a representação do titular, reflete a sua personalidade, ou seja, é considerada uma extensão da personalidade[121]. Por essa razão, a informação é protegida, assim, são dados sensíveis.

Para proteger os dados, faz-se necessário o exercício da autodeterminação informativa pelo titular, que consiste na possibilidade de o sujeito decidir de que maneira os seus dados poderão ser utilizados e se poderão ser utilizados, ou seja, qual o limite com que eles poderão ser manuseados[122]. Desse modo:

> [...] a autodeterminação informativa, significando que, ao se abrir mão parcialmente de sua privacidade para se inserir na era digital, deve ser resguardado o direito ao ser humano de um controle — mesmo que mínimo — de suas informações, bem como das conclusões que se retiram delas[123].

Um dos instrumentos para esse exercício é o *habeas data*, pois assegura a eficácia horizontal dos direitos fundamentais, que se aplica também as relações privada[124]. É um remédio constitucional que pode ser utilizado quando se tratar de bancos de dados criados e mantidos pelo setor público ou privado:

---

[118] BIONI, 2020a.
[119] DONEDA, 2020a.
[120] *Ibidem*, p. 2.
[121] *Ibidem*.
[122] *Ibidem*.
[123] CAMURÇA; MATIAS, 2021, p. 10.
[124] MENDES, 2014.

> Tendo em vista tratar-se de direito à personalidade, já que os dados armazenados representam a pessoa na sociedade, qualquer banco ou registro de dados pessoais deve ser entendido como público, independentemente de ser gerido por organismo privado ou estatal[125].

Nessa esteira, Laura Mendes[126] defende que a autodeterminação informativa tem como fundamento a garantia do direito fundamental do *habeas data.* A Constituição da República de 1988 garante que se concederá *habeas data* (art. 5º, inciso LXXII):

> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Mendes[127], por seu turno, aponta que a Lei do Cadastro Positivo (Lei de n. 12.414/2011) exprime a evolução do conceito da autodeterminação informativa, pois fornece mecanismos de controle que a pessoa pode usar em relação aos seus dados, como a opção da cancelar (*opt out*) o seu cadastro[128]. O *habeas data* é uma garantia processual a que a pessoa pode ter acesso ou, podendo solicitar a correção dos seus dados. Há também, implicitamente, um direito material que fundamenta essa garantia processual[129]:

> O habeas data (eis o dado) é um instituto jurídico típico da sociedade da informação. Muito além do "eis o corpo" relacionado à integridade física ínsita à liberdade de locomoção, também precisamos ter autodeterminação sobre as informações que nos digam respeito[130].

A autodeterminação informativa, por sua vez, é um dos fundamentos da proteção dedados pessoais (art. 2º, inciso, LGPD) e ganha maior relevância na proteção do titular que pode retificar e solicitar a exclusão de seus dados, assim como subsidia o direito ao esquecimento. Ademais, o Supremo Tribunal Federal,

---

[125] *Ibidem*, p. 184.
[126] MENDES, 2019.
[127] *Idem*, 2014.
[128] LCP: "Art. 5º São direitos do cadastrado: I - obter o cancelamento ou a reabertura do cadastro, quando solicitado".
[129] MENDES, 2019.
[130] RODRIGUES, Geisa. **Série carreiras federais** – ações constitucionais. São Paulo: Grupo GEN, 2014. p. 63.

na Ação Direta de Inconstitucionalidade n. 6387 MC-Ref., reconheceu a proteção dos dados pessoais como um direito fundamental, assim como o direito à autodeterminação informativa[131].

Somente estará excluído dessa situação de proteção da LGPD o cadastro utilizado por pessoas físicas para atividades exclusivamente pessoais e domésticas (agenda de contatos, correspondência)[132].

Outro impacto negativo dessa gama de informações sobre as pessoas é a possibilidade de tolher o desenvolvimento da personalidade, bem como inibir como o sujeito age no dia a dia. Isso pode acontecer quando o indivíduo se limita por saber que está sendo monitorado por meio da internet, das redes sociais, dos aplicativos — podendo incluir informações como possíveis inadimplências, por exemplo. Por isso Thiago Junqueira[133] adverte que há um efeito inibitório que faz com que uma pessoa deixe de ter determinados comportamentos ou de fazer algo a fim de ser valorizada pelas decisões que serão tomadas com base em seus dados coletados.

Sob outro aspecto, essa restrição da liberdade pode resultar na oferta de produtos, serviços e nas suas escolhas, pois as ofertas estariam limitadas pelas informações colhidas e armazenadas por dedução[134] que resultam em um perfil. Essa restrição também pode agir no livre desenvolvimento da personalidade, pois pode colocar uma pessoa em determinado perfil sociopolítico em que a

---

131 "De sorte que eu lavro uma ementa concordando inteiramente com o brilhante voto da Ministra Rosa Weber, que foi cirúrgica num momento tão complexo para fazer esse cotejo entre essa liberdade de informação que municia a estatística e, de outro lado, a privacidade pessoal, para, concordando com Sua Excelência, reitero, a Ministra Rosa Weber, assentar, em primeiro lugar, que a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana, conforme foi muito bem destacado já, digamos assim, pela Ministra Rosa Weber e já no primeiro voto, o do Ministro Alexandre de Moraes". BRASIL. Supremo Tribunal Federal. **Referendo na medida cautelar na ação direta de inconstitucionalidade 6.387 Distrito Federal**. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (COVID-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o Instituto Brasileiro de Geografia e Estatística. *Fumus boni juris. Periculum in mora*. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Interessado: Presidente da República. Relatora: Ministra Rosa Weber, 11 nov. 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 30 ago. 2022.

132 MENDES, 2014.

133 JUNQUEIRA, 2020a.

134 DONEDA, 2020a.

privilegia ou a prejudica[135] — nesse caso, há uma vigilância de comportamento prejudicial quando a coleta de dados é aquém do necessário. Portanto, "[...] este controle em relação aos indivíduos pode assentar obstáculos reais ao livre desenvolvimento em torno de perfis historicamente determinados"[136], o que pode inviabilizar "novas identidades coletivas"[137].

No que diz respeito aos dados sensíveis, deve-se considerar o contexto em que são analisados e se eles têm relevância ao tratamento, haja vista que muitas das informações consideradas sensíveis podem estar disponíveis ao público em geral, pois a pessoa pode ter manifestado a sua opinião política, religiosa, por exemplo, abertamente em uma rede social ou em manifestações, protestos, em reuniões[138].

Diante disso, o contexto deve ser balizado com os princípios da finalidade, adequação e necessidade — que serão abordados novamente — assim como o princípio da isonomia para não haver discriminações. Quanto à relevância do contexto das informações:

> Foi o próprio tratamento automático dos dados a demonstrar, à evidência que nenhuma informação tem valor por si mesma, mas em virtude do contexto no qual está inserida, ou pelas finalidades para as quais é utilizada, ou pelas outras informações às quais tem sido associada. As regras sobre a circulação dos dados então tendem a ser cada vez mais orientadas para a consideração de contextos, funções e associações[139].

Como mencionado, os dados sensíveis têm potencialidade discriminatória[140] a depender do contexto em que são utilizados. Portanto, o tema aqui estudado tem relação com a proteção de dados, privacidade, mas também com o princípio da igualdade[141]. Em virtude disso, o tratamento dos dados pessoais sensíveis deve ser norteado pelos "[...] princípios da precaução e da prevenção como pilares de uma constelação jurídica que tem como vetor

---

[135] RODOTÀ, 2008.
[136] *Ibidem*, p. 83.
[137] *Idem*.
[138] RODOTÁ, 2008.
[139] *Ibidem*, p. 77.
[140] *Ibidem*.
[141] *Ibidem*.

primordial a proteção da dignidade da pessoa humana, dentro e fora do ambiente digital”[142].

A Lei Geral de Proteção de Dados Pessoais elenca diversos princípios a serem observados no processamento e tratamento de dados pessoais. Mais especificamente, no artigo 6º, traz o princípio da transparência, que tem significativa importância nas decisões automatizadas quando se fala em direito à explicação, tema a ser abordado no último capítulo. Não obstante isso, convém destacar que:

> [...] a LGPD evidenciou a transparência como elemento central e, desta forma, tornou cristalina a ideia de que todos os procedimentos envolvendo dados pessoais, sobretudo os dados sensíveis, devam ser compatíveis com a finalidade da coleta e minimizados em uma política de uso racional, sobretudo em razão da sua perenidade. Outro aspecto notável foi o fortalecimento da proteção e a decorrente vedação de uso de dados sensíveis para fins discriminatórios independentemente do consentimento do usuário, especialmente face aos riscos de destruição, de divulgação e de acesso indevido em razão da estrutura aberta da internet[143].

A privacidade possibilita o livre desenvolvimento da personalidade que requer espaço para que possa florescer e que esteja livre de “[...] condicionamentos que possam distorcer o processo formativo”.[144] Ademais, os dados pessoais em geral e os sensíveis são “[...] geralmente irrenunciáveis e se encontram atrelados de modo insuperável à identidade pessoal”[145].

Como todos atualmente vivenciam uma sociedade e uma economia baseadas em dados, a classificação das pessoas ou de grupos é muito facilitada pelos algoritmos e pela inteligência artificial. Nos próximos capítulos será vista a legislação para proteção da privacidade e para o exercício da autodeterminação informativa. Para o exercício da autodeterminação informativa, não basta apenas uma legislação, mas faz-se necessária toda uma arquitetura[146] para combater discriminações e exclusões sociais.

---

[142] SARLET; RUARO, 2021, p. 85.
[143] SARLET; RUARO, 2021, p. 99
[144] RODOTÀ, 2008, p. 117.
[145] SARLET; RUARO, 2021, p. 93.
[146] RODOTÀ, *op. cit*.

Isso tem relação com a concessão de crédito, com os seguros que fazem a análise de risco de potenciais contratantes. A concessão de crédito representa um papel importante na sociedade, pois fomenta o desenvolvimento social, os pequenos negócios, assim como crédito estudantil, que contribui para o ingresso de alunos em universidades. Portanto, a concessão de crédito pode contribuir para mudanças sociais ou reproduzir injustiças, ou seja, “automatizar injustiças históricas”[147].

É nesse contexto que Rodotà utiliza a expressão “sociedade da classificação”[148], que faz com que as pessoas tenham menos controle dos seus dados, ainda que haja diversos dispositivos legais voltados para isso. Essa classificação cria pessoas virtuais, que são geradas pelo mercado[149] — trata-se de uma imagem que se projeta sem controle do titular, mas com impactos concretos. Diante disso, o titular dos dados tem:

> direito de acesso e de conhecimento dos dados pessoais existentes em registros (banco de dados) públicos e privados; o direito ao não conhecimento, ao tratamento e à utilização e à difusão de dados pessoais, particularmente no que concerne aos dados sensíveis pelo Estado ou por terceiros. Inclui-se, de toda maneira, um direito de sigilo quanto aos dados pessoais[150].

Um dos principais aspectos da proteção de dados é que o controle deles se torna cada vez mais difícil diante da ubiquidade das tecnologias da informação[151]. Logo, há um desequilíbrio nas relações e de poderes[152]. Por isso, a determinação de se os dados são sensíveis ou como poderão ou não ser utilizados deve ser feita com base nos princípios da LGPD.

1.2 DIREITO À IGUALDADE E O PRINCÍPIO DA NÃO-DISCRIMINAÇÃO

---

[147] VILARINO, Ramon. Pontuação de crédito, aprendizagem de máquina e os riscos de alocar recursos predizendo o passado. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022. p. 221-222.
[148] RODOTÀ, *op. cit.*, p. 114.
[149] RODOTÀ, 2008.
[150] SARLET; RUARO, 2021, p. 94.
[151] MENDES, 2014.
[152] *Ibidem*.

A Constituição da República de 1988 em seu art. 3º, inciso IV, tem como um dos objetivos fundamentais promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. Ademais, o art. 5º da CRFB, inciso VIII, assegura que "[...] ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política, salvo se as invocar para eximir-se de obrigação legal a todos imposta e recusar-se a cumprir prestação alternativa, fixada em lei".

Também está previsto o princípio da igualdade no art. 5º, *caput* da CRFB: "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade".

O princípio da isonomia tem dois aspectos, um formal e outro material. O primeiro pode ser descrito como: "[...] a questão sob a perspectiva das normas e sua aplicação"[153]; e a isonomia material, por sua vez, "[...] se ocupa da situação real em que as pessoas se encontram, embora as duas dimensões interajam continuamente"[154].

No entanto, entende-se o princípio da isonomia, "[...] modernamente, como tendo implicação consequencial de igualdade substancial real, e não apenas formal"[155]. Isso significa que se deve "[...] tratar desigualmente os desiguais na exata medida de suas desigualdades"[156]. Para que se respeite a dignidade da pessoa humana, há de se tomar como pressuposto a garantia da isonomia de todos os seres humanos, por isso os indivíduos não podem ser submetidos a tratamento discriminatório e arbitrário[157].

As causas de discriminações apontadas no art. 3º, inciso IV, da CRFB, dizem respeito a estigmas e discriminações históricas. São denominadas de discriminações diretas[158] as previstas no referido artigo, pois são características

---

[153] BARCELLOS, Ana Paula. **Curso de direito constitucional**. 4. ed. São Paulo: Grupo GEN, 2022. p. 272.
[154] *Ibidem*, p. 272.
[155] GRINOVER, Ada P. *et al*. **Código Brasileiro de Defesa do Consumidor**. 13. ed. São Paulo: Grupo GEN, 2022. p. 488.
[156] *Ibidem*, p. 488.
[157] SARLET, 2018.
[158] "Joaquim Barbosa conceitua a discriminação indireta (preferindo utilizar a expressão norte-americana 'teoria do impacto desproporcional')". (JUNQUEIRA, 2020a, p. RB-1.5).

imutáveis, geralmente[159]. As discriminações indiretas, por sua vez, decorrem de características mutáveis, como o endereço de uma pessoa (CEP)[160].

Junqueira explica que a discriminação direta está protegida constitucionalmente, pois há um critério protegido como as hipóteses previstas no art. 3º, inciso IV, já mencionado[161]. Portanto, "[...] a discriminação direta pressupõe um tratamento desfavorável que tenha como elemento de comparação uma característica protegida"[162].

A discriminação indireta, por outro lado, tem como causa um critério neutro como o CEP (Código de Endereçamento Postal), CPF (Cadastro de Pessoas Físicas), por exemplo. Existe também a discriminação por associação, que tem relação com um fator suspeito, como gravidez e sexo feminino[163], desse modo:

> [...] haverá uma discriminação por associação equivalente à discriminação direta. Geralmente se observa, nessa eventualidade, uma intenção de discriminar por parte do agente. Por outro lado, caso a associação entre o elemento utilizado e o fator suspeito (*e.g.*, consumo de determinado produto alimentício e raça) não seja intuitiva e/ou intencional, dependendo do impacto que dele derivar, poderá ocorrer uma discriminação indireta[164].

De modo geral, objetiva-se, neste estudo, a investigação do princípio da não discriminação e da igualdade em relação ao tratamento de dados pessoais — tendo em vista que o princípio da igualdade é o gênero e a proteção antidiscriminatória uma espécie[165]. Diante disso, há que se verificar se as diferenciações são justificáveis a fim de não tenham efeitos ou propósitos discriminatórios que são socialmente intoleráveis[166].

Celso Antônio Bandeira de Mello[167] ensina qual critério pode ser considerado legitimamente manipulável, em que se pode haver distinção entre

---

[159] *Ibidem*.
[160] *Ibidem*.
[161] *Ibidem*.
[162] *Ibidem*, p. RB-1.5.
[163] *Ibidem*.
[164] JUNQUEIRA, 2020a, p. RB-2.2
[165] *Ibidem*.
[166] *Ibidem*.
[167] MELLO, Celso Antônio Bandeira de. **O conteúdo jurídico do princípio da igualdade**. 3. ed. São Paulo: Malheiros Editores, 2010. p. 11.

as pessoas para tratamentos jurídicos diversos, respeitando-se a isonomia, ou seja, quais discriminações são juridicamente toleráveis[168]. À vista disso, pode-se dizer que há discriminações ou diferenciação consideradas ilícita (proibida), lícita (permitida), e situações em que há discriminação imposta, ou seja, devida[169].

A discriminação lícita pode vir a tornar-se abusiva[170]. Ela decorre de dado ou informação que a princípio não é relevante para uma contratação, mas que é utilizada, como nos casos de "otimização de preço" com base no comportamento da pessoa[171]. Por isso, a LGPD (art. 21) estabelece que dados pessoais referentes ao exercício regular de direitos pelo seu titular não podem ser utilizados em seu prejuízo[172].

As decisões automatizadas podem causar discriminações de maneira sútil, pois podem decorrer da análise de dados de maneira indireta — ou seja, quando se obtém uma informação indiretamente —, em razão do tratamento dos dados colhidos. Além disso, há critérios que não podem ser considerados para criar diferenciações, mas se houver um critério neutro combinado com fatos e situações diferentes, esse pode ser utilizado para justificar o discrímen[173].

O tempo é considerado um elemento neutro, mesmo quando a lei se refere a uma determinada data ou a um direito exercido em um lapso temporal. Desse modo, trata-se de um critério qualificador, ou seja, é considerado um elemento diferenciador[174]. Assim, o que interessa é o que ocorreu em um período de tempo ou data. Por exemplo:

> Então, quando se diz que serão estáveis os concursados, após dois anos, o que, em rigor lógico, admitiu como diferencial entre os que preenchem e os que não preenchem tal requisito, não foi o tempo *qua tale* — pois este é *neutro*, *necessariamente idêntico para todos os seres* — porém *o que ocorreu ao longo dele,* uma certa sucessão, uma dada persistência continuada no exercício de cargo[175].

---

168 *Ibidem*.
169 JUNQUEIRA, 2020a, p. RB-2.3.
170 *Ibidem*.
171 *Ibidem*.
172 LGPD: "Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo".
173 MELLO, 2010.
174 *Ibidem*.
175 *Ibidem*, p. 31.

Portanto, o tempo não é o fator de discrímen. O fator é o exercício funcional de um servidor público que ocorreu em determinado período — ou seja, não se trata de um fator abstrato[176].

Ao mesmo tempo que a Constituição da República combate as discriminações, busca a igualdade material ao trazer tratamento distinto entre os gêneros na previdência social, no serviço militar obrigatório (CRFB, art. 143, §2º e 201), por exemplo. Diante disso, são permitidas desequiparações desde que tenham um fundamento racional e razoável e que se destinem a promover um fim constitucionalmente legítimo[177]:

> A doutrina propõe que a verificação da razoabilidade de uma norma que crie desequiparações envolva três testes sucessivos.
> A doutrina propõe que a verificação da razoabilidade de uma norma que crie desequiparações envolva três testes sucessivos. Em primeiro lugar, verifica-se se o fator de discrímen escolhido pela norma para apurar se tal elemento corresponde a uma diferenciação real — isto é: objetivamente existente entre as pessoas, situações ou coisas — é relevante. [...]
> Na sequência, é preciso que haja um nexo racional e razoável entre a diferença das situações — demarcada pelo elemento de discrímen — e o tratamento diferenciado criado pela norma, tendo em conta o fim por ela pretendido. [...]
> Por fim, em terceiro lugar, ainda que seja racional e razoável o tratamento diferenciado criado pela norma, ele deve ser compatível com os demais princípios e regras constitucionais. [...] Ou seja: o princípio da isonomia não veicula o igualitarismo absoluto, sendo legítimas as normas que criam desequiparações razoáveis[178].

Ademais, para que se possa fazer o tratamento de dados pessoais, deve-se estar amparado por uma das hipóteses legais de tratamento de dados (LGPD, art. 7º) para que a ação seja legítima e lícita — em determinadas situações, deve-se haver o consentimento do titular. Já em relação aos dados pessoais sensíveis, o art. 11 estabelece que o "[...] titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas". Entende-se que o legítimo interesse é uma hipótese com um grau maior de subjetividade para

---

[176] *Ibidem*.
[177] BARCELLOS, 2022.
[178] BARCELLOS, 2022, p. 273.

tratamento de dados pessoais. Os art. 7º e 11 da LGPD, por sua vez, seriam taxativos[179].

O legislador, ao utilizar a expressão “somente” no art. 11, pode indicar que aponta para uma interpretação restritiva para a possibilidade de tratamento de dados e procura enumerá-las devido ao cuidado que esse tema requer: “O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses [...]”.

No que diz respeito ao consentimento, Mario Viola e Chiara Teffé[180] defendem uma interpretação restritiva desse instituto, haja vista a grande utilização de dados para o desenvolvimento de negócios, propagandas, mercantilização desses dados, tratamento de dados pessoais de usuários de serviços *online*. Por isso, não pode o agente estender a autorização concedida para o tratamento de dados para outros meios além dos que foram pactuados, seja em momento posterior ou para finalidade diversa.

Em relação ao tratamento de dados pessoais de crianças e de adolescentes, esses são considerados dados pessoais sensíveis. A legislação registra disposições específicas segundo as quais o uso desses dados deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Sem o consentimento, será possível na seguinte hipótese “§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo”. Entretanto, esse tema específico não será objeto de análise no presente estudo.

A relevância da proteção dos dados pessoais decorre do fato de eles identificarem as pessoas e de que podem representar “o que seria” a pessoa na

---

[179] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.º e 11. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020. p. 133.
[180] *Ibidem*.

sociedade[181]. Por isso, podem afetar as pessoas de maneira direta ou indireta, sem que saibam.

O princípio da não discriminação previsto na LGPD visa a assegurar a proteção dos dados pessoais sensíveis[182]. Ademais, em virtude do conteúdo dos dados pessoais sensíveis, eles oferecem maior vulnerabilidade, o que pode acarretar efeitos negativos como a discriminação. A vulnerabilidade é evidente no ambiente digital, onde há um déficit informacional, educacional, técnico, por isso:

> Para fins de mitigação de riscos, é importante que os controladores considerarem os titulares sempre vulneráveis quanto ao entendimento das infinitas possibilidades de tratamento, notadamente quando ocorrer por meios digitais, em uma "conduta silenciosa", pois o déficit informacional ganha relevância no ambiente cibernético, diante da velocidade das mutações do tratamento de acordo com o avanço tecnológico, aumentando, portanto, a necessidade de informações claras, completas e ostensivas aos titulares, que aceitam determinadas transações ao confiar voluntariamente nas informações concedidas pelos responsáveis[183].

Nesse sentido, as discriminações causadas por algoritmos podem decorrer de erro estatístico, a partir do uso de dados sensíveis, por generalização injustas, ou por ser limitadora de direitos[184]. A discriminação por erro estatístico pode advir da incorreta coleta de dados pelos engenheiros ou cientistas de dados[185]. Já a utilização de dados sensíveis pode levar a discriminações, ainda que sejam estatisticamente corretas. Dessa forma, o fundamento dessa discriminação, da discriminação por aproximação ou de maneira indireta (*proxy*)[186], são os dados em si. Junqueira, por sua vez, indica que há uma

---

[181] MENDES, 2019.
[182] *Idem*, 2014.
[183] MALDONADO; Viviane Nóbregae; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. RL-1.2.
[184] MENDES, Laura S.; MATTIUZZO, Marcela; FUJIMOTO, Mônica T. Discriminação algorítmica à Luz da Lei Geral de Proteção de Dados. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo GEN, 2020.
[185] *Idem*.
[186] "É o que ocorre, por exemplo, quando um algoritmo utiliza informações sobre identificação religiosa de um indivíduo para designar seu credit score no Brasil – a Lei do Cadastro Positivo proíbe o uso desse tipo de informação para essa finalidade. Duas características são relevantes para se considerar um perfilamento como discriminatório nesse caso: além de utilizar dados sensíveis, a classificação deve se basear em características endógenas, ou então deve destacar grupos historicamente discriminados" (MENDES; MATTIUZZO; FUJIMOTO, 2020, p. 43).

distinção entre a discriminação indireta e por aproximação, que pode ser consciente ou inconsciente:

> [...] ainda que programados desconsiderando dados sensíveis, os algoritmos poderão causar discriminação (indireta e por "associação"). A doutrina especializada vem alertando, nesse sentido, que o progresso tecnológico em curso tende a implicar a mudança da "discriminação consciente" e "explícita invasão da privacidade" para "associações inconscientes" e discriminações indiretas pelo segurador, muitas vezes, sem o conhecimento do segurado. E, se não forem tomadas as devidas providências, as decisões automatizadas passarão a ser baseadas em um "conjunto de correlações e previsões que podem sobrecarregar mais alguns grupos específicos do que outros e invadir determinadas áreas privadas[187].

A discriminação por generalização injusta (correlação abusiva), por sua vez, pode estar correta estatisticamente (acurácia), mas categoriza, classifica, enquadra as pessoas em determinados grupos[188]. Por exemplo, uma classificação pode considerar que, se uma pessoa mora em determinada região, ela pertence a um grupo que tem certo poder econômico. Todavia, essa pessoa pode, por algum motivo aleatório e particular, não se enquadrar nesse grupo, ou seja, ser uma exceção[189]:

> Desse modo, embora o algoritmo esteja correto e as informações também, ainda assim o resultado será uma generalização incorreta e injusta, na medida em que mesmo um resultado estatisticamente relevante apresentará um percentual de pessoas que não se encaixam perfeitamente naquela média[190].

Por fim, é possível que ocorra uma discriminação que limite o exercício de direitos, e nesse caso o resultado pode estar correto estatisticamente[191]. Nessa situação, há "[...] uma relação entre a informação emprega pelo algoritmo e a realização de um direito"[192], ou seja, o direito é afetado a ponto de ocorrer uma discriminação.

Adiante, uma outra distinção discriminatória que está na LGPD diferencias as discriminações entre: ilícitas e abusivas — distinção que está prevista no art.

---

187 JUNQUEIRA, 2020a, p. VII.
188 MENDES; MATTIUZZO; FUJIMOTO, 2020.
189 *Ibidem*.
190 *Ibidem*, p. 438.
191 *Ibidem*.
192 *Ibidem*.

6º, inciso IX, no princípio da não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. A abusividade no tratamento dos dados pessoais objetiva evitar discriminações e limitar o uso dos dados sensíveis[193]. Diante disso, Caitlin Mulholland afirma que, quando há potencial discriminatório, veda-se a utilização desses dados. Portanto, "[...] a limitação para o tratamento de dados se concretizaria na proibição de seu uso de maneira a gerar uma discriminação, um uso abusivo e não igualitário de dados"[194].

No que diz respeito à discriminação e aos dados pessoais sensíveis, deve-se também considerar a criação de perfis, pois, para a sua formação, faz-se necessário dados pessoais de diversas pessoas, grupos ou comunidades. Diante disso, extrai-se a presunção de uma realidade que pode refletir ou não a realidade de determinada pessoa. No caso da perfilização (*profiling*), essa prática constitui uma discriminação abusiva[195].

A discriminação ilícita está prevista na Constituição da República de 1988, por exemplo, no art. 3, inciso IV, ou em lei infraconstitucional, como a Lei 7.716/1989[196]. Além dessas, a LGPD também a proíbe no tratamento dos dados. Outro exemplo é o art. 3, §3º da Lei do Cadastro Positivo[197] (Lei n. 12.414/2011) que será abordado no Capítulo 2.

No que diz respeito à discriminação abusiva, Laura Mendes, Marcela Mattiuzzo e Mônica Fujimoto[198] elencam quatro espécies dela, como já se viu: discriminação por erro estatístico, discriminação pelo uso de dados sensíveis, discriminação pela generalização injusta (ou correlação abusiva), discriminação limitadora do exercício de direitos. A discriminação por erro estatístico pode advir do modo como o dado foi tratado, de erro técnico do algoritmo, de erro no *input* ou no cálculo estatístico[199]. Assim, nesse caso, atribui-se indevidamente

---

193 MULHOLLAND, 2021.
194 *Ibidem*, p. 03.
195 *Ibidem*.
196 MENDES; MATTIUZZO; FUJIMOTO, 2020.
197 *Ibidem*.
198 *Ibidem*.
199 *Ibidem*.

determinada característica a um determinado grupo, não importando se houve intenção ou não[200].

Já a discriminação causada pelo uso de dados sensíveis ocorre em situações em que o dado a princípio não é considerado sensível. Trata-se, então, de uma situação residual. As situações que envolvem dados considerados sensíveis expressamente na LGPD não consistem em abusividade[201].

A outra hipótese de discriminação, aquela em virtude de generalização injusta (ou correlação abusiva), acarreta um grande prejuízo para pessoa, pois decorre de uma aleatoriedade ou da ausência de causalidade entre o *input* e o *output*[202].

Por último, a discriminação limitadora do exercício de direitos tem como referência o art. 21 da LGPD: "Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo"[203].

No próximo capítulo serão vistos exemplos, como os critérios aleatórios, que têm sido utilizado para criar diferenciações não justificadas. Diante disso, o conceito de dados pessoais sensíveis não pode ser restrito, nem ter um rol exaustivo ou taxativo, mas deve ser visto dentro das circunstâncias, ou seja, "[...] funcionalizado de acordo com o tratamento que é concedido a eles"[204].

Os dados sensíveis que digam respeito à saúde da pessoa têm normas específicas (LGPD, art. 7º, inciso VIII)[205]. O tratamento desses dados pessoais

---

[200] MENDES; MATTIUZZO; FUJIMOTO, 2020.

[201] "Um exemplo de tratamento auxilia a compreender a questão. Se uma pessoa é filiada a um determinado sindicato, e que por conta disso um algoritmo que direciona publicidade digital e que legitimamente possui essa informação passa a encaminhar a essa pessoa anúncios relacionados a vagas de emprego intimamente ligadas com o sindicato em questão, estamos diante de um cenário de discriminação algorítmica, que faz uso de dados sensíveis e que tanto é estatisticamente relevante quanto impõe um impacto razoável ao grupo discriminado" (MENDES; MATTIUZZO; FUJIMOTO, 2020, p. 447).

[202] "[...] julgamento do recurso repetitivo sobre credit scoring, segundo o qual técnicas de análise de dados permitiriam realizar uma análise do potencial de adimplemento de uma pessoa com base em seu time de futebol, em um caso hipotético em que fosse encontrada uma correlação estatística relevante entre esses dois elementos (STJ, 2014, p. 43). Como dito, o problema aqui é precisamente a completa ausência de causalidade entre o input (o time de futebol) e o output (a capacidade de adimplemento)" (MENDES; MATTIUZZO; FUJIMOTO, 2020, p. 447).

[203] *Ibidem*, p. 449.

[204] MULHOLLAND, 2021, p. 03.

[205] LGPD: "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".

sensíveis somente poderá ocorrer na hipótese: "[...] tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (LGPD, art. 11, alínea "f"). Além disso, veda-se "[...] às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários" (art.11, § 5º)[206].

Como a tecnologia e a ciência dos dados se desenvolveram exponencialmente e as decisões automatizadas impactam a vida das pessoas, deve-se resguardá-las para que não estejam sujeitas a práticas discriminatórias que extrapolam e invadem o âmbito da privacidade e igualdade[207]. A proteção de dados pessoais passa a ter relação com a igualdade, ainda mais quando se tem em vista, por exemplo, a vigilância feita por dispositivos ligados à internet, por câmeras de vigilâncias, que podem classificar os sujeitos de maneira que os afeta[208], como em negócios ou em casos de acesso a políticas públicas.

Dessa forma, a teoria do diálogo das fontes também tem muito a contribuir para essa discussão, pois ela tem como objetivo preservar os direitos fundamentais e dar interpretação a normas e princípios para que não prejudiquem o mais fraco, o mais vulnerável em uma relação jurídica, assim como supera a visão dualista entre direito público e privado[209]. Além disso, colabora para que não seja feita uma interpretação ou uma decisão inconstitucional[210]: "[...] a teoria do diálogo tem direta relação com os direitos

---

[206] LGPD: "Art. 11, § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: [...]". "Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas".

[207] BIONI, 2020a.

[208] MENDES, 2014.

[209] MARQUES, Claudia Lima; BENJAMIN, Antonio Herman. A teoria do diálogo das fontes e seu impacto no Brasil: uma homenagem a Erik Jayme. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 115, p. 21-41, jan./fev. 2018.

[210] MARQUES; BENJAMIN, p. 29-30.

fundamentais, pois põe em relevo o sistema de valores que estes representam e orienta a aplicação simultânea das regras de diferentes fontes para dar efetividade a estes valores".

Tendo em vista as legislações em vigor para o tema, entende Gustavo Tepedino[211] que as respostas para as questões trazidas pela inteligência artificial devem ser encontradas no próprio ordenamento jurídico, ou seja, a partir de sua integralidade, e não em novos diplomas normativos. Esse será um dos objetivos do estudo aqui proposto, qual seja, examinar o tema das decisões automatizadas a partir do ordenamento jurídico brasileiro.

[211] SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O Direito Civil na era da inteligência artificial**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

CAPÍTULO II

2 INTELIGÊNCIA ARTIFICIAL E OPACIDADE

A principal característica que se aponta sobre a Inteligência Artificial (IA) é a sua capacidade de simular o raciocínio humano[212]. O termo "inteligência artificial" se refere a um conceito mais amplo que consiste na capacidade de as máquinas "pensarem" e "discernirem". Elas são consideradas inteligentes se se aproximarem da chamada singularidade tecnológica[213]. Essa singularidade consiste na "[...] aproximação entre o biológico e o tecnológico que permita ao algoritmo processar dados, formular hipóteses e apresentar soluções, mas também agir de forma arbitrária, livre e autônoma"[214].

A resolução n. 332 do CNJ[215] (art. 3º, incisos I e II) considera o modelo de inteligência artificial como um "[...] conjunto de dados e algoritmos computacionais, concebidos a partir de modelos matemáticos, cujo objetivo é oferecer resultados inteligentes, associados ou comparáveis a determinados aspectos do pensamento, do saber ou da atividade humana". E os algoritmos, por sua vez, como uma "[...] sequência finita de instruções executadas por um programa de computador, com o objetivo de processar informações para um fim específico".

Não há um único conceito para designar toda a inteligência artificial, mas há diversas espécies, cada uma com uma potencialidade diferente. No entanto, pode-se dizer que há um consenso em ser afirmar que a inteligência artificial tem como objetivo solucionar problemas específicos[216], utilizando linguagem matemática "[...] para atuar, os algoritmos precisam converter tudo em

---

[212] MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.
[213] FALEIROS JÚNIOR, José Luiz de Moura. A evolução da inteligência artificial em breve retrospectiva. *In*: BARBOSA, Mafalda Miranda *et al*. (coord.). **Direito digital e inteligência artificial**: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021.
[214] *Ibidem*, p. 49.
[215] CONSELHO NACIONAL DE JUSTIÇA. **Resolução n. 332, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança na produção e no uso de inteligência artificial no Poder Judiciário e dá outras providências. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/files/original191707202008255f4563b35f8e8.pdf. Acesso em: 05 fev. 2023.
[216] SARLET *et. al*., 2022.

expressões matemáticas, como se toda qualidade pudesse ser traduzida em quantidades. Eles fazem isso para comparar os dados de entrada e classificá-los conforme sua missão”[217].

O aprendizado da máquina (*machine learning*) consiste em um processo que gera catalogações de resultados (*logs*), o que faz com que o algoritmo possa fornecer soluções devido ao treinamento da máquina baseado em tentativa e erro[218].

Nesse contexto, a IA subdivide-se em duas espécies: IA forte e IA geral. Costuma-se indicar como característica da IA o objetivo de resolver problemas, tarefas específicas e predeterminadas[219]. É possível ainda dividir o sistema de aprendizado da máquina (*machine learning*) em supervisionado e não supervisionado[220]. No modelo supervisionado, os critérios de correlações iniciais são parametrizados, ou seja, ensinados por uma pessoa da criação do programa de computador. São feitos testes, treinamentos do sistema até que se obtenham resultados satisfatórios e precisos[221].

O professor Diogo Cortiz[222] explica que a expressão “inteligência artificial” é um termo amplo que abrange as suas diversas espécies. Entretanto, não há ainda uma IA geral que resolva problemas, o que se cria são modelos para a resolução de problemas específicos.

Entre as técnicas que podem ser utilizadas, existem a baseada em conhecimento e a em aprendizado estatístico: na primeira, não mais utilizada, fazia-se o mapeamento do conhecimento específico de uma área e a partir disso se codificava um programa[223]. Explica o professor[224] que, atualmente, utiliza-se

---

[217] SILVEIRA, Sérgio Amadeu da. **Democracia e os códigos invisíveis**: como os algoritmos estão modulando comportamentos e escolhas políticas. São Paulo: Edições Sesc, 2019. p. 30.
[218] *Ibidem*.
[219] MAGRANI, 2019.
[220] GUTIERREZ, Andriei. É possível confiar em um sistema de inteligência artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de accountability. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.
[221] *Ibidem*.
[222] CURSO de inteligência artificial para todos – aula 1. Apresentado por Diogo Cortiz. [*S. l.*: *s. n.*], 2020. 1 vídeo (38 min). Publicado pelo canal Diogo Cortiz. Disponível em: https://www.youtube.com/watch?v=Ze-Q6ZNWpco&ab_channel=DiogoCortiz. Acesso em: 30 jan. 2023.
[223] *Ibidem*.
[224] *Ibidem*.

a técnica de aprendizado específico, na qual a máquina aprende por métodos estatísticos — isso se chama de aprendizado da máquina (*machine learning*). Nessa técnica, cria-se um código, ou seja, um programa que poderá aprender com a inserção dos dados, bem como com os dados de saída. Nesse modelo, a saída, isto é, o resultado, consiste em uma classificação[225]. Além disso, os principais tipos de aprendizado de máquina são o supervisionado, o não supervisionado e o por reforço, embora existam outros[226].

O aprendizado supervisionado[227] utiliza uma quantidade grande de dados que estão rotulados e explicados, ou seja, os dados estão supervisionados. Por exemplo, para saber se houve uma fraude, primeiro se faz uma rotulação que define o que é fraude em cada caso.

Por outro lado, quando se dispõe de dados ou informações, mas não se sabe o que é fraude em cada caso, se está diante de um aprendizado não supervisionado[228]. Nesse caso, pode-se fazer uma segmentação, ou seja, agrupar informações, por exemplo, dizer que em determinado grupo há ou não fraude.

Na aprendizagem por reforço, por sua vez, não há a necessidade de uma quantidade enorme de dados, e muitas vezes não é preciso de dado algum. Esse tipo de aprendizagem é utilizado na robótica e nos jogos, por exemplo, se há um acerto, reforça-se o aprendizado.

Portanto, quando se diz que o aprendizado da máquina resolve um problema específico, resulta-se disso um modelo para reconhecer fala, ou outro para reconhecer imagem e outro para reconhecer linguagem, por isso, não existe uma IA geral, o que existe são modelos e técnicas distintas que podem ser combinados, mas trabalhando de maneira independente[229].

No aprendizado supervisionado, por exemplo, pode-se classificar, fazer regressão e, no aprendizado não supervisionado, é possível fazer segmentação, agrupar as situações semelhantes[230]. Assim, no aprendizado da máquina não

---

[225] CURSO..., 2020.
[226] *Ibidem*.
[227] *Ibidem*.
[228] *Ibidem*.
[229] *Ibidem*.
[230] *Ibidem*.

supervisionado, não há necessidade de que seja feita uma calibragem inicial[231], haja vista que isso será desenvolvido por meio das redes neurais ou pelo aprendizado da máquina profundo (*deep learning*)[232]. Esse sistema cria padrões próprios, alheios ao raciocínio humano[233]:

> Isso é alcançado por meio da criação de uma rede de múltiplas unidades não lineares de processamento de dados que se retroalimentam de modo a imitar (de maneira rudimentar) um cérebro humano. Esses sistemas de IA são capazes de analisar um ambiente dinâmico e dele extrair correlações e padrões por si só[234].

A robótica, por seu turno, utiliza o aprendizado por reforço (tentativa e erro), por exemplo, um carro autônomo, — mas nesse caso não pode operar sem supervisão[235].

Ademais, as correlações são "[...] a probabilidade de um evento ocorrer, caso outro evento também se realize. É uma relação estatística entre tais acontecimentos"[236]. Utilizam-se estatísticas que demonstram uma realidade passada, por isso, pode-se reforçar estereótipos "[...] sem demonstrar uma relação de causalidade entre os dados fáticos e as inferências realizadas"[237]. Desse modo, é possível que aconteçam erros estatísticos, como na indevida generalização ou no uso de dados pessoais sensíveis[238].

Além disso, uma característica marcante da inteligência artificial é a opacidade. Entre os motivos para a existência de opacidade na IA estão: a proteção da propriedade intelectual ou a proteção de um segredo comercial; motivos de ordem técnica, ou seja, motivos que para se entender é necessário conhecimento técnico; divergência entre a linguagem matemática e a linguagem

---

[231] GUTIERREZ, 2019.
[232] GUTIERREZ, 2019.
[233] *Ibidem*.
[234] *Ibidem*, p. RB-6.2.
[235] CURSO..., 2020.
[236] MENDES; MATTIUZZO; FUJIMOTO, 2020, p. 432.
[237] MIRAGEM, Bruno. Sistemas de pontuação de crédito e acesso ao consumo: liberdade de contratar e proteção dos consumidores contra a discriminação injusta. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022. p. 312.
[238] *Ibidem*.

humana[239]; ou ainda questões mercadológicas, por exemplo, para evitar colocar uma empresa em desvantagem em relação à sua concorrência em caso de código aberto[240]. Nesse caso, alega-se que, se o algoritmo for aberto, as pessoas podem tentar burlar o sistema, o que poderia ser feito por questões técnicas ou não[241].

Por outro lado, há um fator a ser levado em consideração que diz respeito aos programas de computador e a possibilidade de aplicação da Lei 9.6209/1998 e da Lei 9.279/1996:

> Os programas de computador, genericamente assim considerados, recebem o tratamento equivalente às obras literárias pela legislação de direitos autorais, conforme determina o artigo 2º da Lei 9.609/1998. Dessa forma, caso os algoritmos de avaliação de crédito produzidos pelos sistemas de inteligência artificial sejam consubstanciados em programas de computador, sua autoria poderá ser registrada no Instituto Nacional de Propriedade Intelectual, com a atribuição de direitos de exploração econômica ao titular do programa, que pode ser pessoa jurídica, conforme dispõe o artigo 3º da mesma Lei 9.609/1998. Por outro lado, o modelo de avaliação de crédito poderá preencher os requisitos para ter sua patente registrada, caso os parâmetros de análise utilizados no algoritmo sejam suficientemente concretos e bem delimitados, afastada a possibilidade de registro de patentes "puramente abstratas" ou "métodos matemáticos", conforme previsto no artigo 10 da Lei 9.279/1996[242].

A LGPD menciona diversas vezes a necessária observância do segredo comercial e industrial — nessa discussão também entra a questão da propriedade intelectual. Essa discussão desenvolveu-se no sentido de que não se deveria haver a abertura dos algoritmos em virtude do direito à propriedade intelectual. Outro argumento para a não abertura é que, mesmo abertos, os algoritmos não seriam inteligíveis para a maioria das pessoas e a abertura poderia colocar em risco as pessoas que fazem parte dos bancos de dados com

---

[239] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. **Big Data & Society**, [*s. l.*], v. 3, n. 1, jan. 2016. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512. Acesso em: 29 jan. 2023.
[240] DONEDA, Danilo; ALMEIDA, Virgílio A. F. O que é a governança de algoritmos? *In*: BRUNO, Fernanda *et al*. (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. 1. ed. São Paulo: Boitempo, 2018. p. 143.
[241] *Ibidem*.
[242] GOETTENAUER, Carlos. Algoritmos de credit score, dados pessoais: um mapa regulatório para o compliance na análise de crédito. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022. p. RB-24.5.

a divulgação dos dados disponíveis. Portanto, essa opacidade pode ter como objetivo garantir vantagens concorrenciais e a segurança[243]. Neste estudo, porém, não será aprofundado o tema de propriedade intelectual.

Desenvolveu-se um estudo interdisciplinar acerca da justiça dos algoritmos. No geral, entendeu-se que a chave para esse caso é a transparência, por isso, os algoritmos devem ser continuamente testados por auditores independentes que fazem o uso de dados falsos para verificar se há enviesamento[244].

Ainda no escopo das questões relacionadas aos algoritmos, outro fator que costuma ser mencionado é o de não ser possível identificar qual o fundamento do resultado de uma decisão, uma vez que, para que seja tomada, faz-se o uso de um conjunto de regras que combinam funções matemáticas complexas[245]. Desse modo, é possível que as decisões automatizadas possam decorrer de vieses criados pelos próprios algoritmos.

De modo geral, uma das principais características do ser humano é a criatividade, a qual exige uma certa aleatoriedade que, por sua vez, tem a contribuição da intuição. Isso diferencia as decisões tomadas por pessoas daquelas feitas pelos programas de computador[246]. Os algoritmos, por sua vez, são uma criação humana e estão dentro de um contexto; são construções sociais. Além disso, é possível que os algoritmos se programem de maneira independente, ou seja, eles são capazes de aprender[247]. Em outras palavras:

> Algoritmos são fórmulas matemáticas. Basicamente, uma série de instruções colhidas de símbolos e signos que são solucionados por microprocessadores, gerando novas fórmulas, em ciclo constante de

---

[243] BURRELL, 2016.

[244] "[...] *by feeding in a set of false data to see what biases result*. [...] The Interdisciplinary Working Group on Algorithmic Justice suggests that transparency is the key. These algorithms cannot hide behind the curtain of intellectual property. For those algorithms that are like a 'black box,' independent auditors need to continually test these algorithms by feeding in a set of false data to see what biases result". FERNANDEZ, Elizabeth. Will machine learning algorithms erase the progress of the fair housing act? **Forbes**, [*s. l.*], 17 nov. 2019. Disponível em: https://www.forbes.com/sites/fernandezelizabeth/2019/11/17/will-machine-learning-algorithms-erase-the-progress-of-the-fair-housing-act/#38fa291a1d7c. Acesso em: 05 dez. 2019.

[245] SILVEIRA, 2019.

[246] KAPLAN, Jerry. **Artificial intelligence**: what everyone needs to know. Oxford: Oxford University Press, 2016.

[247] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**. São Paulo: Grupo GEN, 2020.

> inputs e outputs, com dados que são recebidos, processados pelo algoritmo, e devolvidos como resultado do processamento[248].

Nesse sentido, a governança dos algoritmos pode ser utilizada para mitigar os problemas causados por eles (como a discriminação, o enviesamento). Essa governança pode ocorrer por meios técnicos, jurídicos ou por regulamentação, para que haja uma maior transparência[249], ou seja, como no caso de cumprimento da LGPD quando do tratamento dos dados pessoais. Há autores, por seu turno, que defendem que há princípios éticos que devem estar presentes desde o desenvolvimento do sistema[250].

A governança do algoritmo, nesse sentido, deve ser feita em duas frentes concomitantemente, seja pelo setor privado que desenvolve o sistema ou por um órgão público, como a Autoridade Nacional de Proteção de Dados (ANPD):

> Para que funcione sistematicamente, essa abordagem da iniciativa privada deve ser parte da organização interna das empresas, que, ao usar algoritmos, definem os padrões que refletem o interesse público e estabelecem um processo de revisão e um órgão interno para garantir a integridade e a conformidade com valores de interesse público. Essa abordagem também pode basear-se em processos de autorregulação no âmbito da indústria como um todo, em que, por exemplo, padrões coletivos e valores de interesse público são definidos para um setor específico — conforme acontece quando a indústria automobilística define padrões de qualidade e segurança para software embarcado nos automóveis. Um órgão de supervisão específico para a indústria, capaz de assumir a forma de comitês multissetoriais, teria a incumbência de exigir de quem os cria as informações relativas aos algoritmos[251].

Por outro lado, fazer a auditoria do código-fonte pode colocar em risco a propriedade intelectual, assim como pode possibilitar o "[...] vazamento dessas chaves de acesso com potencial de colocar em risco a segurança e robustez dos sistemas compostos por esses algoritmos"[252].

Para os sistemas de aprendizagem da máquina — que por sua natureza fazem correlações que não decorrem do código em sim, mas da interação com

---

[248] FALEIROS JÚNIOR, 2021, p. 48.
[249] DONEDA; ALMEIDA, 2018.
[250] MÖKANDER, Jakob. *et al.* Ethics-based auditing of automated decision-making systems: nature, scope, and limitations. **Science and Engineering Ethics**, [*s. l.*], v. 27, n. 44, p. 1-30, 6 jul. 2021.
[251] DONEDA; ALMEIDA, 2018, p. 147.
[252] GUTIERREZ, 2019.

o ambiente externo, de maneira dinâmica[253] —, mais especificamente para os sistemas de aprendizagem de máquina supervisionados, é possível realizar auditoria e aplicar processos de *accountability*:

> Nesse caso específico, é possível que se faça um registro dos *logs* de treinamento e calibragem dos sistemas de IA. A auditoria seria focada não no código-fonte, mas nesses *logs* que são os *inputs* paramétricos desse tipo de sistemas de IA[254].

Outra possibilidade, nessa lógica, seria definir que a construção da IA e a revisão dos parâmetros sejam feitas por equipes interdisciplinares, compostas de diversidade[255].

Costuma-se criticar que a opacidade dos algoritmos é intencional e que deveria haver maior transparência[256]. Contudo, Jenna Burrell[257] explica que, no aprendizado da máquina, a representação de uma classificação é feita sem a preocupação com a compreensão humana. Isso é feito a partir do tratamento dos dados, isto é, de treinamentos, e não de acordo com a linguagem utilizada pelo ser humano. Por isso, o problema da opacidade não será resolvido com uma única ferramenta ou processo, mas com a combinação de regulamentação e auditória, seja do código ou do funcionamento do código (com o

---

[253] *Ibidem*.
[254] GUTIERREZ, 2019, p. RB-6.4.
[255] *Ibidem*.
[256] "Legal critiques of algorithmic opacity often focus on the capacity for intentional secrecy and lead to calls for regulations to enforce transparency. [...] However, the opacity of machine learning algorithms is challenging at a more fundamental level. When a computer learns and consequently builds its own representation of a classification decision, it does so without regard for human comprehension. Machine optimizations based on training data do not naturally accord with human semantic explanations. The examples of handwriting recognition and spam filtering helped to illustrate how the workings of machine learning algorithms can escape full understanding and interpretation by humans, even for those with specialized training, even for computer scientists. Ultimately partnerships between legal scholars, social scientists, domain experts, along with computer scientists may chip away at these challenging questions of fairness in classification in light of the barrier of opacity. Additionally, user populations and the general public can give voice to exclusions and forms of experienced discrimination (algorithmic or otherwise) that the 'domain experts' may lack insight into. Alleviating problems of black boxed classification will not be accomplished by a single tool or process, but some combination of regulations or audits (of the code itself and, more importantly, of the algorithms functioning), the use of alternatives that are more transparent (i.e. open source), education of the general public as well as the sensitization of those bestowed with the power to write such consequential code. The particular combination of approaches will depend upon what a given application space requires" (BURRELL, 2016, p. 10).
[257] *Ibidem*.

compartilhamento pelo usuário de sua experiência quando sofrer algum tipo de discriminação)[258].

Outra solução apresentada pela autora é a adoção de alternativas que tenham mais transparência, como o uso de código-fonte aberto (software livre), a educação das pessoas sobre o assunto[259], ou mesmo a sensibilização daqueles que desenvolvem os programas. A aplicação das ferramentas para solucionar o problema da opacidade será feita conforme a necessidade e dentro de um contexto[260].

Dessa forma, a transparência e a explicabilidade dos sistemas operacionais poderão contribuir para enfrentar o enviesamento da IA, o que pode garantir o seu pleno funcionamento e avalizar a conscientização das partes interessadas[261].

No próximo capítulo será discutida as legislações existentes que podem auxiliar nas decisões automatizadas para que não haja discriminações injustificadas e inconstitucionais.

O Brasil propôs a Estratégia Brasileira de Inteligência Artificial (EBIA), instituída pelo Ministério da Ciência, Tecnologia e Inovação (MTCI) pela Portaria n. 4.979/2014, a qual norteia as ações do Estado brasileiro para o desenvolvimento da inteligência artificial no país de maneira ética e para o uso consciente[262].

Essa estratégia abrange questões éticas que envolvem a sociedade civil, o governo e aqueles que desenvolvem a tecnologia[263]. Os princípios a serem observados no desenvolvimento da inteligência artificial são: o crescimento inclusivo, o desenvolvimento sustentável e o bem-estar; os valores centrados no ser humano e na equidade; a transparência e explicabilidade; a robustez, a

---

[258] *Ibidem*.
[259] *Ibidem*.
[260] BURRELL, 2016.
[261] SARLET *et al.*, 2022.
[262] BRASIL. Ministério da Ciência, Tecnologia e Inovação. **Estratégia Brasileira de Inteligência Artificial – EBIA**. Brasília, DF: Ministério da Ciência, Tecnologia e Inovações, 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf. Acesso em: 15 set. 2022.
[263] MAGRANI, 2019.

segurança e a proteção; e a responsabilização ou a prestação de contas (*accountability*)[264]. Tem a EBIA como objetivos:

> • Contribuir para a elaboração de princípios éticos para o desenvolvimento e uso de IA responsáveis.
> • Promover investimentos sustentados em pesquisa e desenvolvimento em IA.
> • Remover barreiras à inovação em IA.
> • Capacitar e formar profissionais para o ecossistema da IA.
> • Estimular a inovação e o desenvolvimento da IA brasileira em ambiente internacional.
> • Promover ambiente de cooperação entre os entes públicos e privados, a indústria e os centros de pesquisas para o desenvolvimento da Inteligência Artificial[265].

O marco legal da inteligência artificial no Brasil266 entrou em discussão e foi aprovado pela Câmara de Deputados Federais em 2021.

Embora já se estejam desenvolvendo máquinas que podem captar as emoções que as pessoas estão sentindo, deve-se questionar se uma máquina que utiliza lógica e equação matemáticas e estatísticas complexas atendem às necessidades e às peculiaridades do ser humano. Quando se diz que a máquina tem como objetivo agir como uma pessoa, deve-se pensar até que ponto isso é possível, pois, para que isso seja considerado possível, deve-se levar em consideração o que se entende como a atividade de pensar, raciocinar e aprender[267].

O aprendizado da máquina só é possível pois acontece a partir dos dados fornecidos à máquina. Desse modo, conclui Kaplan que a máquina tem a habilidade de imitar e encontrar correlações, padrões provenientes de estratégias obtidas de inúmeros exemplos de comportamentos dos seres humanos[268].

Questões éticas, no desenvolvimento dessas tecnologias, também devem ser observadas desde a coleta de dados para o aprendizado da máquina, que tem por fim alimentá-la para tomar decisões. Devem ser observadas também regras e princípios trazidos pela Lei Geral de Proteção de Dados, pela

---

[264] BRASIL, 2021.
[265] BRASIL, 2021, p. 7.
[266] *Ibidem*.
[267] KAPLAN, 2016.
[268] *Ibidem*.

Constituição da República, pelos direitos e deveres previstos no Código Civil, constantes no Código de Defesa do Consumidor e demais legislações.

Por conseguinte, a fim de evitar discriminações e ilegalidade no tratamento dos dados, deve-se considerar o ordenamento jurídico como um todo para se ter mecanismos para evitar discriminações, exclusões a bens de consumo e a serviços. Como explicam Bruno Lorenzetto e Amílcar Teixeira Filho[269], o mecanismo eficiente é aquele que possibilita verificar se houve a observância dos procedimentos, das leis, das regulamentações, enfim, do Direito na utilização da inteligência artificial a fim de que erros, preconceitos, discriminações sejam evitados e corrigidos ao invés de serem perpetuados.

Por isso, Mario Viola e Chiara Teffé[270] argumentam pela possibilidade de oxigenar "[...] os processos de tomada de decisão, além de incentivar configurações de privacidade personalizáveis e a possibilidade da manifestação do consentimento de forma granular"[271].

De modo geral, pode-se apontar como aspectos positivos da IA a possibilidade de decisões acuradas, eficientes, imparciais, consistentes, e de ser auditável[272].

Ordinariamente, utiliza-se muito o termo algoritmo, que pode ser conceituado da seguinte maneira: "[...] são basicamente um conjunto de instruções para realizar uma tarefa, produzindo um resultado final a partir de algum ponto de partida"[273]. As decisões automatizadas, por seu lado, utilizam algoritmos complexos. Por meio da aprendizagem automática, reorganiza-se o funcionamento interno da máquina com os dados de que dispõe para fazer a análise[274].

---

[269] LORENZETTO, Bruno Meneses; TEIXEIRA FILHO, Amilcar Cordeiro. A inteligência artificial e o direito à explicação. *In*: SCHIER, Adriana da Costa Ricardo; BITENCOURT, Caroline Müller (org.). **Direito administrativo, políticas públicas e estado sustentável**. Curitiba: Íthala, 2020. p. 97-118.
[270] VIOLA; TEFFÉ, 2020.
[271] *Ibidem*, p. 137.
[272] JUNQUEIRA, 2020a.
[273] DONEDA; ALMEIDA, 2018, p. 141.
[274] *Ibidem*.

Na busca pela justiça nos algoritmos, fazer a análise do código-fonte[275] não seria o mais indicado, uma vez que não é uma tarefa de fácil entendimento, seja pelos consumidores, seja pelos operadores do Direito[276]. Outro motivo a ser considerado é a opacidade dos algoritmos. Portanto, a fase de treinamento dos algoritmos também é relevante até mesmo para a proteção de dados pessoais.

O tema da neutralidade sempre vem à tona quando se discutem as decisões automatizadas, haja vista que o ser humano pode ser tendencioso, principalmente se tiver alguma ligação ou apego a determinado assunto. No Poder Judiciário, de modo geral, há um terceiro não interessado, imparcial, que substitui a vontade das partes quando há conflito de interesses.

Contudo, cumpre lembrar que existe uma diferença entre imparcialidade e neutralidade. Fredie Didier Jr.[277] afirma que o mito da neutralidade se funda na ideia de que o juiz é desprovido de vontade inconsciente. O autor argumenta, porém, que ninguém é neutro, haja vista que as pessoas levam em consideração as suas experiências passadas, traumas, preferências ao analisar uma determinada situação. Conclui o professor[278], então, que o juiz não deve ter interesse no litígio, e deve tratar as partes com igualdade, zelar pelo contraditório em paridade de armas — e isso é atuar com imparcialidade.

Sabe-se que a lei processual deve conter leis claras, objetivas, ainda que se tenha certo grau de subjetividade. Em algumas áreas do Direito há uma menor flexibilidade, como no Direito Penal e no Direito Processual. A mente humana, por sua vez, pode ter apagões, pode confundir detalhes do passado, pode engendrar generalizações equivocadas. Por isso, há respaldo para se questionar as decisões humanas. Desse modo, não pode ser diferente nas decisões automatizadas, na utilização de recursos de mineração de dados e perfilizações das pessoas. Em razão disso, questiona-se também o artigo 20 da LGPD quando restringe a revisão para decisões tomadas unicamente por máquinas.

---

[275] LORENZETTO; TEIXEIRA FILHO, 2020.
[276] *Ibidem*.
[277] DIDIER JR., Fredie. **Curso de direito processual civil**: introdução ao direito processual civil, parte geral e processo de conhecimento. 18. ed. Salvador: JusPodivm, 2016.
[278] *Ibidem*.

Diante disso, entende-se que uma pessoa que toma decisões pode ser falível, pode ser abatida pelo cansaço, ser corrompida, ser subordinada[279]. Nas decisões de humanos e de máquinas há vantagens, desvantagens, aspectos positivos ou negativos. Por isso, no próximo capítulo será debatido como o melhor uso da tecnologia poderá ser feito em consonância com os direitos fundamentais e o ordenamento jurídico brasileiro.

Com relação à tecnologia, o seu desenvolvimento requer a presença de pessoas, de organização técnica e social, implementando-se objetivos estipulados previamente[280]. Diante disso, o desenvolvimento de um programa de computador "[...] pode ser orientado para experiências anteriores e possíveis consequências e pode exigir seleções"[281]. Ademais, há uma seleção prévia de dados, para uma finalidade pré-estabelecida, que pode trazer preconceitos, intenções prévias que podem ser intencionais[282] ou inconscientes[283].

Desse modo, quando se desenvolve um sistema, também se está fazendo escolhas, como quais dados são relevantes para a decisão, quem compõe a equipe de desenvolvimento. Tendo em vista o monopólio no desenvolvimento da inteligência artificial — além de estar centralizados em alguns países —, deve-se questionar a diversidade[284].

---

[279] JUNQUEIRA, 2020a.
[280] HOFFMANN-RIEM, 2020.
[281] *Ibidem*, p. 54.
[282] TUNES, Suzel. Algoritmos parciais: como a inteligência artificial absorve padrões discriminatórios e o que a ciência pode fazer para evitar essas distorções. **Revista Pesquisa FAPESP**, ed. 287, [*s. l.*], jan. 2020. Disponível em: https://revistapesquisa.fapesp.br/algoritmos-parciais-2/. Acesso em: 05 fev. 2023.
[283] "Ocorre que os sistemas de inteligência artificial são alimentados por dados, e quem faz a seleção desses dados são seres humanos – que podem ser movidos por preconceitos de forma inconsciente ou intencional. Um exemplo disso foi explicitado por um estudo publicado em outubro na revista Science, liderado por um cientista da Universidade da Califórnia em Berkeley, nos Estados Unidos. Em um hospital daquele país, os pesquisadores verificaram que o algoritmo responsável por classificar os pacientes mais necessitados de acompanhamento — por estarem em maior risco — privilegiava brancos em detrimento de negros. Isso acontecia porque o sistema se baseava nos pagamentos aos planos de saúde, que são maiores no caso de pessoas que têm mais acesso a atendimento médico, e não na probabilidade de cada um ter doenças graves ou crônicas. Essa situação evidencia que a construção do algoritmo pode ser responsável pelo preconceito embutido nos resultados" (TUNES, 2020).
[284] BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

A concepção de autorregulação deve ser uma das frentes na proteção de dados pessoais, mas não a única — esse tema será visto no próximo capítulo. No Brasil, é possível que esses aspectos regulatórios caminhem juntos por se tratar de uma concepção baseada no Estado do Direito, por existir uma lei geral de proteção de dados pessoais que se aplica em todo o território nacional e pela previsão expressa de proteção de dados pessoais ser um direito fundamental.

Por isso, para Magrani[285], deve existir uma combinação entre o dever-ser e uma técnica de regulação do *design* de códigos e de arquiteturas desenvolvidas. Em suma: "O Direito, lastreado por um embasamento ético adequado, servirá como um catalizador do processamento de dados e demais materialidades tecnológicas evitando uma tecnorregulação nociva à humanidade"[286].

Outro ponto a ser considerado nessa discussão são as limitações dos algoritmos e o fato de as análises serem feitas com dados do passado e não terem a capacidade de contextualizar os fatos, principalmente quanto a injustiças. Para Jerry Kaplan[287] a inteligência artificial tem a habilidade de, com poucos dados, tomar decisões generalizadas — trata-se de um processo de generalizações[288]. Por isso, o autor explica que, para que o pensamento seja criativo, exige-se certa aleatoriedade, assim como a intuição[289], que são características o ser humano possui, diferentemente dos programas de computador. Sobre o questionamento de se as máquinas podem pensar, a resposta, segundo o autor[290], dependerá do que se entende por pensar, raciocinar, aprender.

---

[285] MAGRANI, 2019.
[286] *Ibidem*, p. 257.
[287] "Which leads me to my personal view of the meaning of AI. The essence of AI — indeed, the essence of intelligence — is the ability to make appropriate generalizations in a timely fashion based on limited data. The broader the domain of application, the quicker conclusions are drawn with minimal information, the more intelligent the behavior. If the same program that learns tic-tac-toe can learn any board gam" (KAPLAN, 2016, p. 05).
[288] *Ibidem*.
[289] "A fairly attractive and yet clearly incomplete conjecture is that the difference between creative thinking and unimaginative competent thinking lies in the injection of some randomness. The randomness must be guided by intuition to be efficient" (KAPLAN, 2016, p. 15).
[290] "(The parallel here is the ongoing debates as to whether machines can really think or just simulate thinking. And the answer is the same: it depends on what you mean)" (KAPLAN, 2016, p. 16).

Para Cathy O´Neil[291], deve-se ponderar que os algoritmos são uma projeção feita com base em dados do passado, por isso, elabora-se a repetição de ciclos. Desse modo, as máquinas por si só não fazem ajustes para que haja justiça, ou para que algo seja justo[292]. Para isso, deve haver a intervenção humana no processo de aplicação de um sistema automatizado, como uma garantia para que haja a contextualização. Assim, podem ser aplicados, nesses casos de decisões automatizadas, bom senso e justiça, que são capacidades do ser humano[293].

2.1 PERFILIZAÇÃO E BANCO DE DADOS

Há inúmeras possibilidades de coleta de dados, por causa da hiperconectividade, como por meio dos dispositivos ligados à internet (Internet das coisas – IOT)[294], redes sociais. No entanto, o fato de haver muitas possibilidades não significa necessariamente que se deve fazer uso de todas elas. As pessoas e os grupos de pessoas estão sob vigilância constante, e o uso da tecnologia é aplicado para classificá-las quanto ao seu valor econômico, político[295] ou social.

A Lei n. 13.709/2018 (LGPD) e a Lei n. 12.414/2011 (LCP) estabelecem diversas limitações e direcionamentos para que se tome cuidado no

---

[291] "But injustice persists. When automatic systems sift through our data to size us up for an e-score, they naturally project the past into the future. [...] Yet we can't count on automatic systems to address the issue. For all of their startling power, machines cannot yet make adjustments for fairness, at least not by themselves. Sifting through data and judging what is fair is utterly foreign to them and enormously complicated." O´NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crowm Publishers, 2016. p. 155.

[292] *Ibidem*.

[293] "Only human beings can impose that constraint. There's a paradox here. If we return one last time to that '50s-era banker, we see that his mind was occupied with human distortions — desires, prejudice, distrust of outsiders. To carry out the job more fairly and efficiently, he and the rest of his industry handed the work over to an algorithm. Sixty years later, the world is dominated by automatic systems chomping away on our error-ridden dossiers. They urgently require the context, common sense, and fairness that only humans can provide" (O´NEIL, 2016, p. 155).

[294] "Fazem parte desse conceito os dispositivos de nosso cotidiano que são equiparados com sensores capazes de captar aspectos do mundo real, como, por exemplo: temperatura, umidade e presença, e enviá-los a centrais que recebem estas informações e as utilizam de forma inteligente" (MAGRANI, 2019, p. 29).

[295] GANDY JR., Oscar H. **The panoptic sort**: a political economy of personal information. Colorado: Records, 1993.

processamento dos dados pessoais, bem como apresentam direitos que os consumidores podem exercer na proteção deles. Desse modo, ver-se-ão as limitações de tempo, de origem e de quais dados podem ser utilizados.

Assim, os bancos de dados das pessoas jurídicas de direito público interno serão regidos por legislação específica. A Lei Complementar n. 166/2019 alterou a Lei do Cadastro Positivo, bem como a Lei Complementar n. 105/2001, a fim de dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil.

Entre os elementos relevantes para uma decisão automatizada estão: os dados pessoais e as informações obtidas a partir deles. Em tese, para a concretização desse processo, é necessária uma quantidade enorme de dados.

A criação do perfil, por sua vez, tem propósitos distintos a depender da espécie de contrato a ser firmado. No contrato de seguro, o perfil tem visa a objetivo aferir os riscos a fim de estipular o valor pago pelo prêmio[296]. A pontuação de crédito (*credit scoring*) objetiva analisar os riscos na concessão de crédito, se o contratante adimplirá com as suas obrigações e se não está em situação de superendividamento.

Entre as hipóteses permitidas de tratamento de dados pessoais, segundo a LGPD, art. 7º, inciso X, está a sua possibilidade "[...] para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente". Além disso, o art. 12, § 2º, da mesma lei estabelece que são considerados dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. Isso significa que:

> Neste parágrafo, há a posição de que caso os dados tratados mantenham o usuário identificável, mesmo que considerando a formação de perfil comportamental, ainda assim, deverão seguir o regime de tratamento de dado pessoal. Isso significa dizer que se o processo de anonimização não for suficiente para impedir a identificação do titular, não poderão ser utilizados os benefícios legais trazidos, quando o procedimento é efetivo[297].

---

[296] BESSA, Leonardo Roscoe. **Nova lei do cadastro positivo**: comentários à lei 12.414, com as alterações da lei complementar n. 166/2019 e de acordo com a LGPD. São Paulo: Thomson Reuters Brasil, 2019.

[297] LIMA, Caio César Carvalho Lima. Capítulo II, do tratamento de dados pessoais. *In*: MALDONADO; Viviane Nóbregae; BLUM, Renato Opice. 2. ed. **LGPD**: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

A partir do tratamento dos dados é possível traçar um perfil de uma pessoa, o qual pode ser utilizado para beneficiá-la ou prejudicá-la, conceder-lhe ou não crédito, prestar-lhe ou não algum serviço. Nesse contexto, a perfilização pode ser direta, indireta, ou ainda individual ou de grupos[298]. O RGDP, no art. 4.4, define perfil como:

> [...] qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações[299].

Portanto, para o RGPD, o perfil é composto de três fatores: deve decorrer de um tratamento automatizado, ter dados pessoais e ter como objetivo avaliar os aspetos pessoais de uma pessoa singular[300]. Disso se extraem novas informações e são feitas generalizações sobre uma pessoa[301] ou grupo de pessoas.

No entanto, Doneda[302] alerta que o banco de dados não precisa, necessariamente, de um recurso de informática. Além disso, há outros modos como o processamento de dados pode ser feito, não só a partir de banco de dados, mas com a utilização de outras técnicas[303]. Entretanto, em razão da tecnologia é possível processar dados em tempo recorde. Além disso, o resultado desse processo é muito valioso para aqueles que o detêm[304].

---

[298] ZANATTA, Rafael A. F. Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção De Dados Pessoais. MARQUES, Claudia L.; MIRAGEM, Bruno; MAGALHÃES, Lucia Ancona Lopez de (org.). **Direito do consumidor** – 30 anos de CDC. São Paulo: Grupo GEN, 2020.

[299] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**. Bruxelas, Bélgica: Conselho Europeu, [2017]. Disponível em: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 16 fev. 2023.

[300] GRUPO..., 2017.

[301] MARTINS, Pedro Bastos Lobo. **Profiling na Lei Geral de Proteção de Dados**: desenvolvimento da personalidade em face da governamentabilidade algorítmica. Indaiatuba: Foco, 2022.

[302] DONEDA, 2020a.

[303] *Ibidem*.

[304] *Ibidem*.

Ademais, a distinção entre cadastro e banco de dados passou a ser diluída diante da utilização de programas de computador, algoritmos, inteligência artificial e a constante coleta de dados, contexto em que é muito difícil a pessoa exercer a sua autodeterminação informativa. Em virtude disso, Bruno Bioni[305] entende que essa taxonomia não faz muito sentido na sociedade da informação.

Portanto, assim como Bioni, neste estudo o termo “banco de dados” é usado de forma ampla[306], devido às inúmeras possibilidades de coleta de dados e de seu processamento. Para Rodotà[307], a ideia do banco de dados como um arquivo estático em um computador pode estar superada ou ser uma noção insuficiente por conta das diversas técnicas que podem ser utilizadas para o processamento de dados.

Desse modo, banco de dados é onde se armazenam as informações sobre a pessoa, as quais são obtidas a partir dos seus dados; esse conjunto de informações é organizado conforme uma determinada lógica[308]. Bioni[309], por seu turno, explica que os bancos de dados não são somente onde se armazenam os dados de entrada (*input*), mas também onde é feito o processamento de dados que entrega uma informação (*output*). Esse gerenciamento, no que lhe toca, pode ser feito de maneira manual ou automatizada[310].

A despeito disso, Milena Oliva e Francisco Viégas[311] salientam que, embora o *credit scoring* não seja tecnicamente um banco de dados, nele aplicam-se fórmulas estatísticas que se servem de dados pessoais.

Nesse sentido, um ponto importante para o sucesso do processamento de dados se relaciona com a origem e a qualidade dos dados que são utilizados

---

[305] BIONI, 2020a.
[306] *Ibidem*.
[307] RODOTÀ, 2008.
[308] DONEDA, 2020a.
[309] BIONI, 2020a.
[310] BIONI, 2020a.
[311] OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. Tratamento de dados para a concessão de crédito. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

pelas fórmulas[312]. O´Neil[313], então, explica que a mensuração da qualidade dos dados, para os cientistas de dados, refere-se a se há dados suficientes para testar a máquina, se os números representam o que se espera ou são aleatórios. Além disso, afirma que a comunidade técnica deve atuar no sentido de os dados representarem o mundo de maneira efetiva e abrangente[314].

Ademais, há também aquele que detém o banco de dados, que o gerencia e compartilha as informações para terceiros, como os órgãos de proteção ao crédito[315], como se vê nos exemplos a seguir.

A Lei n. 8.078/1990 (Código de Defesa do Consumidor), no art. 43, tratou do assunto dos Bancos de Dados e Cadastros de Consumidores. Foi, desse modo, uma das primeiras legislações a serem utilizadas para a proteção de dados pessoais. De acordo com Doneda, esse art. 43 do CDC, ao ser elaborado, foi inspirado pela legislação dos Estado Unidos que trata da proteção de crédito, chamada de *Nacional Consumer Act*, e pelo *Fair Credit Reporting Act* (FCRA) da década de 70[316].

Uma seguradora também pode usar banco de dados, "[...] o que equivale a dizer que o segurador e o gestor de um banco de dados compartilhado pelo mercado devem reger o tratamento dos dados pessoais dos segurados/consumidores conforme esses preceitos"[317]. Desse modo, os dados que componham os bancos devem ser:

> Objeto de um tratamento leal e lícito, sejam adequados pertinentes e não excessivos em relação à finalidade declarada, além de serem objetivos, exatos e atualizados. Tal princípio enseja cautela na formação do banco de dados, assim como demanda a sua constante atualização, de forma a impedir que os dados contidos restem ultrapassados com o passar do tempo[318].

---

[312] *Ibidem*.
[313] "When data scientists talk about 'data quality', we're usually referring to the amount or cleanliness of the data — is there enough to train an algorithm? Are the numbers representing what we expect or are they random?" (O´NEIL, 2016, p. 199).
[314] "The technical community is to blame as well, and we have work to do. We need to ensure that data effectively and comprehensively represents the world—even, we hope, bears witness to the world and its suffering, rather than shaping the world—especially in ways that exacerbate misery" (O´NEIL, 2016, p. 199).
[315] BIONI, 2020a.
[316] DONEDA, 2020a.
[317] JUNQUEIRA, 2020a, p. RB-1.6.
[318] MENDES, 2014, p. 72.

A própria LGPD, em seu art. 6º, inciso V, elenca como princípio a qualidade dos dados, que consiste na garantia, aos titulares, da exatidão, da clareza, da relevância e da atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Há outros direitos previstos nos art. 5º e 18 da LGPD que contribuem para a qualidade dos dados[319]:

> Art. 5º - XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> Art. 5º - XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> Art. 5º - XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> Art. 18 - III - correção de dados incompletos, inexatos ou desatualizados;
> Art. 18 - IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

Por isso, enquanto estiverem armazenados e poderem ser utilizados para as decisões automatizadas, o titular deve ter acesso a eles e ter a possibilidade de retificá-los, assim como pode atualizá-los. Sobre o papel dos bancos de dados, além de servir como agrupamento lógico, objetivam extrair informações:

> Por isso, os bancos de dados não são somente um agrupamento lógico e interrelacionado do estado primitivo da informação, mas são, também, um ferramental que deve criar uma interface para quem manipula analisar e descobrir informações para tomada de decisões[320].

De acordo com a LCP, art. 2º, inciso I, o banco de dados consiste em um conjunto de dados que pode dizer respeito à pessoa natural ou à pessoa jurídica. Esses dados são armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro. Portanto, pode, o banco de dados, ter como objetivo a concessão de crédito, a venda a prazo, transações comerciais e empresariais e a análise de risco financeiro.

---

[319] MIRAGEM, 2020.
[320] BIONI, 2020a, p. 34.

O banco de dados deve ser alimentado com dados objetivos que visem à proteção de crédito ou a concessão de crédito. De acordo com a legislação consumerista, os cadastros de consumo tinham finalidades mais restritas, como a promoção de ofertas e o direcionamento de produtos ou serviços, e deveriam ter autorização dos consumidores para atingirem esse objetivo[321].

Entre as finalidades do setor de birôs de crédito, estão a de verificar a probabilidade de adimplemento de uma dívida. Desse modo, a pessoa é alocada em uma certa categoria de risco de modo a fundamentar as decisões quanto à concessão de crédito, à taxa de juros a ser fixada e até sobre à eventual conclusão do contrato[322]. Pode-se citar outras motivações, tais como:

> (1) melhora da avaliação dos riscos de eventual inadimplência do tomador de empréstimo;
> (2) possibilidade de se estabelecer uma taxa de juros menor para o consumidor como um bom histórico creditício;
> (3) constituição de "dispositivo" de disciplina do consumidor;
> (4) educação do comportamento do consumidor, evitando situações de superendividamento[323].

Além disso, as bases de dados podem identificar padrões de comportamento e fazer previsões deles com base nas informações obtidas[324]. Os cadastros de consumo, por sua vez, visam a promover ofertas, promoções ou direcionar um tipo de oferta de produtos ou serviços, e devem ter autorização dos consumidores para tanto[325].

A LGPD define banco de dados como o "[...] conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico" (art. 5º, inciso IV) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A criação de perfis é feita a partir da coleta e da mineração dos dados (*data mining*), em que se faz uso de estatísticas que, dentro de uma

---

[321] *Ibidem*.
[322] ITS. **Transparência e governança nos algoritmos**: um estudo de caso sobre o setor de birôs de crédito. Rio de Janeiro: ITS, 2017.Disponível em: https://itsrio.org/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf. Acesso em: 29 jan. 2023.
[323] BESSA, 2019, p. 38.
[324] BIONI, 2020a.
[325] BIONI, 2020a.

racionalidade, etiquetam indivíduos a partir de características[326]. Nesse sentido, a mineração de dados:

> [...] 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[327].

A mineração de dados é utilizada no *credit scoring* (*crediscore*)*,* ou seja, para formar a pontuação de crédito do consumidor; além disso, a mineração pode fixar os prêmios de seguros[328], por exemplo. Essa técnica utiliza banco de dados e programas de computador e a ela se aplica o princípio da transparência e da finalidade, pois não se pode violar o princípio fundamental da igualdade[329]: "Nesse sentido, pode-se inferir que nesse aspecto reside um risco dessa técnica, uma vez que, ao facilitar a classificação e a segmentação, ela pode gerar análises discriminatórias, violando o direito à igualdade"[330].

Antes da Lei n. 12.414/2011 (Lei do Cadastro Positivo), entendia-se no geral pela possibilidade de utilização do sistema de pontuação de crédito. O Superior Tribunal de Justiça interpretou dessa maneira a partir do artigo 5º, inciso IV e pelo art. 7º, inciso I, da Lei n. 12.414/2011. Esse entendimento encontrava-se na Súmula de n. 550:

> A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. (Súmula 550, SEGUNDA SEÇÃO, julgado em 14/10/2015, DJe 19/10/2015).

---

326 MEDON, Filipe. Decisões automatizadas: o necessário diálogo entre a inteligência artificial e a proteção de dados pessoais para a tutela de direitos fundamentais. *In*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O Direito Civil na era da inteligência artificial**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.
327 DONEDA, 2020a, p. RB-2.6.
328 MEDON, 2020.
329 MENDES, 2014a.
330 *Ibidem*, p. 109-110.

Esse entendimento está corroborado pela jurisprudência em teses do Superior Tribunal de Justiça de n. 42, Direito do Consumidor II, item 1, assevera que:

> 1) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do Código de Defesa do Consumidor - CDC e da Lei n. 12.414/2011. (Tese julgada sob o rito do art. 543-C do CPC/1973 - TEMA 710).

Nessa esteira, Carlos Costa[331] argumenta que, embora a Lei do Cadastro Positivo tenha sido "[...] clara sua aplicabilidade tão somente a negócios (ou transações) comerciais, como parte da análise dos dados para 'finalidade de concessão de crédito', a Lei abrange":

> [...] os negócios comerciais que envolvam crédito, como a compra e venda a prazo de bens de consumo (crediário), o financiamento bancário, imobiliário ou mobiliário, consórcio, capitalização, previdência privada, seguros, leasing, descontos, abertura de contas correntes, contrato de cartão de crédito, e também a prestação de serviços, principalmente quando contínua no tempo[332].

Portanto, segundo o autor, os dados e as informações sobre as pessoas poderão propiciar a realização de negócios a prazo[333].

A LCP objetiva facilitar a concessão de crédito e a oferta de juros mais vantajosos para os contratantes. Como esclarece Bessa, atribui-se ao cliente uma pontuação que leva em consideração o risco na concessão do crédito, com base no "[...] tipo da situação normal, risco de atraso, risco de perda, o banco de dados emite opinião sobre os riscos de um negócio específico"[334]. Todavia, ainda não há um padrão mínimo expresso de quais dados podem ser coletados[335], haja

---

[331] COSTA, Carlos Celso Orcesi D. **Cadastro positivo**: lei n. 12.414/2011: comentada artigo por artigo. São Paulo: Editora Saraiva, 2012. p. 14.
[332] *Idem*.
[333] *Ibidem*.
[334] BESSA, 2019, p. 111.
[335] IDEC. Cadastro positivo acolhe sugestões do IDEC, mas mantém pontos críticos. **IDEC**, [*s. l.*], 26 jul. 2019. Disponível em: https://idec.org.br/noticia/cadastro-positivo-acolhe-sugestoes-do-idec-mas-mantem-pontos-criticos. Acesso em: 29 jul. 2019.

vista que caberá a quem coleta os dados definir aquilo que é relevante para a sua atividade.

Em 24 de julho de 2019 entrou em vigor o Decreto n. 9.936/2019, que regulamenta a Lei n. 12.414/2011, e disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação do histórico de crédito. Por seu turno, essa lei possibilita à pessoa o exercício da autodeterminação informativa, pois pode exercer controle de suas informações[336].

Essa legislação também se coaduna com os fundamentos da República Federativa do Brasil, como a livre iniciativa, ao propiciar o acesso ao crédito para a abertura de empreendimentos (art. 1º, inciso IV). Laura Mendes define o sistema de avaliação (*scoring*) como:

> O sistema de avaliação [que] objetiva identificar os consumidores que têm maior valor para a empresa, para que esses sejam os alvos de promoções e estratégias de fidelização de clientes. Isto é, a empresa tem interesse em identificar os "melhores consumidores" para que possa construir com eles uma relação duradoura, garantindo vantagens competitivas e manutenção dos níveis de lucratividade. Além disso, o sistema de avaliação tem como finalidade dimensionar os riscos de contratação indicando quais consumidores apresentam "menor risco" de inadimplência. Como é de se esperar, a identificação dos melhores também pressupõe a identificação daqueles considerados os "piores consumidores". Esses são aqueles para quem as empresas têm interesse de oferecer as piores ofertas ou nenhuma oferta. Ademais, esses podem ter o seu acesso a bens e serviços negado, em razão da sua classificação como um consumidor "ruim"[337].

Renato Monteiro e Sinuhe e Cruz, por sua vez, definem pontuação de crédito (*credit scoring*) como:

> [...] uma metodologia que objetiva auxiliar os tomadores de decisão a inferir o grau de risco de inadimplência de um determinado tomador de crédito. Com base no emprego de algoritmos e da utilização de técnicas de análise estatística, realiza-se o cruzamento dos dados pessoais ('*inputs*') de determinado consumidor que, uma vez categorizados, valorados, combinados e comparados, dão origem a uma pontuação ('*output*') capaz de representar o risco de perda ou de inadimplência associado àquele indivíduo[338].

---

[336] BIONI, 2020a.
[337] MENDES, 2014, p. 54.
[338] MONTEIRO, Renato Leite; CRUZ, Sinuhe Nascimento e. Desafios da transparência e direito à informação no desenvolvimento de algoritmos de *credit scoring*: uma análise sob a ótica do

As contratações visam ao cumprimento das obrigações que contribuem para a segurança jurídica, isto é, a segurança das relações, e isso possibilita que juros possam ser reduzidos. Como se sabe, o Brasil tem como característica ter juros altos[339]. Muito se discutiu sobre a possibilidade de juros sobre juros e o Supremo Tribunal Federal pacificou essa questão; além disso, o art. 192 da Constituição da República de 1988[340],§3º, que limitava os juros, teve nova redação. Porém, não é objetivo deste trabalho aprofundar o tema dos juros, haja vista que é um assunto complexo e cabem às medidas econômicas tomadas pelo Poder Público, pelo Banco Central e pelo setor financeiro.

Entretanto, os consumidores são vulneráveis. Assim, existe a hipossuficiência técnica do consumidor, que fica à mercê dessa situação, ainda mais pela regra usada ser o *opt in*, na LCP, ou seja, a pessoa é inscrita como participante do banco de dados do *score* e pode optar em retirar-se. Essa comunicação ao cadastrado é feita (LCP, art. 4, §4º):

> I - ocorrer em até 30 (trinta) dias após a abertura do cadastro no banco de dados, sem custo para o cadastrado;
> II - ser realizada pelo gestor, diretamente ou por intermédio de fontes; e
> III - informar de maneira clara e objetiva os canais disponíveis para o cancelamento do cadastro no banco de dados.

A abertura pode ser feita mediante cláusula contratual[341], segundo o Código do Consumidor, art. 54, §4º.

Verifica-se que o modelo adotado pela LCP é o do *opt out*, ou seja, a criação do cadastro positivo não precisa de autorização do cadastrado, mas ele tem o direito de solicitar seu cancelamento ou reabertura (art. 5º, inciso I). Por

---

devido processo informacional. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022. p. 164.

339 FALLA, Naty. Brasil tem a 3ª maior taxa de juros do mundo; confira o *ranking*: levantamento mostra que país fica atrás apenas de Argentina e Turquia. **Forbes Money**, [*s. l.*], 16 ago. 2022. Disponível em: https://forbes.com.br/forbes-money/2022/08/brasil-tem-a-3a-maior-taxa-de-juros-do-mundo-confira-o-ranking/. Acesso em: 07 fev. 2023.

340 Redação anterior: "§ 3º As taxas de juros reais, nelas incluídas comissões e quaisquer outras remunerações direta ou indiretamente referidas à concessão de crédito, não poderão ser superiores a doze por cento ao ano; a cobrança acima deste limite será conceituada como crime de usura, punido, em todas as suas modalidades, nos termos que a lei determinar".

341 CDC: "Art. 54, § 4° As cláusulas que implicarem limitação de direito do consumidor deverão ser redigidas com destaque, permitindo sua imediata e fácil compreensão".

outro lado, para a disponibilização do histórico aos consulentes, é necessária prévia autorização[342], caso contrário somente será possível disponibilizar a pontuação[343]. Essa disposição está de acordo com a LGPD, art. 8º:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

Não será necessária a realização dessa comunicação quando o cadastrado já tenha cadastro aberto em outro banco de dados (art. 4º, § 5º). Determina a referida lei que as informações constantes no cadastro somente poderão ser disponibilizadas aos consulentes 60 (sessenta) dias após a abertura do cadastro (art. 4, § 7º). Poderão ter acesso a essas informações somente consulentes que com ele mantiverem ou pretenderem manter relação comercial ou creditícia (art. 15, LCP).

---

[342] "[...] abusividade de cláusulas insertas em contrato de cartão de crédito. Precedentes. 3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento. 4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança. 5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada. 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição. 7. Considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão. 8. Não se estende a abusividade, por óbvio, à inscrição do nome e CPF de eventuais devedores em cadastros negativos de consumidores (SPC, SERASA, dentre outros), por inadimplência, uma vez que dita providência encontra amparo em lei (Lei n. 8.078/1990, art. 43 e 44). [...] 11. Recurso especial parcialmente provido". BRASIL. Superior Tribunal de Justiça (4. turma). **Recurso Especial n. 1348532/SP**. Consumidor. Cerceamento de defesa. Não ocorrência. Contrato de cartão de crédito. Cláusulas abusivas. Compartilhamento de dados pessoais. Necessidade de opção por sua negativa. Desrespeito aos princípios da transparência e confiança. Abrangência da sentença. *Astreintes*. Razoabilidade. Recorrente: HSBC Bank Brasil. Recorrido: Associação Nacional de Defesa da Cidadania e do Consumidor. Relator: Ministro Luis Felipe Salomão, 10 out. 2010. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/526809457/inteiro-teor-526809464. Acesso em: 30 jan. 2023.

[343] OLIVA; VIÉGAS, 2020.

Nesse sentido, alguns questionamentos surgem, por exemplo, como esses dados são adquiridos, como são armazenados e tratados, pois podem não só colocar em risco a privacidade, mas implicar discriminações. A referida lei definia que, em caso de discordância do *score*, a pessoa poderia impugnar, ou seja, requerer a revisão de decisão quando ela tiver sido realizada exclusivamente por meios automatizados (art. 5º, VI).

Além do mais, deve ser considerada a realidade brasileira, que tem uma economia que está em constante altos e baixos, pois é continuamente afetada por crises financeiras internas, externas e, mais recentemente, pela Pandemia de COVID-19, que teve início em 2020[344]. Assim, há uma população enorme que está ingressando na sociedade de consumo e que pode vir a se consolidar nela.

Ainda dentro do contexto brasileiro, há que se questionar como as pessoas exercerão esse direito à informação, à explicação, tendo em vista o grau de compreensão das implicações que acarretam bancos de dados como esses, o nível de escolaridade, e a urgência para suprir necessidades urgentes e imediatas da sua família.

A Lei n.12.414/2011 disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, e a esse tema também se aplica o Código de Defesa do Consumidor. No entanto, à LCP aplicam-se as informações de adimplemento, ou seja, positivas; não obstante isso, quando feito o tratamento de dados, não há como se diferenciar informações positivas das negativas[345], haja vista que se objetiva fazer um retrato fiel do histórico da pessoa[346].

O CDC (art. 43), por sua vez, aborda as informações negativas, cadastros negativos, assim como todo e qualquer dado pessoal referente ao consumidor[347]. Esses dois sistemas funcionam em paralelo[348]. No referido artigo,

---

[344] UNA-SUS. Organização Mundial de Saúde declara pandemia do novo coronavírus. **UNA-SUS**, [*s. l.*], 11 mar. 2020. Disponível em: https://revistapesquisa.fapesp.br/algoritmos-parciais-2/. Acesso em: 17 fev. 2023.
[345] OLIVA; VIÉGAS, 2020.
[346] *Ibidem*.
[347] BIONI, 2020a.
[348] COSTA, 2012.

o CDC possibilita ao consumidor o controle dos seus dados, pois ele deve ter "[...] acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes".

Além disso, de acordo com o CDC, se não houver a solicitação da "abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor", art. 43, §2º, CDC. Diante disso, o CDC "[...] buscou conferir a autodeterminação informacional, o que perpassa desde regras para garantir a exatidão dos dados até limitações temporais para o seu armazenamento"[349].

De acordo com o CDC, os bancos de dados e cadastros, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público (art. 43, § 4º). Trata-se de uma garantia, assim como "[...] aproxima o interesse público da atuação das entidades arquivistas"[350].

A LGPD assegura o direito do titular dos dados à obtenção de informações com o controlador[351] (art. 18), tais como: confirmação da existência da realização de tratamento de dados, acesso aos dados, correção dos dados incompletos, inexatos e que estejam desatualizados. Além disso, garante a eliminação de dados desnecessários, excessivos ou que tenham sido tratados em desconformidade com a legislação. Como esse direito pode ser efetivamente exercido será abordado no Capítulo 3.

A LCP define o histórico de crédito como o conjunto de dados financeiros e de pagamentos relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica (art. 2º, inciso VII). Costa explica que o termo "histórico" abrange não só informações positivas do consumidor, mas todo o seu histórico, seja positivo ou negativo[352].

Há uma nítida assimetria de informações entre aquele que coleta os dados e faz o processamento (ainda que contrate uma empresa que o faça, ou seja,

---

[349] BIONI, 2020a, p. 122.
[350] OLIVA; VIÉGAS, 2020, p. 567.
[351] LGPD: "Art. 5º, inciso VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".
[352] COSTA, 2012.

que venha a ter acesso somente à pontuação) e o titular dos dados. O primeiro tem mais informações que o segundo, que, por sua vez, tem mais dificuldade para saber quais dados foram utilizados, como foram e se foi possível extrair informações sensíveis — portanto, há uma situação em que existe um desequilíbrio de poder e de informação nessa relação.

Se informação é poder, ela também pode ser considerada uma forma de capital para quem a detém[353]. E pode-se dizer que essa desigualdade de poder entre esse e o titular de dados supera, atualmente, a daquele que irá conceder o crédito ou realizar o contrato de seguro, por exemplo.

> Portanto, o problema da privacidade hoje é causado pelo conflito consequente da assimetria de poderes existente entre os titulares de dados e aqueles que realizam o tratamento dos dados. Esta assimetria gera um desequilíbrio social que, por sua vez, leva à violação dos princípios da igualdade e da liberdade. Proteger de maneira rigorosa os dados pessoais sensíveis se torna, assim, instrumento para a efetivação da igualdade e da liberdade[354].

Ademais, a regra é o *opt in*, ou seja, a pessoa é inscrita como participante do banco de dados do *score*, mas poderá optar em cancelar. No entanto, ao fazer isso, pode reduzir as suas chances de conseguir uma contração ou isso pode afetar a taxa de juros.

Interessante notar que a LCP, art. 7º-A, dispõe que não podem ser utilizadas informações de pessoas que não tenham relação de parentesco de primeiro grau com o cadastrado ou de dependência econômica[355]. O que se pode entender é que a situação financeira a ser analisada leva em consideração a relação de parentesco até o primeiro grau. Assim, para essa legislação, a relação familiar pode afetar a adimplência daquele que adquire crédito[356]. Contudo, qual a real justificativa para se utilizar tal informação, haja vista que esse terceiro, ainda que parente, possa ser um devedor contumaz[357], ou não ter o mesmo estilo

---

353 GANDY JR., 1993.
354 MULHOLLAND, 2018, p. 177.
355 Lei n. 12.414/2011: “Art. 7-A, II - de pessoas que não tenham com o cadastrado relação de parentesco de primeiro grau ou de dependência econômica; e para que se restrinja a utilização ilimitada de informações, ainda que, estejam disponíveis, há as limitações previstas na LGPD como os seus princípios e as normas do CDC e da LCP”.
356 BESSA, 2019.
357 BIONI, 2020a.

de vida, e os dois serem pessoas com realidades econômicas diversas, ou até mesmo nem terem relações próximas, mesmo que tenham um parentesco de primeiro grau (pais e filhos) — portanto, por que essas informações poderão ser consideradas na composição da pontuação[358]?

Porque pode acontecer de essas pessoas dependerem economicamente uma da outra, a depender da situação concreta. Desse modo, caberá o questionamento dessa informação, se utilizada para prejudicar o cadastrado quando essas pessoas não tenham uma relação próxima, por exemplo. Bioni entende que essa informação de terceiros parentes não deveria ser levada em consideração em relação àquele que terá acesso a crédito:

> i) excepciona-se, contudo, o caso de terceiros que com ele mantenha relação de parentesco de primeiro grau ou dependência econômica, hipótese na qual a disseminação de tais informações externas, não diretamente vinculadas à pessoa avaliada, poderia agregar na análise de seu crédito. Ainda assim, há o ônus argumentativo do porquê tais exceções seriam aplicáveis por parte de quem processará tais informações excepcionadas por tal regra proibitivas.
> ii) com isso, por exemplo, de nada adiantará argumentar pura e simplesmente que a informação utilizada é o do genitor ou do filho do avaliado, senão for de, demonstrada qual é a sua pertinência com a análise de crédito realizada. Caso contrário, uma pessoa com uma histórico de crédito extremamente positivo poderia ser prejudicada pelo único fato de um terceiro, com qual mantém primeiro grau de parentesco, ser um devedor contumaz[359].

Como já mencionado, não há um critério objetivo explícito na lei quanto a quais e como as informações podem ser coletadas pelas entidades de proteção ao crédito[360]. Na atual sociedade em que vivemos, é muito fácil utilizar redes sociais para a coleta de informações pessoais, até porque muitos dos serviços prestados são pagos pelas próprias pessoas com os seus dados ou com a utilização de aplicativos que poderão armazenar muitas informações colhidas de um celular ou de um computador utilizado para fazer transações.

Interessante notar que o art. 4º, inciso III e o art. 9º, *caput* da LCP, estabelecem que é possível que o gestor compartilhe informações cadastrais e

---

[358] BESSA, Leonardo Roscoe. Responsabilidade civil e limites normativos para o tratamento de dados do consumidor na pontuação de crédito. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022.
[359] BIONI, 2020a, p. 213.
[360] BESSA, 2019.

de adimplemento com outros bancos de dados. Por isso, o titular deve ter muito cuidado ao expor certas informações e dados pessoais. Ademais, sempre devem ser observadas as regras expressas e claras para a sua coleta previstas na legislação.

A utilização de dados estatísticos é feita há muito tempo para prever o comportamento humano a fim de evitar risco, técnica essa que é útil e importante para o desenvolvimento da sociedade. Carlos Costa[361] explica que, durante mais de 50 (cinquenta) anos, os cadastros negativos dos consumidores e das empresas eram classificados tão somente em duas genéricas categorias: aptos e inaptos. Desse modo, havia um vácuo em relação aos aptos, pois os cadastros os tinham como iguais, não os distinguindo. Por isso:

> Se a informação usual restringia-se a negativações, mesmo quando o consumidor se reabilitava, considerando ser vedado revelar "informações pregressas" ou "antigas restrições", não havia como avaliar a maior ou menor probabilidade de futuro ou novo inadimplemento. O argumento favorável mais invocado pelos defensores do cadastro positivo é a possibilidade de analisar os dados, de separar o joio do trigo, distinguir as várias tonalidades de cores entre os extremos do branco e do preto[362].

A necessidade dos serviços não pode seguir a lógica do tudo ou nada, em outras palavras, binária, em que só pode se aceitar ou não se aceitar as condições impostas, pois, a depender do serviço ou produto, a pessoa não poderá adquiri-los, ainda mais se não puder questionar.

Carlos Costa atenta-se para o fato de que a lei não proíbe expressamente e de maneira específica a possibilidade de obter dados disponíveis por meio de entrevistas concedidas, palestras, negócios em andamento[363]. Sabe-se que a

---

[361] COSTA, 2012.

[362] *Ibidem*, p. 31.

[363] "Por outro lado, não está proibido que os birôs se sirvam de outras fontes para a obtenção de dados, não relativas a negócios. Por exemplo, advindos de fontes tais como entrevistas, participações em seminários, títulos (p. ex., professor universitário), livros, balanços de empresas, negócios em andamento (p. ex., a Vale tentando adquirir a Xstrata suíça). Afinal, dados pessoais são "qualunque informazione relativa a persone identificabili, anche indiretamente mediante un riferimento ad qualsiasi altra informazione", considerando-se dado anônimo "quello non associabile ad un interessato identificabile" (Antonino Attanasio, La tutela della privacy, cit., p. 49). Qualquer tipo de informação ou de obrigação pode ser incluído, não apenas as advindas de negócios concretos, como notícias da imprensa, qualificação e títulos do pretendente ao crédito (por exemplo, uma grande empresa tentando financiar a incorporação de

China tem utilizado informações sociais para compor os bancos de dados, o que se chama de Sistema de Crédito Social[364]. Na Polônia, utilizam-se os perfis para a assistência social aos desempregados[365].

Quanto à análise do histórico das informações, surgem alguns questionamentos, tais como: qual será a limitação do prazo anterior da formação da relação jurídica para a utilização dos dados e, posteriormente, os que tiverem sido coletados poderão ficar armazenados por aquele que faz o tratamento dos dados por quanto tempo? Quanto tempo leva para que uma pessoa possa reabilitar as suas informações negativas? Se a quitação de uma obrigação não torna imediata a reabilitação, o novo processo de avaliação levará em consideração o conjunto do comportamento de uma pessoa? Afinal, a quitação de uma dívida não leva, necessariamente, ao acesso imediato ao crédito, uma vez que se trata de uma análise de risco. Portanto, será analisado um comportamento provável no futuro[366].

A LCP determina que a manutenção de tais informações de adimplemento não podem ser mantidas por prazo superior a 15 (quinze) anos (art. 14). Contudo, o CDC[367], no art. 43, §1º, estabelece que os cadastros negativos, isto é, os que contêm informações negativas, não poderão ser superiores a 05 (cinco) anos. Aplica-se esse mesmo prazo para a negativação no nome do consumidor no Serviço de Proteção ao Crédito, dessa forma, após esse prazo deve ser cancelada a negativação[368].

---

outra), imagem pública etc., desde que tenham interesse para avaliar a situação econômica do cadastrado e não envolvam dados privados (§ 3° do art. 3°)" (COSTA, 2012, p. 31).

[364] OLIVA; VIÉGAS, 2020.

[365] *Ibidem*.

[366] COSTA, 2012.

[367] Art. 43. [...] § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

[368] BRASIL. Superior Tribunal de Justiça (4. Turma). **Recurso Especial n. 22337/RS**. Serviço de proteção ao crédito. Cancelamento do registro. Prazo (cinco anos). O registro de dados pessoais no SPC deve ser cancelado após cinco anos. Art. 43, § 1º, do Código de Defesa do Consumidor (lei 8.078/90). Recorrente: Clube de Diretores Lojistas de Passo Fundo-RS. Recorrido: José Orivaldo Moreira Branco. Relator: Ministro Ruy Rosado Aguiar, 13 fev. 1995. Disponível em: https://jurisprudencia.s3.amazonaws.com/STJ/IT/RESP_22337_RS_1313696547418.pdf?AWSAccessKeyId=AKIARMMD5JEAO67SMCVA&Expires=1682995976&Signature=5%2FKYSv5n5HYCiGNN1hjtAHa3c80%3D. Acesso em: 15 set. 2022.

Nesse contexto, Bessa[369] sugere que a melhor interpretação seria contar a partir da data do vencimento da dívida em consonância com o entendimento do Superior Tribunal de Justiça em relação à inscrição em banco de dados de inadimplência. Ainda assim, não há muita segurança, tendo em vista que há dívidas que são pagas de forma parcelada. Bruno Miragem lança o seguinte questionamento: é possível utilizar dívidas prescritas na análise com a finalidade de melhorar a nota?[370].

Como a LGPD não define um prazo para que dados passados possam ser utilizados, a depender da decisão a ser tomada, será razoável utilizar determinado dado ou informação do passado ou não, sempre norteando-se pelos princípios da finalidade, da necessidade e da adequação (art. 5º, LGPD). Todavia, em muitos casos já se aplicou o Código de Defesa do Consumidor, ainda que haja lei específica em sentido contrário, em razão da teoria do Diálogo das Fontes. Bessa faz a seguinte reflexão:

> Fica claro pela leitura do dispositivo que o acesso ao crédito é algo positivo: as informações relativas a dívidas prescritas não devem ser divulgadas para não serem consideradas nas análises de concessão de crédito. [...] Nesse contexto, as informações *positivas* devem ser compreendidas *em contraste* com os dados caracterizadores de dívidas vencidas e não pagas: qualquer dado além das informações necessárias para identificar um débito vencido e não pago pode ser classificado como *informação positiva*[371].

De acordo com LCP (art. 3º, §1)[372], as informações devem ser objetivas e sem juízo de valor. Poderá ocorrer, por exemplo, que uma pessoa com informações positivas tenha o seu crédito negado para não contrair mais uma dívida e estar em situação de superendividamento[373]. O inadimplemento ou o atraso podem ser considerados negativos, cada sistema estipula o critério[374]. Desse modo, o atraso pode não ser considerado negativo se for visto o

---

[369] BESSA, 2019.
[370] MIRAGEM, 2022.
[371] BESSA, 2019, p. 33-34.
[372] LCP: “Art. 3º, § 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado”.
[373] BESSA, 2019.
[374] *Ibidem*.

comportamento como um todo do consumidor[375]. Em suma, esses critérios serão considerados por aquele que faz o processamento de dados.

O perfil tem como objetivo obter informações de gostos, hábitos de consumo, preferências, padrões de comportamento[376]. Por conseguinte, a perfilização (*profiling*) resulta de dados dos pessoais. Esse perfil, por sua vez, serve de base para a tomada de decisões a partir de estereótipos e de conteúdos que foram acessados na internet, por exemplo[377].

Os perfilamentos são criados pelo controlador a fim de avaliar e tomar uma decisão automatizada. Desse modo, são geradores de grandes preocupações, haja vista a potencialidade de discriminações[378] e de invasão de privacidade, muitas delas já demonstradas na prática, como ver-se-á a seguir.

Como seu objetivo é obter uma imagem detalhada do consumidor, o perfil expressa uma imagem sobre a personalidade[379], e a mineração de dados possibilita analisar comportamentos anteriores e prever possíveis comportamentos futuros. À vista disso, as pessoas estarão sujeitas a decisões automatizadas, que poderão, eventualmente, ser discriminatórias[380].

Como já discutido, o perfil é uma representação virtual da pessoa e com ela pode se confundir. Além disso, como serve de base para decisões automatizadas, pode restringir a sua liberdade, pois os dados que o alimentam podem não corresponder à realidade, ter se tornado obsoletos ou ter como base alguma informação discriminatória, por isso a importância da qualidade dos dados e de sua atualização constante é tão grande. É nesse sentido que deve ser garantido o direito ao livre acesso a eles pelo titular.

A perfilização pode ser direcionada a determinadas pessoas, assim como a grupos de pessoas. No entanto, não se pode ter uma visão individualista sobre

---

375 *Ibidem*.
376 MENDES, 2014.
377 BIONI, 2020a.
378 MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Frajhof. Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.
379 MENDES, 2014.
380 BIONI, 2020a.

esse tema, pois a perfilização tem mais relação com grupos sociais do que com uma pessoa específica[381]. Rafael Zanatta[382] explica que a perfilização é um ato sociotécnico e dela há as seguintes obrigações de natureza:

> (i) informacional, relacionada à obrigação de dar ciência da existência do perfil e garantir sua máxima transparência, (ii) antidiscriminatórias, relacionada à obrigação de não utilizar parâmetros de raça, gênero e orientação religiosa como determinantes na construção do perfil, e (iii) dialógica, relacionada à obrigação de se engajar em um "processo dialógico" com as pessoas afetadas, garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e de como decisões são tomadas[383].

A Comissão Europeia explica que as decisões automatizadas podem ser tomadas com base em um perfil ou sem uma definição prévia de um perfil:

> A definição de perfis é efetuada quando os seus aspetos pessoais são avaliados para fazer previsões sobre si, mesmo que não seja tomada qualquer decisão. Por exemplo, se uma empresa ou organização avaliar as suas características (como a idade, o sexo ou a altura) ou o classificar numa categoria, isto significa que está a definir o seu perfil. As decisões individuais exclusivamente automatizadas ocorrem quando são tomadas decisões sobre si por meios tecnológicos e sem envolvimento humano. Estas podem ser efetuadas mesmo sem definição de perfis[384].

Para a criação de perfis, aplicam-se métodos estatísticos e inteligência artificial, resultando em uma "metainformação"[385], o que, por seu turno, pode ser muito valioso, pois assim pode-se aferir os hábitos, preferências pessoais, dados de saúde das pessoas, por exemplo. Na aplicação do resultado obtido, ou seja, de um perfil, a pessoa não precisa estar identificada[386]. A criação dos perfis passa pelas seguintes etapas: "(i) registro de dados, (ii) agregação e monitoramento de dados, (iii) identificação de padrões nos dados, (iv)

---

381 ZANATTA, 2020.
382 *Ibidem*.
383 ZANATTA, 2020, p. 524.
384 COMISSÃO EUROPEIA. Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis? **Comissão Europeia**, [*s. l.*], [20--]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt. Acesso em: 10 fev. 2023.
385 DONEDA, 2020a.
386 BIONI, 2020a.

interpretação de resultados, (v) monitoramento dos dados para checar resultados e (vi) aplicação de perfis (profiles)”[387].

Dessa forma, ainda que o tratamento de dados seja anonimizado, é possível haver repercussão na esfera do livre desenvolvimento da personalidade das pessoas[388]. Os algoritmos fazem a mineração desses dados que foram anonimizados e podem vir a esconder várias práticas discriminatórias anteriores em prejuízo de uma coletividade e de indivíduos[389].

Convém ponderar que os perfis, individuais ou de grupos, nem sempre necessariamente terão aplicação negativa[390], pois é a partir de análise de dados que é possível traçar políticas públicas ou fazer planejamento empresarial. Essa reflexão é feita por Rodotà:

> Por isso se pergunta se essa produção de perfis automatizados não acarreta, concretamente, o empobrecimento da capacidade cognitiva da realidade sócio-econômica em toda a sua riqueza e variedade. Objeta-se ao contrário, que os perfis permitem perceber melhor as propensões individuais e coletivas e, sobre essa base, colocar efetivamente à disposição de cada um aquilo que lhe serve ou que deseja, assim concretizando uma condição de igualdade substancial (“a cada um segundo as suas necessidades”)[391].

Os perfis não devem ser completamente vilanizados ou terem as possibilidades restritas, apenas devem ser operados com cuidado e atenção para que não ocorram eventuais discriminações daqueles que não têm um perfil “preferido”, ou para que se não reflita erroneamente quem é alguém na realidade.

No caso da análise do crédito, a pontuação (*score*) influencia não só na concessão do crédito em si, mas na variabilidade dos juros, decorre daí a importância de saber sobre os critérios utilizados. Outro aspecto do resultado dessas informações são o que elas representam, pois nem o próprio detentor dos dados pode mensurar o resultado delas ou ter controle sobre elas, o que pode afetar a sua autonomia[392].

---

[387] ZANATTA, 2020, p. 525.
[388] BIONI, 2020a.
[389] *Ibidem*.
[390] RODOTÀ, 2008.
[391] *Ibidem*, p. 82.
[392] DONEDA, 2020a.

A partir de agora, demonstrar-se-á uma série de exemplos de como estão fazendo os bancos de dados para tomar decisões automatizadas. Então, no próximo capítulo, poder-se-á discutir os mecanismos e procedimentos disponíveis sob o aspecto jurídico para se evitar discriminações.

Com efeito, existe a possibilidade de o tratamento de dados acarretar discriminação, o que pode afetar a dignidade da pessoa humana, principalmente quando há dados pessoais sensíveis envolvidos na situação.

A empresa Serasa Experian[393], que atua não só no Brasil (pertence ao grupo Experian), desenvolve soluções para reduzir os riscos de crédito. Lançada em 2014, utiliza a seguinte classificação para a população brasileira, principalmente no setor de marketing e de seguros (Mosaic Brasil)[394]: para cruzar 400 variáveis, utilizou algoritmos em que se usam modelos matemáticos e estatísticos, e assim criou 11 grupos e 400 subgrupos para classificar os brasileiros[395]. Agruparam-se segmentos da sociedade que têm semelhanças, como estilo de vida, localização, comportamento financeiro e de consumo[396].

Desse modo, é possível, por exemplo, enquadrar uma pessoa no grupo denominado de juventude trabalhadora urbana, que, por sua vez, divide-se em três subgrupos[397]. O grupo de jovens da periferia é composto de seis subgrupos, entre os quais o maior é o “vida da periferia”[398]. A partir dessas informações do serviço Mosaic, pode-se conceder ou não crédito, reduzir ou não as taxas de juros e o risco, empregar ou não uma pessoa[399].

De acordo com a pesquisa realizada pelo Instituto de Tecnologia e Sociedade do Rio (ITS), publicado em 2017, o serviço prestado pela Mosaic, da Serasa-Experian faz uso de fontes variadas de informações sobre os consumidores, empresas e leva em consideração integrantes pertencentes a uma família, a um mesmo domicílio[400]. Além do mais, “[...] realiza o enquadramento de um cidadão — a partir de seus dados pessoais — em

---

393 SILVEIRA, 2019.
394 SILVEIRA, 2019.
395 *Ibidem*.
396 *Ibidem*.
397 *Ibidem*.
398 *Ibidem*.
399 *Ibidem*.
400 INSTITUTO..., 2017.

determinadas categorias socioeconômicas”[401]. Quanto ao serviço, a utilização de dados pessoais pode ocorrer das seguintes maneiras: “(i) pela coleta de dados para que seja realizada a estratificação; (ii) pelo tratamento de dados para que sejam definidos os critérios e variáveis para a estratificação”[402].

A empresa Experian Data Labs, localizada em San Diego nos Estados Unidos, tem utilizado dados de redes sociais (*Twitter*, *Facebook*, *Yelp* e outras) para empréstimos de empresas jovens ou pequenas para compor a pontuação de crédito[403].

Pode-se mencionar a curiosa prática de uma empresa nos Estados Unidos que usa como informação o fato de a pessoa pesquisada escrever seu nome todo em letra maiúscula, ou seja, em caixa alta, inferindo a partir disso que, se assim o fizer, ela oferece maior risco à companhia. Para seu executivo, todos os dados são dados para análise, embora não sejam utilizados dados retirados de redes sociais[404]. Poderia se pensar que esse critério foi retirado de um estudo científico da área de psicologia ou de alguma outra área científica, mas não é o caso. O executivo dessa empresa não sabe informar qual o motivo que levou a essa dedução — por que há mais riscos nesse caso da escrita do nome em letra maiúscula[405].

Outra empresa utiliza a informação de quanto tempo a pessoa está na mesma profissão e se tem ensino superior[406]. Nesse exemplo, o objetivo é aferir em quanto tempo a pessoa encontrará emprego quando estiver desempregada[407].

Em razão disso, ao se fazer uma análise de crédito ou se concretizar um negócio jurídico, deve-se verificar a relevância de tais informações para que não

---

[401] *Ibidem*, p. 37.
[402] *Ibidem*, p. 38.
[403] KOREN, James Rufus. Beyond mere numbers: some leaders and credit scores use unorhordox data – of ten – unrelated to money – to assess potential borrowers. **Los Angeles Times**, [*s. l.*], 20 dez. 2015. Disponível em: https://www.pressreader.com/usa/los-angeles-times/20151220/281990376480210. Acesso em: 24 set. 2022.
[404] KOREN, 2015.
[405] *Ibidem*.
[406] *Ibidem*.
[407] *Ibidem*.

haja discriminações aleatórias[408]. Por outro lado, como as pessoas poderão melhorar a sua pontuação (*score*) se não têm acesso ao critério utilizado, às informações e não sabe a quais dos seus dados pessoais a empresa tem acesso?

Nos seguros de veículos, também se utiliza a pontuação (*score*), a qual é feita, a princípio, a partir do questionário respondido pelo contratante, o que afeta o valor a ser pago pelo seguro contratado[409]. As respostas dadas têm pesos diferentes. Diante disso, se um determinado modelo de veículo estiver com maior potencial para sinistro, o valor do seguro será mais alto. Além disso, as seguradoras também se baseiam em índices de segurança pública para estipular o valor de seu serviço[410].

O endereço residencial é uma informação necessária e aparentemente neutra. Porém, nos casos de seguro, a depender da região em que a pessoa more, será um fator para elevar o valor do seu seguro. A análise do código de endereçamento postal (CEP), combinado com dados sociodemográficos sobre o conjunto de habitantes em determinadas localidades, pode levar a inferências que prejudiquem ainda mais as pessoas que já estão em uma situação de vulnerabilidade[411].

---

[408] "Significa dizer que para fins de análise de concessão de crédito — fundamentado no princípio da finalidade — estão vedadas inclusões nas bases de dados de quaisquer informações de natureza personalíssima e que não se relacione à finalidade almejada com a análise de crédito, com o objetivo de evitar o tratamento discriminatório — fundamentado no princípio da não discriminação" (MULHOLLAND, 2021).

[409] TAKAR, Téo. Seguro de carro é quase R$ 3.000 mais caro em bairro pobre do que em rico. **Portal UOL**, [*s. l.*], 17 out. 2018. Disponível em: https://economia.uol.com.br/financas-pessoais/noticias/redacao/2018/08/17/como-economizar-seguro-carro.htm?cmpid=copiaecola. Acesso em: 24 set. 2022.

[410] "Há outros critérios como idade, gênero, bairro que reside entre outros: Um levantamento feito pela TEx mostra que o preço do seguro do Chevrolet Ônix, um dos carros mais vendidos do país, pode variar até 140% dentro de São Paulo, dependendo do bairro da capital. Na simulação, foram consideradas duas mulheres com o mesmo perfil: solteiras, com 24 anos e motoristas do mesmo modelo, um Ônix 2017. Porém, uma mora nos Jardins, na zona oeste da capital. A outra reside em Itaquera, na zona leste. A diferença no valor dos seguros chega a R$ 2.806, ou 140%. A moradora dos Jardins pagará R$ 1.998, enquanto a mulher que reside em Itaquera terá que desembolsar R$ 4.804 para ter a mesma cobertura" (TAKAR, 2018).

[411] INSTITUTO..., 2017.

Já se sabe que a utilização da inteligência artificial pode gerar resultados desastrosos e causar discriminação, tendo em vista que um dado considerado trivial pode ser convertido em um dado sensível[412].

A LCP determina que, para a produção do *credit score*, deve-se considerar dados objetivos. Por exemplo, pode-se ter em vista diversas variáveis como a idade, a profissão, a finalidade da obtenção do crédito. Essas variáveis são utilizadas em fórmulas matemáticas e estatísticas, e a partir disso atribuir-se-á uma espécie de pontuação ou nota ao consumidor. Diante disso, quanto maior a nota, menor será o risco de se conceder o crédito para o consumidor[413].

Portanto, a utilização do cadastro positivo é lícita[414] já há algum tempo, todavia, deve-se existir transparência, pois o cadastro tem impactos não só econômicos, mas também em relação à privacidade, à proteção de dados pessoais, podendo causar discriminação. Ademais, deve-se existir transparência em relação aos dados coletados[415], a fim de que não haja discriminação em

[412] BIONI, 2020a.
[413] CAVALCANTE, Márcio André Lopes. Informativo esquematizado: informativo 551-STJ. **Dizer o Direito**, [*s. l.*], 2014. Disponível em: https://dizerodireitodotnet.files.wordpress.com/2015/01/info-551-stj.pdf. Acesso em: 05 dez. 2019.
[414] "Vale ressaltar, no entanto, que para o "credit scoring" ser lícito, é necessário que respeite os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei nº 12.414/2011" (CAVALCANTE, 2014, p. 9).
[415] CAVALCANTE, 2014.

relação a determinados grupos sociais — por exemplo[416], a LGPD estabelece expressamente os princípios da transparência e da não discriminação[417].

Outro aspecto interessante acerca desse tema é que a fórmula matemática utilizada, ou seja, a metodologia aplicada, não precisa ser fornecida, haja vista que é considerada segredo da atividade empresarial, conforme o Superior Tribunal de Justiça[418]. Por outro lado, o artigo 3º, inciso IV, da referida

---

[416] "[...] no tocante ao sistema *scoring* de pontuação, 'apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas [...]'". BRASIL. Superior Tribunal de Justiça (4. turma). **Recurso Especial n. 1268478/RS**. Recurso especial. Ação cautelar de exibição de documentos. Crediscore. Interesse de agir. Demonstração de que a recusa de crédito se deu em razão da ferramenta de scoring, além de requerimento na instituição responsável por este e a sua negativa ou omissão. Relator: Ministro Luis Felipe Salomão, 18 dez. 2014. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/863738929. Acesso em: 17 jul. 2022.
"[...] O sistema '*credit scoring*' é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). [...] Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). [...] Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas. [...] O desrespeito aos limites legais na utilização do sistema '*credit scoring*', configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados. [...]" BRASIL. Superior Tribunal de Justiça (2. seção). **Recurso Especial n. 1.419.697/RS**. Recurso especial representativo de controvérsia (art. 543-C do CPC). Direito do consumidor. Arquivos de crédito. Sistema "credit scoring". Compatibilidade com o direito brasileiro. Limites. Dano moral. Recorrente: Boa Vista Serviços. Recorrido: Anderson Guilherme Prado Soares. Relator: Ministro Paulo de Tarso Sanseverino, 12 nov. 2014. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/152068666. Acesso em: 30 jan. 2023.
"[...] declarar que 'o sistema '*credit scoring*' é um método de avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito)' e para afastar a necessidade de consentimento prévio do consumidor consultado". BRASIL. Superior Tribunal de Justiça (2. seção). **Recurso Especial n. 1457199/RS**. Recurso especial representativo de controvérsia (Art. 543-C do CPC). Direto do consumidor. Arquivos de crédito. Sistema "credit scoring". Compatibilidade com o direito brasileiro. Limites. Dano moral. Relator: Ministro Paulo de Tarso Sanseverino, 12 nov. 2014. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/158643665. Acesso em: 30 jan. 2023.

[417] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; [...] IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos".

[418] "O consumidor terá direito de saber a sua pontuação e as informações pessoais utilizadas. No entanto, nem o consumidor nem ninguém terá direito de saber a metodologia de cálculo, ou seja, qual foi a fórmula matemática e os dados estatísticos utilizados no '*credit scoring*'. Isso

lei exige que as informações coletadas devam ser de fácil compreensão e que se deve ter acesso a elas, principalmente aos dados pessoais. Essas informações poderão contribuir para saber o motivo da negativa de crédito e o motivo pelo qual não houve a redução de juros[419].

Isso possibilita que o cadastrado possa exigir a retificação dos seus dados. Ademais, o CDC no art. 6º, inciso III, estabelece como direito básico do consumidor que a informação esteja clara e adequada dos serviços. Isso afeta também o princípio da transparência, que tem por objetivo proteger o sujeito contra as situações em que ele seja colocado em uma posição de vulnerabilidade em função de decisões potencialmente arbitrárias sem quaisquer justificativas ou possibilidades de recurso[420].

Para Mendes[421], o consumidor deve ser informado do sistema de avaliação e conhecer os critérios utilizados, senão o sistema será ilegítimo, pois viola os princípios da proteção de dados pessoais. Ademais, não pode haver um pseudoconsentimento — para isso, em consonância com o art. 46 do CDC, assegura-se:

> É minimamente leal, ético e legal que se haja uma compreensão prévia, e não mero conhecimento, sobre o que se está concordando. Com isso, não se está mais a tolerar o tratamento de dados pessoais a partir de um pseudoconsentimento do usuário, sem a sua real compreensão das implicações da análise de suas informações e sua estratificação em perfis de consumo[422].

Entre os direitos previstos no art. 6º, inciso V, da Lei do Cadastro Positivo, está o de receber o sumário de quais seriam esses direitos do cadastrado. Entre eles deveriam constar não só o de obter a sua pontuação, mas também o de

---

porque essa fórmula é fruto de estudos e investimentos, constituindo segredo da atividade empresarial (art. 5º, IV, da Lei n. 12.414⁄2011: [...] 'resguardado o segredo empresarial')" (CAVALCANTI, 2014, p. 10).

[419] BESSA, 2019.

[420] SILVA, Priscilla; MEDEIROS, Juliana. A polêmica da revisão (humana) sobre decisões automatizadas. **ITS Rio**, [*s. l.*] 10 dez. 2019. Disponível em: https://feed.itsrio.org/a-pol%C3%AAmica-da-revis%C3%A3o-humana-sobre-decis%C3%B5es-automatizadas-a81592886345. Acesso em: 06 fev. 2023.

[421] MENDES, 2014.

[422] CAMURÇA; MATIAS, 2021, p. 11.

acessar quais foram os dados e os critérios utilizados, bem como o de ser indenizado em caso de tratamento irregular dos seus dados[423].

Há sanções civis e administrativas previstas na LCP (art. 16 e 17) caso os dados sejam colhidos sem finalidade específica ou tenham a sua utilização para fins diversos, pois há ofensa à privacidade[424].

Deve-se ponderar que esse sistema também pode ser utilizado para evitar o superendividamento. Por outro lado, o excesso de concessões de crédito poderia ser considerado um abuso de direito daqueles que têm essas informações e, mesmo assim, continuam a conceder crédito sem observar tais critérios.

As informações pessoais e os dados podem ser obtidos diretamente a partir de respostas de um questionário ou por correlações feitas pela máquina. Em um primeiro momento, não se questiona a religião de uma pessoa, mas a partir de dados que se tem, pode-se concluir que a pessoa professa determinada fé, o que pode ser obtido indiretamente pelo programa de computador, por aplicativos ou dispositivos (*wearables*) que a pessoa usa, por exemplo, para monitorar quantos passos dá durante o dia, o quanto de água ingere por dia, se pratica exercícios físicos.

Não se pode perder de vista que os dados coletados devem observar os princípios da necessidade, da adequação e da finalidade (art. 6º, LGPD). Essa é uma proteção do titular e deve ser atendida por aquele que coleta os dados, ou seja, pelos agentes de tratamento de dados, para que possa justificar a sua atividade, bem como se resguardar de eventuais responsabilizações.

---

[423] "No mínimo, o texto deve indicar os seguintes direitos: 1) direito de cancelamento do cadastro positivo; 2) direito de acesso; 3) direito de exigir a correção; 4) direito de obter a pontuação de crédito, bem como todos os elementos e critérios considerados; 5) direito de conhecer a qualificação dos bancos de dados, consulentes e fontes; 6) limite temporal das informações negativas e positivas; 7) direito a ser comunicado por escrito do registro de informação negativa; 8) direito a ser indenizado pelo banco de dados e fornecedor em caso de tratamento irregular dos seus dados; 9) direito a reclamar perante órgãos de defesa do consumidor (Senacon e Procon) e/ou Autoridade Nacional de Proteção de Dados (ANPD)" (BESSA, 2019, p. 107).

[424] BESSA, 2019.

Em razão disso, Rodotà[425] assevera que, se não houver necessidade de dados para uma determinada atividade, não se deve coletar, ou seja, se a atividade puder sem alcançada sem a coleta, assim deve ser feita.

Em relação aos perfis dos consumidores, no que diz respeito aos dados sensíveis acerca da saúde do sujeito, a LGPD, art. 11, §5º, veda às operadoras de planos privados de assistência à saúde que os utilizem para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. Ademais, o art. 21 da LGPD proíbe a utilização de dados pessoais em prejuízo do titular dos dados para exercício regular de seus direitos.

No que diz respeito à responsabilidade, essa é objetiva e solidária ao banco de dados (LCP, art. 16). Portanto, respondem a fonte e o consulente pelos danos que causarem ao cadastrado nos termos do Código de Defesa do Consumidor.

Como já mencionado, em regra, os dados anonimizados não são considerados dados pessoais para os fins da LGPD, art. 12. Contudo, o processo de anonimização ao qual foram submetidos os dados pode ser revertido[426]. Isso pode ser feito ao se utilizar exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Mas há uma outra situação em que os dados anonimizados utilizados podem interferir na formação do perfil comportamental de determinada pessoa natural, e, caso ela seja identificada, serão considerados dados pessoais. Nesse sentido:

---

[425] RODOTÀ, 2008.

[426] "De fato, o que caracteriza um dado como pessoal é, sem dúvida alguma, entendido a partir da relação entre o contexto, o uso e a qualidade da tecnologia empregada. Não há, dessa forma, uma radical metodologia de anonimização total, vez que toda parametrização pode ser alvo de engenharia reversa. As principais técnicas são a supressão, a generalização, a randomização e a pseudoanonimização, tendo em vista sempre a noção de quebra da vinculação entre o dado e a pessoa. A ideia primordial é tornar o vínculo, na medida do possível, mediato, inexato e impreciso. Assim, o que se tem, na realidade, é uma espécie de gerenciamento contínuo da identificabilidade das bases de dados. Todo processo de anonimização, conveniente reconhecer, é circunstancial e precarizado em face do desenvolvimento de novas técnicas, tratando-se de um mito que se impõe de uma maneira geral para o engendramento da proteção sistemática da pessoa na sociedade informacional e que exige uma atenção redobrada e contínua, em particular quando se tem em vista a criação de algoritmos para a desanonimização de bases de dados pessoais, inclusive sensíveis" (SARLET; RUARO, 2021, p. 90-91).

> Com isso, houve permissão legal para que os dados coletados continuem sendo utilizados de forma anônima, totalmente destacados do seu titular. Inclusive, consoante o art. 16, inciso IV, uma das possibilidades de conservação de dados após o término do tratamento é que haja uso exclusivo do controlador, desde que anonimizados os dados. Em não sendo dados pessoais, a comercialização de dados anônimos resta autorizada a quem neles obtiver interesse. No entanto, as atuais práticas de vendas de blocos de cadastros com dados pessoais ficam praticamente inviabilizadas, mas para que ocorram deve-se haver o consentimento inequívoco de todos os titulares dos dados[427].

Adiante, as consultas sobre a pontuação são feitas nos birôs. Não são eles que concedem ou negam o crédito, são eles que detêm as informações, portanto, não cabe a eles a decisão de realizar ou não um negócio[428].

As incongruências que podem ser geradas pelos algoritmos também geram responsabilização. A governança dos algoritmos[429] pode ser feita com a criação de órgãos supervisores. Faz-se necessário várias frentes de atuação, desde legislação adequada, responsabilização e supervisão governamental[430]. Portanto, deve haver transparência e responsabilização na utilização de algoritmos, haja vista que afeta diretamente os direitos fundamentais e o desenvolvimento da personalidade[431] (LGPD, art. 1º e 2º, inciso VII).

Mas será a partir de algoritmos, que contêm instruções precisas, que poder-se-á processar os dados coletados. Os algoritmos são uma sequência lógica, isto é, "[...] uma sociedade operada por algoritmos é uma sociedade matematizada"[432]. Em razão disso, questiona-se se a matemática, a lógica, os algoritmos[433], os programas de computador, por meio de decisões automatizadas, podem solucionar os problemas de crédito, de seguros, de distribuição de renda, de juros altos, de emprego, de problemas complexos existentes há décadas na sociedade brasileira.

---

427 CAMURÇA; MATIAS, 2021, p. 19.
428 COSTA, 2012.
429 DONEDA; ALMEIDA, 2018.
430 *Ibidem*.
431 BIONI, 2020a.
432 SILVEIRA, 2019, p. 19.
433 "O pesquisador Pedro Domingos alerta que 'um algoritmo não é apenas qualquer conjunto de instruções: elas têm de ser suficientemente precisas e não ambíguas para serem executadas por um computador" (SILVEIRA, 2019, p. 19).

Esses programas de computador e os seus algoritmos buscam por padrões, classificações, hierarquia[434]. Trata-se de um sistema que pode ser muito útil para operar com essas informações, que podem ser probabilidades ou prescritíveis[435]. O aprendizado da máquina (*machine learning*) correlaciona dados armazenados, busca por padrões e antevê as tendências para o futuro[436].

Posto isso, além de a pessoa ser informada que os seus dados serão passados por tratamento, também deve ser informada sobre o tipo de inteligência artificial que será utilizado no processamento dos dados. Nem sempre as pessoas saberão a fundo sobre esse tema, mas isso pode vir a ser uma informação relevante quanto ao viés discriminatório e a opacidade (*black box*) — opacidade essa decorrente da dificuldade de decodificação dos resultados[437].

Ademais, a mineração dos dados tem como objetivo buscar padrões comportamentais e diminuir os riscos nas relações comerciais, ou seja, procura "[...] padrões de organização social"[438]. Buscar por padrões ou fazer generalizações por si só não é um problema, mas pode passar a ser quando tiver por consequências discriminações e exclusões de pessoas ou determinados grupos que não sejam justificáveis ou adequadas. Quais dados ou informações pessoais, por exemplo, terão mais peso para justificar uma negativa?

Os chamados birôs de crédito utilizam generalizações que projetam um perfil de risco ou até mesmo, quando analisam riscos individuais, utilizam comportamentos anteriores de outras pessoas que têm características semelhantes ao cliente em análise, como idade, gênero, etnia, localização (CEP), residência[439].

Há um entendimento de que deve ser proibida a utilização de dados de geolocalização para compor a pontuação, pois a objetividade do sistema de avaliação é prejudicada, uma vez que há uma suposição da condição financeira

---

[434] SILVEIRA, 2019.
[435] *Ibidem*.
[436] *Ibidem*.
[437] DONEDA; ALMEIDA, 2018.
[438] SILVEIRA, 2019, p. 24.
[439] INSTITUTO..., 2017.

do consumidor a partir do endereço onde mora[440]. Isso ocorre porque trata-se de:

> Um complicador importante diz respeito às chamadas “variáveis por representação”, no qual um parâmetro específico é utilizado como substituto (involuntário ou não) de um parâmetro vedado. O exemplo mais comum é a utilização do endereço como substituto de origem social e étnica. Nesses casos é cabível diligência do agente responsável pelo tratamento de dados na avaliação dos parâmetros, para evitar a parametrização irregular dos algoritmos de avaliação de crédito, ainda que ela esteja ocultada sob o emprego de parâmetros à primeira vista válidos[441].

Como mencionado anteriormente, muitas dessas decisões automatizadas são tomadas com base em dados anonimizados que estão catalogados, os quais verificam se a pessoa pertence a determinado grupo — e isso pode decorrer de um perfil comportamental[442], por exemplo. Nos seguros de automóveis, podem ser utilizadas diversas informações já existentes, como dados de roubos e furtos, acidentes, idade e gênero, que pertencem não só ao banco de dados internos, mas que estão disponíveis para a sociedade.

A Lei de n. 12.414/2011 (LCP) veda expressamente que sejam feitas anotações que sejam excessivas ou sensíveis: (art. 3, §3º):

> I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
> II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Consideram-se informações excessivas, segundo o julgado do Superior Tribunal de Justiça, informações que digam respeito aos gostos pessoais e ao clube de futebol para o qual a pessoa torce, por exemplo[443]. Não se pode reduzir o entendimento de que excessivas informações dizem respeito a quantidades de dados. Diante disso, as informações excessivas podem ser aquelas aferidas a partir de metadados ou dados alternativos, que não tenham necessariamente relação direta com a pessoa, isto é, a sua personalidade — como qual a marca

---

[440] MENDES, 2014.
[441] GOETTENAUER, 2022, p. RB-24.5.
[442] BIONI, 2020a, *op. cit.*, p. 78.
[443] BRASIL, 2014.

e o modelo de celular que a pessoa usa para acessar um aplicativo ou se faz compras pela internet[444].

Zanatta[445] defende que as informações excessivas não podem ser restritas a uma ideia tautológica, que se restringe às informações com análise de crédito. Com essa informação é possível:

> Em outras palavras, o problema fundamental da discriminação abusiva aqui é uma catalogação e perfilização, feitas com base em metadados não diretamente relacionados a adimplementos obrigacionais, que fazem com que uma pessoa seja julgada não por *quem ela é*, mas sim por aproximação estatística de *probabilidade de pertencimento a um grupo social*, que é constituído artificialmente pelo fluxo de informações e por uma análise preditiva[446].

Desse modo, com a análise feita a partir de metadados é possível determinar o comportamento de um grupo que tenha características semelhantes[447]. Nesse caso, o autor sustenta a aplicação do princípio da boa-fé e do abuso do direito previsto no art. 187 do CC/2002, pois "[...] também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes".

O conceito de *big data* define um grande volume de dados estruturados, semiestruturados ou não estruturados dos quais extraem-se informações[448]. A ciência de dados (*data science*), por sua vez, analisa os dados brutos que permitem a compreensão de fenômenos que são objeto de análise ou de estudo para se extrair informações[449]. Deve-se entender, atualmente, o banco de dados do seguinte modo:

> Portanto, que um banco de dados deve ser necessariamente atrelado à ideia de um sistema de informação, cuja dinâmica explicita, sequencialmente, um processo que se inicia pela coleta e estruturação

---

[444] ZANATTA, Rafael A. F. O uso de informações excessivas nos sistemas de pontuação de crédito: a importância de critérios para aferir discriminação abusiva. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022.
[445] *Ibidem*.
[446] ZANATTA, 2022, p. 263.
[447] *Ibidem*, p. 264.
[448] MAGRANI, 2019.
[449] *Ibidem*.

> dos dados, perpassa a extração de uma informação que, por fim, agrega conhecimento[450].

Por conseguinte, o *big data* faz um diagnóstico e não questiona as razões, os motivos que estão por trás dos dados[451]. Costuma-se discutir muito sobre o excesso de dados e informações arquivadas, coletadas para o processamento de dados. Contudo, há um caso, no Brasil, em que uma equipe de programadores desenvolveu um sistema de crédito que teve soluções racistas causadas pelo algoritmo[452]. Nesses sistemas experimentais, utilizaram-se 10 (dez) informações para aferir a probabilidade de inadimplência. Entre as informações, estavam os três primeiros dígitos de CEP (Código de Endereçamento Postal) do consumidor[453], os quais são responsáveis por delimitar as regiões maiores com bairros específicos de uma região[454]. Ao cabo, esse sistema não foi implantado. Ramon Vilarino participou do desenvolvimento desse sistema experimental e explica que:

> [...] o uso que esse sistema experimental de pontuação de crédito fazia da variável CEP-3 é uma excelente aprovação para distribuição racial do país. Essa aproximação é tão boa que nos fez perguntar: como seria um modelo que fizesse o uso explícito da proporção de pessoas não-brancas vivendo em cada vizinhança no lugar do CEP-3? Dentro do paradigma de predição e minimização de risco, podemos dizer que obtivemos sistemas equivalentes. Não apenas os padrões estatísticos de erros e acertos são virtualmente idênticos, como a substituição variável de não-branquitude se mostrou muito evidente: quanto mais branca uma região, maior o impacto dessa informação para aumentar as pontuações de crédito das pessoas que vivem ali[455].

Por conseguinte, se uma pessoa se mudasse de São Paulo para a Bahia, alterando assim o CEP-3, ela teria sua pontuação do crédito diminuída em 99,8% no experimento. Diante disso:

> É de se esperar, portanto, que — caso esse sistema tivesse sido de fato implantado — as pessoas nas regiões menos brancas do país teriam menos acesso a crédito nem mercado que confia nessas

---

[450] BIONI, 2020a, p. 33.
[451] BIONI, 2020a.
[452] VILARINO, 2022.
[453] VILARINO, 2022.
[454] *Ibidem*.
[455] *Ibidem*, p. 219.

> predições para restringir a oferta ao grupo de consumidores que julgue mais rentáveis e menos arriscados[456].

Thiago Junqueira[457] ilustra um caso de discriminação que ocorreu na Inglaterra, em 2018, quando foi divulgado pela imprensa que seguradoras de automóveis teriam fixado prêmios distintos para perfis distintos. Nesse caso, o nome de um determinado condutor é que teria desencadeado a discriminação, pois tinha como sobrenome Mohammed Ali, ou seja, tratava-se de um nome que não tinha origem tipicamente inglesa. Por conta disso, o seu seguro acabou tendo uma precificação diferente[458]. Nota-se, nesse exemplo, que não foi necessária uma quantidade enorme de dados para se verificar um caso de discriminação.

Ao cabo, este capítulo teve como foco a fase anterior da tomada das decisões automatizadas, a reflexão sobre quais dados podem ser coletados e a exposição de alguns dos direitos dos titulares dos dados antes da tomada de decisão. No Capítulo 3, discutir-se-á que medidas podem ser tomadas para se evitar discriminações.

---

[456] Idem, p. 220.
[457] JUNQUEIRA, 2020a.
[458] *Ibidem*.

CAPÍTULO III

3 OS MECANISMOS EXISTENTES PARA ENFRENTAR A DECISÃO AUTOMATIZADA E A SUA REVISÃO

Neste capítulo, discutir-se-ão o tema da decisão automatizada e a sua revisão e os mecanismos jurídicos que podem ser aplicáveis a fim de que os direitos fundamentais sejam efetivamente protegidos.

Antes disso, ver-se-á como foi o processo de elaboração do art. 20 da LGPD e de seus parágrafos. Havia uma outra redação para esse artigo, mas houve o veto presidencial (PLV/2019)[459] de seu parágrafo terceiro. Nele, havia a possibilidade de revisão humana, que teria como objetivo reduzir os "falsos positivos", que "[...] são aqueles casos em que parece, mas não é. Eles, todavia, nem sempre são capazes de dirimir problemas mais profundos, como discriminação incorporada no algoritmo. Para estes, a intervenção humana serve para chamar atenção e sinalizar a existência de um problema"[460].

Houve a tentativa de derrubar o referido veto pelo Congresso Nacional. A Câmara dos Deputados contabilizou 261 (duzentos e sessenta e um) votos pela derrubada do veto, no entanto, no Senado Federal foram 40 (quarenta) votos a favor — e por um voto o veto foi mantido[461]. As justificativas apresentadas para o veto foram as seguintes:

> 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

[459] SILVA; MEDEIROS, 2019.
[460] SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020. p. 271.
[461] SILVA; MEDEIROS, 2019.

> reflexos, ainda, nos índices de inflação e na condução da política monetária[462].

Como salienta Thiago Junqueira[463], o legislador deixou passar uma oportunidade de oferecer mecanismos com maior fiscalização para combater, principalmente, a discriminação indireta. Ao se ter um olhar constitucional sobre a LGPD e as demais legislações infraconstitucionais que se aplicam ao tema, é possível identificar mecanismos jurídicos que possam ser utilizados para a proteção dos titulares dos dados pessoais. A atual redação do artigo 20, *caput*, da LGPD é a seguinte:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019).

Interessante notar que o art. 20, *caput*, dispõe sobre decisão tomada "unicamente" com base em tratamento automatizado, portanto, é possível haver situações em que o tratamento seja parcialmente automatizado. A LCP utiliza a expressão "exclusivamente" em seu art. 5º, inciso VI: "solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados".

A retirada da possibilidade de revisão da decisão automatizada poderia induzir a um entendimento de que essa não pode ser feita por pessoa natural, mas somente por outra máquina. Difícil argumentar que não pode haver a revisão da decisão por pessoa natural, haja vista que não se trata de uma ilegalidade ou de uma proibição. Aliás, a CRFB, em seu art. 5º, inciso II, dispõe que "[...] ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei".

O grupo de trabalho, do artigo 29 para a proteção de dados da Diretiva 95/46/CE, conceitua a decisão automatizada como aquela que pode sobrepor-se parcialmente à definição de perfis ou resultar dela[464]. A decisão

---

[462] BRASIL. **Mensagem n. 288, de 8 de julho de 2019**. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: 06 fev. 2023.
[463] JUNQUEIRA, 2020a, RB-14.2.
[464] GRUPO…, 2017.

exclusivamente automatizada, por sua vez, é aquela em que a decisão é tomada por um sistema sem nenhuma intervenção humana. Nessa espécie de decisão, não é necessário existir um perfil prévio[465]. A distinção entre a decisão unicamente e exclusivamente automatizada consiste na ausência de intervenção humana na decisão, ou seja, uma vez tomada a decisão, aplica-se o resultado sem nenhuma interferência[466]. Quando há a intervenção humana, por outro lado, a pessoa toma conhecimento da decisão para então decidir se concederá um empréstimo ou se utilizará ou não o que se decidiu com base em um perfil. Nessa segunda hipótese, o perfil é o que corresponde a uma decisão automatizada[467].

Desse modo, devem os agentes de tratamentos de dados pessoais documentar o grau de intervenção humana na tomada da decisão, como é explicado pelo grupo de trabalho do artigo 29 que se refere à RGPD:

> Para que se considere haver uma intervenção humana, o responsável pelo tratamento tem de garantir que qualquer supervisão da decisão seja relevante, e não um mero gesto simbólico. Essa supervisão deve ser levada a cabo por alguém com autoridade e competência para alterar a decisão e que, no âmbito da análise, deverá tomar em consideração todos os dados pertinentes.
> No âmbito da sua AIPD, compete ao responsável pelo tratamento identificar e registar o grau de intervenção humana no processo decisório e a fase em que essa intervenção ocorre[468].

O direito à informação, à explicação e à oposição são garantidos mesmo que não seja unicamente automatizada a decisão, haja vista as demais disposições legislativas. Ana Frazão[469] entende que o art. 20 da LGPD garante uma espécie de devido processo legal que protege o sujeito contra a ação dos algoritmos preditivos. Na ADI n. 6389[470], o ministro Gilmar Mendes, em seu voto, fez menção ao devido processo informacional (*informational due process privacy*

---

[465] *Ibidem*.
[466] GRUPO…, 2017.
[467] *Ibidem*.
[468] ***Ibidem***, p. 23.
[469] FRAZÃO, Ana. O direito à explicação e à oposição diante de decisões totalmente automatizadas. **JOTA**, [*s. l.*], 05 dez. 2018a. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018. Acesso em: 25 ago. 2022.
[470] BRASIL, 2020.

right), em que a dimensão subjetiva do direito à proteção de dados pessoais[471] propicia ao titular o direito de evitar exposições de seus dados e de poder exercer o controle sobre eles, a fim de não esteja sujeito a julgamentos preditivos e peremptórios[472]. Portanto, o devido processo informacional, segundo o ministro, é um corolário da proteção de dados pessoais no que diz respeito à sua dimensão subjetiva[473].

Além disso, no art. 20, na sua parte final, há as seguintes situações "[...] incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade". Portanto, deve-se levar em consideração o fator preponderante da máquina mais a probabilidade de afetar de maneira negativa os direitos fundamentais, assim como a definição de perfil pessoal, de consumo de crédito ou de aspectos de sua personalidade, todos os quais estão abrangidos pela revisão das decisões, bem como do direito à explicação[474]. Por isso, deve-se aplicar uma interpretação que abarque todas essas possibilidades para questionamentos e informações.

Pode-se dizer, ainda, que o devido processo informacional, além de ter uma dimensão processual para o exercício de direitos via judicial, também pode contribuir para assegurar a simetria e proporcionalidade no âmbito extrajudicial[475]. Desse modo, tanto nas relações entre o indivíduo e o poder estatal, quanto nas relações privadas em que exista a "[...] assimetria de poder devem ser permeadas pela garantia do devido processo, evitando que ações arbitrárias e intrusivas sejam tomadas sem que o sujeito tenha a capacidade de se defender"[476].

---

[471] "A dimensão objetiva do direito à proteção de dados pessoais consiste na "afirmação do direito fundamental à proteção de dados pessoais que impõe ao legislador um verdadeiro dever de proteção (*Schutzpflicht*) do direito à autodeterminação informacional, o qual deve ser colmatado a partir da previsão de mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento (*Recht auf Organisation und Verfahren*) e normas de proteção (*Recht auf Schutz*)" (BRASIL, 2020, p. 26).

[472] BRASIL, 2020.

[473] *Ibidem*.

[474] MARTINS, 2022.

[475] BIONI, Bruno; MARTINS, Pedro. Devido processo informacional: um salto teórico-dogmático necessário? **Portal Bruno Bioni**, [*s. l.*], 08 ago. 2020. Disponível em: https://brunobioni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-Processo-Informacional1.pdf. Acesso em: 18 fev. 2023.

[476] BIONI; MARTINS, 2020, p. 04.

Verifica-se então a existência de decisões do STJ no sentido de eficácia horizontal dos direitos fundamentais, por exemplo, como ocorre nas divergências entre condôminos em que se aplica o direito de defesa, contraditório, ainda que em sede extrajudicial[477]. Do mesmo modo ocorre nas decisões automatizadas, nas quais também deve ser aplicada a eficácia horizontal dos direitos fundamentais, ou seja, nas relações privadas.

Convém destacar que, de modo geral, nos Estados Unidos, a tendência é proceder voltando-se para uma teoria do devido processo legal com base nos princípios da transparência, podendo os interessados se manifestar[478]. Na Europa, por sua vez, enfatiza-se o direito à explicação, à informação e à

---

[477] "DIREITO CIVIL. RECURSO ESPECIAL. CONDOMÍNIO. AÇÃO DE COBRANÇA DE MULTA CONVENCIONAL. ATO ANTISSOCIAL (ART. 1.337, PARÁGRAFO ÚNICO, DO CÓDIGO CIVIL). FALTA DE PRÉVIA COMUNICAÇÃO AO CONDÔMINO PUNIDO. DIREITO DE DEFESA. NECESSIDADE. EFICÁCIA HORIZONTAL DOS DIREITOS FUNDAMENTAIS. PENALIDADE ANULADA. 1. O art. 1.337 do Código Civil estabeleceu sancionamento para o condômino que reiteradamente venha a violar seus deveres para com o condomínio, além de instituir, em seu parágrafo único, punição extrema àquele que reitera comportamento antissocial, *verbis*: 'O condômino ou possuidor que, por seu reiterado comportamento antissocial, gerar incompatibilidade de convivência com os demais condôminos ou possuidores, poderá ser constrangido a pagar multa correspondente ao décuplo do valor atribuído à contribuição para as despesas condominiais, até ulterior deliberação da assembléia'. 2. Por se tratar de punição imputada por conduta contrária ao direito, na esteira da visão civil-constitucional do sistema, deve-se reconhecer a aplicação imediata dos princípios que protegem a pessoa humana nas relações entre particulares, a reconhecida eficácia horizontal dos direitos fundamentais que, também, deve incidir nas relações condominiais, para assegurar, na medida do possível, a ampla defesa e o contraditório. Com efeito, buscando concretizar a dignidade da pessoa humana nas relações privadas, a Constituição Federal, como vértice axiológico de todo o ordenamento, irradiou a incidência dos direitos fundamentais também nas relações particulares, emprestando máximo efeito aos valores constitucionais. Precedentes do STF. 3. Também foi a conclusão tirada das Jornadas de Direito Civil do CJF: En. 92: Art. 1.337: As sanções do art. 1.337 do novo Código Civil não podem ser aplicadas sem que se garanta direito de defesa ao condômino nocivo. 4. Na hipótese, a assembleia extraordinária, com quórum qualificado, apenou o recorrido pelo seu comportamento nocivo, sem, no entanto, notificá-lo para fins de apresentação de defesa. Ocorre que a gravidade da punição do condômino antissocial, sem nenhuma garantia de defesa, acaba por onerar consideravelmente o suposto infrator, o qual fica impossibilitado de demonstrar, por qualquer motivo, que seu comportamento não era antijurídico nem afetou a harmonia, a qualidade de vida e o bem-estar geral, sob pena de restringir o seu próprio direito de propriedade. 5. Recurso especial a que se nega provimento". BRASIL. Superior Tribunal de Justiça (4. turma). **Recurso Especial n. 1.365.279/SP**. Direito civil. Recurso especial. Condomínio. Ação de cobrança de multa convencional. Ato antissocial (art. 1.337, parágrafo único, do código civil). Falta de comunicação prévia ao condômino punido. Direito de defesa. Necessidade. Eficácia horizontal dos direitos fundamentais. Penalidade anulada. Recorrente: Condomínio Edifício São Tomás. Recorrido: Jurandy Carador. Relator: Ministro Luis Felipe Salomão, 25 ago. 2015. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/864106706/inteiro-teor-864106715. Acesso em: 30 ago. 2022.

[478] SOUZA; PERRONE; MAGRANI, 2020.

transparência para o exercício do controle por parte do titular dos dados[479]. Contudo, como o direito à explicação e à transparência não podem se restringir a um exercício individual[480], no Brasil há também a previsão de atuação da ANPD e da realização de auditoria, o que contribui para a proteção coletiva, por exemplo. No Reino Unido, por outro lado, há um procedimento expresso, embora não utilize a expressão "direito à explicação"[481]:

> A lei estrutura a relação em três momentos: i) notificação, ii) requisição do titular, e iii) explanação dos passos dados e resultado do cumprimento da requisição do indivíduo.
> Dessa forma, o controlador deve, logo que possível, notificar o titular dos dados de que se utiliza de uma ferramenta de decisão automatizada. O titular, por sua vez, tem trinta dias após receber a notificação para requerer do controlador que: ou reconsidere a decisão — presumivelmente com uma sugestão de novos dados ou novo peso aos mesmos dados apresentados — ou tome uma nova decisão, aí não somente automatizada, mas com participação humana. [...]
> Por fim, o controlador tem o prazo de um mês, podendo estender por mais quinze dias para considerar os pedidos do titular e acatar, ou informar sobre os resultados e os passos tomados[482].

Como demonstrado no capítulo anterior, os dados podem ter sido anonimizados e, ainda assim, afetarem os interesses de uma pessoa ou utilizarem aspectos de sua personalidade[483]; por isso, todos os dados pessoais que compõem perfis terão direito à revisão da decisão tomada (LGPD, art. 12, §3º).

A redação original do artigo 20, §3º da LGPD, que dizia que poderia haver revisão por uma pessoa natural, prescrevia o seguinte:

> § 3º A revisão de que trata o caput deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Esse parágrafo já demonstrava a importância do papel que teria a ANPD na efetiva proteção de dados pessoais. Extrai-se da leitura do artigo 20, com redação atual, que não há menção expressa ao direito à explicação. Apesar

---

[479] *Ibidem*.
[480] *Ibidem*.
[481] *Ibidem*.
[482] SOUZA; PERRONE; MAGRANI, 2020, p. 266.
[483] BIONI, 2020a.

disso, ele tem sido defendido pela doutrina com fundamento no direito à informação. Isso se faz necessário para que seja protegido o direito fundamental à proteção de dados pessoais e à autodeterminação informativa.

Ademais, a redação anterior da Medida Provisória n. 869/2018 possibilitava a revisão da decisão automatizada por pessoa natural[484]. Para alguns, só será possível, a partir desta mudança, a revisão por uma outra máquina, por se ter excluído a revisão por pessoa natural, mas, como explica Ana Frazão[485], o que restaria seria um duplo grau algorítmico, pois uma outra máquina teria a competência para fazer a revisão. Por conseguinte, não haveria a garantia de inteligibilidade das decisões e demais garantias[486].

Não é possível sustentar uma visão simplista de que, para solucionar a questão, basta uma revisão por outra máquina, pois os problemas de transparência, discriminações, enviesamentos continuarão a existir, com base na afirmação dos especialistas da área de tecnologia, em razão da opacidade (*black-box)*, que muitas vezes decorre do próprio sistema — ou por motivos legais ou para não estar sob escrutínio de terceiros[487], ou por não ser possível haver uma explicação por uma pessoa da área técnica.

Como se viu no Capítulo 2, devido à complexidade do sistema, faz-se necessário que haja medidas protetivas desde o desenvolvimento do sistema e

---

[484] "De acordo com o Parecer do Deputado Federal Orlando Silva (PCdoB-SP), os argumentos principais para a volta da revisão humana eram: (i) que a retirada da pessoa humana enfraqueceria o exercício dos direitos humanos, de cidadania e do consumidor previstos no artigo 2º, incisos VI e VII, da LGPD; (ii) que a interação de pessoas com deficiência de julgamento ou falta de experiência com controladores seria dificultada, pois a inexistência de contato com revisores humanos poderia levar a práticas abusivas; (iii) que os algoritmos que processam os dados são baseados em cálculos probabilísticos e estatísticas e que, por não englobarem o universo dos titulares e seus comportamentos, poderiam levar a erros e desvios-padrões, já que se baseiam apenas em amostras e intervalos de confiança, além de estarem sujeitos a incorreções próprias do desenvolvimento tecnológico; (iv) que a retirada iria de encontro ao que prevê a GDPR em seu art. 22, o que poderia dificultar a integração comercial e a geração de oportunidades e investimentos. Com base nessas ponderações, a lei foi aprovada, até que, na fase da sanção, o Presidente da República vetou o § 3º, que previa a revisão humana, em defesa das *startups* e *fintechs*, apesar de o Poder Legislativo ter expressamente sopesado os argumentos referentes a elas" (MEDON, 2020, RB-17.4).

[485] FRAZÃO, Ana. O jogo da imitação jurídica: o direito à revisão de decisões algorítmicas como um mecanismo para a necessária conciliação entre linguagem natural e infraestrutura matemática. *In*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O Direito Civil na era da inteligência artificial**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

[486] *Ibidem*.

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

ao longo da sua utilização, haja vista a possibilidade de discriminações diretas ou indiretas, por associação, que não podem ser toleradas ou justificadas, pois isso não condiz com a Constituição de 1988. Para o exercício do direito de revisão, faz-se necessário:

> Não diferente do sistema europeu, não pode existir um exercício efetivo do direito de revisão sem que o indivíduo possa apresentar a sua percepção de como os dados devem ser analisados e de onde podem existir erros, discrepâncias ou mesmo de por que determinado fator não se aplica diretamente a ele ou ela. O direito à explicação é, portanto, no mínimo, um pressuposto para o exercício dos outros direitos, particularmente o de requerer uma revisão[488].

Para Danielle Citron e Frank Paquale[489], deve ser desenvolvido o devido processo legal tecnológico (*technological due process*) para que os algoritmos estejam de acordo com algum critério de análise e de revisão para assegurar a sua justiça e acurácia. Os autores defendem também que seja aplicado um procedimento às decisões tomadas baseadas em algoritmos que façam previsões. Os princípios que servem de fundamento para esse devido processo tecnológico são os seguintes: da transparência, da acurácia, da *accountability*[490], da participação e da justiça[491].

Os consumidores cadastrados terão diferentes etapas ao longo do procedimento, que incluem: a coleta dos dados sobre os indivíduos; o cálculo feito a partir dos dados coletados para a pontuação; o uso da pontuação (*score*) por empregadores ou outros para a tomada de decisão[492]. Em uma primeira

---

[488] SOUZA; PERRONE; MAGRANI, 2020, p. 256.

[489] "How should we accomplish accountability? Protections could draw insights from what one of us has called 'technological due process' — procedures ensuring that predictive algorithms live up to some standard of review and revision to ensure their fairness and accuracy" CITRON, Danielle Keats; PASQUALE, Frank A. The scored society: due process for automated predictions. **Washington Law Review**, Washington, v. 89, p. 01-33, 2014. Disponível em: https://ssrn.com/abstract=2376209. Acesso em: 03 fev. 2023. p. 19.

[490] De acordo com a ANPD consiste na responsabilização e prestação de contas (AUTORIDADE..., 2021).

[491] "Nonetheless, the underlying values of due process — transparency, accuracy, accountability, participation, and fairness — should animate the oversight of scoring systems given their profound impact on people's lives" (CITRON; PASQUALE, 2014, p. 20).

[492] "The first step toward reform will be to clearly distinguish between steps in the scoring process, giving scored individuals different rights at different steps" (CITRON; PASQUALE, 2014, p. 20).

etapa as pessoas deveriam ter o direito de inspecionar, verificar se os dados estão corretos, contestá-los e saber a origem deles[493].

Então, a segunda fase desse processo seria o cálculo dos dados, que de preferência deveria ser público. E todo o processo deveria ser examinado[494]. Não obstante isso, o segredo comercial não deveria ser um obstáculo, pois as pessoas devem saber como as notas são dadas e como são feitas as classificações.

Já na terceira etapa, as pessoas deveriam ser notificadas quando a pontuação ou os dados são transmitidos a alguma organização/ entidade[495]. Na quarta e última etapa, o sistema de pontuação deveria estar sujeito a requisitos de licenciamento e auditoria, principalmente quando se tratar de pontuação para emprego, seguro e plano de saúde[496].

Os autores sugerem ainda que deveria ser feita uma auditoria[497], que consistiria em realizar testes que possam executar cenários esperados ou não desenvolvidos por especialistas. Além disso, o titular deveria ter acesso a todos os seus dados. Com essa auditoria, existiriam meios para as pessoas entenderem como foram calculadas as suas pontuações[498]. Outra possibilidade seria deixar os consumidores verem o que aconteceria com a alteração

---

493 "1) Gathering data about scored individuals; 2) Calculating the gathered data into scores; 3) Disseminating the scores to decisionmakers, such as employers; 4) Employers' and others' use of the scores in decisionmaking" (CITRON; PASQUALE, 2014, p. 20).

494 "Second, at the calculation of data stage, ideally such calculations would be public, and all processes (whether driven by AI or other computing) would be inspectable" ((CITRON; PASQUALE, 2014, p. 21).

495 "Nevertheless, scored individuals should be notified when scores or data are communicated to an entity" (CITRON; PASQUALE, 2014, p. 21).

496 "The fourth and final stage is the most controversial. We believe that — given the sensitivity of scoring and their disparate impact on vulnerable populations — scoring systems should be subject to licensing and audit requirements when they enter critical settings like employment, insurance, and health care. Such licensing could be completed by private entities that are themselves licensed by the EEOC, OSHA, or the Department of Labor" (CITRON; PASQUALE, 2014, p. 21-22).

497 "Scoring systems should be run through testing suites that run expected and unexpected hypothetical scenarios designed by policy experts.139 Testing reflects the norm of proper software development, and would help detect both programmers' potential bias and bias emerging from the AI system's Evolution" (CITRON; PASQUALE, 2014, p. 25).

498 "With audit trails, individuals would have the means to understand their scores. They could challenge mischaracterizations and erroneous inferences that led to their scores. (CITRON; PASQUALE, 2014, p. 28).

hipotética dos seus históricos de crédito[499]. Essas são algumas das recomendações apresentadas pelo estudo.

Devido à possibilidade de as decisões com base em algoritmos preditivos afetarem o consumo de bens e serviços, o acesso ao crédito para aquisição de moradia, crédito estudantil[500], contratação de seguros, plano de saúde, ou o fomento de atividades produtivas, e diante da complexidade, por exemplo, das relações humanas, sociológicas, históricas, econômicas,

> [...] algoritmos não podem ser a única ou a última palavra em assuntos humanos ou sociais. E tal conclusão decorre não apenas porque algoritmos são secretos ou difíceis de explicar, mas porque são incapazes de oferecer explicações, pelo menos no nível adequado. De acordo com essa perspectiva, todas as tentativas de encontrar explicações convincentes em algoritmos tenderão a ser mal sucedidas[501].

A inteligência artificial e o Direito constituem duas ciências distintas com objetivos distintos, linguagem e técnicas distintas. A primeira utiliza matemática, estatísticas, objetiva a certeza e a objetividade e tem como característica a dificuldade com questões subjetivas e exceções. O Direito, por outro lado, deve debruçar-se sobre os dados concretos, a realidade fática e ter objetividade e imparcialidade. À vista disso, quando se trata de decisões automatizadas, é difícil de sustentar que só elas bastam para entender e atender à complexidade da vida e da desigualdade.

Em relação ao Direito e às decisões automatizadas, parece haver um embate entre a funcionalização[502] do Direito, sua constitucionalização e a

---

[499] "Another approach would be to give consumers the chance to see what happens to their score with different hypothetical alterations of their credit histories" (CITRON; PASQUALE, 2014, p. 28-29).

[500] MULHOLLAND; FRAJHOF, 2019.

[501] FRAZÃO, Ana. Decisões algorítmicas e direito à explicação. **Jota**, [*s. l.*], 24 nov. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/decisoes-algoritmicas-e-direito-a-explicacao-24112021. Acesso em: 30 jan. 2023.

[502] CC/2002: "Art. 421. A liberdade contratual será exercida nos limites da função social do contrato. Art. 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé. Art. 423. Quando houver no contrato de adesão cláusulas ambíguas ou contraditórias, dever-se-á adotar a interpretação mais favorável ao aderente".
CPC/2015: "Art. 1º O processo civil será ordenado, disciplinado e interpretado conforme os valores e as normas fundamentais estabelecidos na Constituição da República Federativa do Brasil , observando-se as disposições deste Código".

“metrificação ou contabilização”[503] das condutas e das decisões: “[...] é possível sistematizar três elementos desse processo que desafiam a racionalidade jurídica: o reducionismo, a presunção de racionalidade estatística e a autoexecutividade das decisões algorítmicas”[504]. Por outro lado, deve ser levada em consideração a linguagem utilizada no âmbito jurídico:

> [...] natureza linguística das regras jurídicas. Por vezes, as prescrições de condutas podem ser fortemente genéricas e indeterminadas, cuja aplicação dependeria de maior exercício de interpretação. Esse é o caso dos princípios jurídicos, colocados, como propõe Alexy, como a dimensão normativa dos valores. Em extremo oposto estariam as regras que descrevem minuciosamente as condutas previstas para os agentes dos sistemas regulatórios. Embora com configurações distintas, ambas as espécies de regra são construções linguísticas prescritivas de conduta direcionadas a controlar a conduta futura de agentes no sistema regulatório. E seja qual for a configuração, as regras corporificam decisões políticas, de forma que o sucesso da regulação jurídica pode ser medido conforme a política que incorporam se mostre efetiva ou não[505].

Além disso não é possível dizer que as decisões são neutras. Por outro lado, a generalização é uma das características da máquina, pois a partir das estatísticas ela projeta o que pode ou não ocorrer em determinadas situações:

> Dando-se início à análise, a generalização é uma característica indelével ao agrupamento que constitui o mutualismo do seguro e, igualmente, ao método estatístico que se utiliza para fazê-lo. Com base em teorias probabilísticas, a estatística serve de instrumento para se encontrarem relações ou padrões entre variáveis disponíveis, não necessariamente — ou melhor, raramente — ocupando-se de relações de causa e efeito entre elas. Em outras palavras, parte-se de alguns dados disponíveis e tem-se como fim o alcance da mais apurada informação em uma determinada situação[506].

Portanto, entende-se que, para a avaliação do risco, faz-se necessária a generalização[507]. No entanto, para evitar discriminações, deve-se ter como guia das operações o princípio da não discriminação, assim será possível prevenir e reprimir as discriminações e generalizações não toleradas pelo ordenamento

---

[503] FRAZÃO, 2020, p. RB-3.4.
[504] *Idem*.
[505] *Ibidem*, p. RB-3.2.
[506] JUNQUEIRA, 2020a, p. RB-1.4.
[507] *Ibidem*.

jurídico[508]. É possível que a discriminação ocorra em dois momentos distintos, na coleta de dados e na tomada da decisão, como se vê:

> (i) os dados não são suficientemente representativos; (ii) os dados refletem comportamentos pretéritos que já são considerados discriminatórios – e que serão repetidos, naturalmente, pelos algoritmos; (iii) pela falta de cuidado no uso de dados pessoais sensíveis – seja pela supressão desses dados, que pode autorizar inferências e correlações espúrias, seja pelo uso desautorizado e pouco cuidadoso desses dados que, por já traduzirem informações potencialmente discriminatórias, podem interferir no processo decisório; e (iv) pela anonimização de dados pessoais que pode acabar sendo revertida pela leitura do algoritmo[509].

No processamento de dados, também podem ocorrer discriminações indevidas como:

> (v) do desenho algorítmico, desenhada para prestigiar ou prejudicar, de forma injustificada, grupos específicos; (vi) do modelo e treinamento do algoritmo, que pode vir a ser ensinado a produzir *outputs* discriminatórios; e (vii) das correlações e inferências produzidas no processo de leitura dos dados – e que, em grande medida, ocorrem como consequência da opacidade algorítmica —, mas que podem produzir resultados não condizentes com a realidade e injustificadamente prejudiciais para determinados grupos[510].

Apesar de a negativação e a restrição do crédito terem como objetivo incentivar certas condutas e que a partir delas as pessoas e a sociedade possam também se beneficiar, como o pagamento em dia, a LCP igualmente tem como objetivo impor o dever-ser, isto é, condutas positivas. Mas pode haver uma relação entre o dever-ser e a manipulação algorítmica para que as pessoas ajam de maneira que possa ser prejudicial à sua personalidade. Elas podem se sentir obrigadas a terem determinados comportamentos que não condizem com a sua personalidade para se encaixarem nos termos exigidos para melhorar a sua nota (valor).

Para a concessão de auxílio emergencial, que tinha natureza de uma política de transferência de renda (Lei n. 13.982/2022), durante a pandemia,

---

[508] *Ibidem*.
[509] LINDOSO, Maria Cristine. O uso do *compliance* e das políticas de proteção de dados como formas de coibir a discriminação algorítmica. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022. p. RB-13.2.
[510] LINDOSO, 2022, p. RB-13.2.

foram utilizadas decisões automatizadas, por meio de um aplicativo[511]. Utilizou-se diversas bases de dados do governo federal. O prazo para que as pessoas contestassem a decisão no próprio aplicativo era de 10 (dez) dias[512]. A revisão foi feita por uma reanálise a partir das bases atualizadas, no mês posterior à contestação[513].

Contudo, não havia outras formas administrativas de revisão, por isso, foi necessário o ingresso de inúmeras ações individuais e coletivas via judicial[514]. A pesquisa realizada identificou quatro obstáculos: (i) ausência de documentação requerida, (ii) exclusão digital, (iii) limitação de acesso à justiça e (iv) bases de dados desatualizadas e erros cadastrais[515]. Cabia à Dataprev construir dos algoritmos do programa e processar o reconhecimento dos direitos dos requerentes[516]. Contudo, diante da dificuldade de acesso ao aplicativo, foi realizada uma parceria com os Correios para a solicitação do auxílio[517].

Há diversos elementos para se aferir sobre a dificuldade de essas pessoas contestarem as decisões: a ausência de auxílio humano contribuiu para o ingresso de diversas ações perante o Poder Judiciário; o fato de muitas pessoas não disporem de dispositivos tecnológicos e/ou serem analfabetas digitais; a falta de documentos suficientes; a impossibilidade de contestação, efetivamente, da decisão automatizada.

---

[511] No auxílio emergencial o prazo para desemprego deveria ser 03 (três) meses anteriores à pandemia, contudo muitas pessoas ficaram desempregadas por causa ou no início da pandemia. Em razão disso, esse prazo (dado) não parecia justificável para negar o auxílio. Posteriormente foi corrigido, pois não é um critério para exclusão Cf.: TAVARES, Clarice *et al*. **O auxílio emergencial no Brasil**: desafios na implementação de uma política de proteção social datificada. [*S. l.*]: Derechos Digitales América Latina, 2022. Disponível em : https://www.derechosdigitales.org/wp-content/uploads/01_Informe-Brasil_Inteligencia-Artificial-e-Inclusao_PT_22042022.pdf. Acesso em: 29 jul. 2022.; EXPLICABILIDADE algorítmica e revisão das decisões automatizadas. [*S. l.*: *s. n.*], 2022. 1 vídeo (81 min). Publicado pelo canal Data Privacy Brasil. Disponível em: https://www.youtube.com/watch?v=Cntu132CjUc&ab_channel=DataPrivacyBrasil. Acesso em: 29 jul. 2022; CC/2002: "Art. 421. A liberdade contratual será exercida nos limites da função social do contrato. Art. 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios".

[512] EXPLICABILIDADE..., 2022.

[513] TAVARES *et al*., 2022. .

[514] *Ibidem*.

[515] TAVARES *et al*., 2022.

[516] *Ibidem*.

[517] *Ibidem*.

A decisão automatizada pode decorrer dos critérios prévios estabelecidos e em relação aos dados da pessoa. Também pode decorrer de um perfil já estabelecido a partir de diversas análises anteriores para verificar se os sujeitos se encaixam em determinado perfil existente.

Por se tratar de um direito fundamental à proteção de dados pessoais, assim como o princípio da igualdade, deve existir um procedimento para que a pessoa possa exercer o seu direito à autodeterminação informativa. Essa proteção é assegurada pela legislação e o seu exercício pode ocorrer por via judicial ou via extrajudicial, devendo existir um procedimento para isso. Uma vez que a decisão automatizada envolve diversos direitos fundamentais, assim como existe a potencialidade discriminatória, os agentes de tratamentos também devem atentar-se à eficácia horizontal desses direitos.

As decisões automatizadas serão tomadas com base nos dados que compõem o banco de dados com o objetivo de que se evitem prejuízos aos contratantes. Mas deve, principalmente, afastar violações de direitos fundamentais, como a proteção de dados e a não discriminação de pessoas ou de grupos. Nesse sentido, os três principais princípios que norteiam a coleta de dados são: a finalidade, a adequação e a necessidade deles. Antes da coleta dos dados, as pessoas devem ser informadas para qual finalidade serão utilizados e se serão compartilhados.

Para aplicação e eficácia dos direitos fundamentais, faz-se necessária uma interpretação dialógica em que haja a harmonia e a integridade do sistema jurídico[518]. Para a efetivação desse procedimento, deve ser observada a transparência, o tratamento de dados compatível com a finalidade da coleta, a garantia do dos direitos de acesso, retificação e cancelamento, a proteção dos dados sensíveis, a limitação temporal, a segurança dos dados pessoais[519]. Isso foi proposto durante a elaboração do *Fair Information Principles*, e consistia no devido processo informacional (o contraditório, a ampla defesa e a imposição de regras de procedimento) no tratamento dos dados pessoais[520].

---

[518] MENDES, 2014.
[519] *Ibidem*.
[520] MARTINS, 2022.

Contudo, nem todos os dados e informações disponíveis poderão ser utilizados, pois como Rodotà[521] menciona há informações pessoais sensíveis que estão abertamente disponíveis, ou seja, por sua própria característica não estão em sigilo. Embora tenham sido disponibilizadas abertamente pelo próprio titular, não devem ser utilizadas por não estarem dentro das autorizações legais, ainda que a obtenção de dados ou informações tenha sido feita de maneira direta ou indireta.

Outro fator a se questionar seria se, a partir do tratamento de dados, obtêm-se dados sensíveis, ou se determinadas informações ou dados podem ser considerados sensíveis, como são coletados os e se são coletados dados disponíveis em outros locais — seja em ambiente virtual ou não. Isso decorre também do princípio da transparência. Trata-se, de fato, de tema complexo e de difícil controle.

A título de ilustração dessa complexidade, retoma-se um caso concreto em que, em uma análise de dados, se retirou o gênero e mesmo assim mulheres foram prejudicadas na seleção de empregos, privilegiando-se o gênero masculino mesmo quando eram elas que tinham mais qualificação para o cargo[522]. Isso pode ocorrer, por exemplo, quando se tira o dado racial, mas por associação ou correlação, a IA chega a uma discriminação utilizando-se de outra variável — como ocorreu no citado caso em que um nome ligava uma pessoa a uma determinada etnia/religião, impactando na contratação do seguro[523].

No âmbito dos seguros, Junqueira, por seu turno, defende a possibilidade de utilização do gênero na análise atuarial:

> De tudo o que se deixou registrado e firme na premissa de que o exame de merecimento de tutela da classificação dos riscos pelo segurador deve ser baseado em aspectos legais, sociais e econômicos em um determinado contexto histórico-cultural, defende-se, nestas linhas, a atual possibilidade de utilização do gênero como fator atuarial no

[521] RODOTÀ, 2008.
[522] "É conhecido o caso do sistema de IA de recrutamento de empregados da *Amazon*, que, em 2018, foi desativado pelo seu viés discriminatório. Ao que parece, mesmo não se tendo valido do gênero como *input*, o algoritmo foi capaz de identificá-lo, por meio de algumas palavras utilizadas nos currículos e, como resultado, desenvolveu um viés a favor dos homens — historicamente, o gênero predominante nas empresas de tecnologia" (JUNQUEIRA, 2020a, p. RB-3.3).
[523] JUNQUEIRA, 2020a.

> contrato de seguro de automóvel no Brasil. Além de ser tido como aceitável ao público, possuir um baixo grau de intrusão, ser um generalização exógena e não reforçar desvantagem sistêmica na sociedade, o gênero do candidato a segurado trata-se de um elemento que possui uma conexão lógica plausível (embora não inquestionável) com o risco garantido pelo segurador no âmbito do seguro de automóvel. Ou seja: uma análise funcional da tutela antidiscriminatória impõe a conclusão de que, se objetiva e razoável, feita com base em dados fiáveis e atualizados, bem como oferecendo, no geral, melhores condições às mulheres, o uso do gênero como um dos fatores de cálculo do prêmio no seguro de automóvel corresponde a uma *diferenciação admissível*[524].

Na distinção entre atributos endógenos ou exógenos, a discriminação que tiver efeitos endógenos é sempre discriminatória[525]. Agora, se for exógena, ainda que decorra de um dado pessoal sensível, o resultado pode não ser considerado discriminatório[526]. Ademais, a utilização do gênero na contratação do seguro[527] é considerado um atributo exógeno entre grupos, por isso, não é proibida a utilização[528].

Portanto, a variável que causa a distinção pode ser interna ou externa, por exemplo, o número de acidentes entre jovens do sexo masculino tem como base dado estatístico, logo, trata-se de um aspecto exógeno. No entanto, se a discriminação tiver como fundamento questões históricas[529] de discriminação, por exemplo, será um aspecto endógeno[530].

---

[524] *Ibidem*, 2020, p. RB-1.8.
[525] MENDES; MATTIUZZO; FUJIMOTO, 2020.
[526] *Ibidem*, 2020.
[527] "O gênero guarda forte correlação com a taxa de acidentes de trânsito e, assim, é frequentemente utilizado para precificação. Neste segundo cenário, porém, o gênero não é uma variável endógena, mas sim exógena, pois nada no fato de que os homens pagam mais por seguros leva esse grupo a efetivamente se envolver em mais acidentes" (MENDES; MATTIUZZO; FUJIMOTO, 2020, p. 437).
[528] MENDES; MATTIUZZO; FUJIMOTO, 2020.
[529] "A título de ilustração, dois casos relatam os malefícios do perfilamento (*profiling*), com uso de dados pessoais que geraram tratamento discriminatório. Os casos ocorreram nos EUA e se referiram à contratação de serviços médicos e de seguridade. No primeiro caso, algumas seguradoras utilizaram dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez" (MULHOLLAND, 2021, p. 04).
[530] "[...] exemplo anterior do mercado de trabalho para esclarecer essa distinção, é possível afirmar que as mulheres foram, historicamente, mais envolvidas na criação dos filhos e em tarefas domésticas que os homens. No entanto, esse é um resultado do fato de que a elas foram dadas menos oportunidades profissionais, consideradas por muito tempo como incompatíveis com as tarefas domésticas, e não uma característica inerente do sexo feminino que torna as mulheres menos capacitadas ou menos interessadas em oportunidades profissionais. A

A distinção entre dados pessoais e dados pessoais sensíveis é relevante, todavia, devem ser levados em consideração a situação concreta e o contexto, como dados do Instituto Brasileiro de Geografia e Estatística (IBGE), por exemplo, uma vez que se pode variar o discrímen ou a discriminação positiva.

Há seguros que coletam apenas as seguintes informações para a contratação: *e-mail*, a placa do carro e o CEP, pois apenas com esses dados é possível buscar pela internet mais de 30 (trinta) fontes de informações para oferecer uma apólice adequada[531]. Outros, por sua vez, colhem dados de aplicativos utilizados pelos clientes, os quais podem ser uma fonte de stress ao contratante quando ele estiver dirigindo, por estar em estado de vigilância constante — por isso, ele deve saber disso anteriormente e consentir. Em um contexto como esse, volta-se à questão já discutida se todo e qualquer dado tornado público pelo titular atende à finalidade do processamento dos dados. Ademais, eles devem atender aos princípios da necessidade e da adequação para uma determinada contratação.

Renato Monteiro e Sinuhe N. e Cruz propõem uma cláusula geral do devido processo informacional aos sistemas de *credit scoring*:

> (i) isentos, ou seja, sem vieses que possam acarretar conclusões discriminárias ou que favoreçam ou desfavoreçam desproporcionalmente alguém em face dos seus dados;
> (ii) informados, ou seja, é necessário estruturar processos e procedimentos que garantam o acesso aos dados utilizados no processo automatizado e também aos critérios utilizados para valoração e cruzamento de tais dados;
> (iii) compreensíveis, pois não basta o simples fornecimento dos dados e de informação sobre o seu processamento, é necessário que seja dada uma efetiva explicação sobre o funcionamento do algoritmo, de tal forma que o destinatário possa compreender os seus detalhes e a sua lógica para, caso não concorde ou identifique uma prática inadequada com impactos desproporcionais em seus direitos, desafiá-la;
> (iv) a possibilidade de recorrer de uma decisão, o elemento de recorribilidade, depende do desenvolvimento de estruturas formais que viabilizem o desafio à decisão automatizada sem que sejam

consequência da discriminação, nesse caso, leva à confirmação da hipótese inicial, pois estamos analisando uma variável endógena" (MENDES; MATTIUZZO; FUJIMOTO, 2020, p. 437).

[531] CARVALHO, Isadora. O preço do seu seguro será definido pela forma como você dirige. **Quatro Rodas**, [*s. l.*], 05 mar. 2021. Disponível em: https://quatrorodas.abril.com.br/noticias/o-preco-do-seu-seguro-sera-definido-pela-forma-como-voce-dirige/. Acesso em: 30 jan. 2023.

> criados obstáculos procedimentais impeditivos, como alguns dos elencados no Recurso Especial n. 1.304.736/RS; e
> (v) na existência de uma estrutura que permita a recorribilidade, a revisão da decisão, que deve ser feita por agente isento, independentemente da primeira da primeira entidade decisora, com poder para alterar o resultado do processo automatizado[532].

O princípio da finalidade está expresso na LGPD, assim como na Lei do Cadastro Positivo, art. 5º, inciso VII, que é aquele que consiste em "[...] ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados". Um exemplo de violação da finalidade é a utilização do serviço de proteção ao crédito para contratação de um funcionário[533], pois os dados foram obtidos originalmente para a outra finalidade.

O princípio da finalidade relaciona-se com a atividade a ser desenvolvida ou com o serviço prestado e, uma vez que não atendem à finalidade descrita, os dados coletados não poderão ser utilizados[534]. Isso contribui para a não circulação deles[535]:

> De consequência, a referência a tal princípio torna-se essencial para determinar a legitimidade do uso dos dados coletados, seu tempo de conservação, a admissibilidade de sua interconexão com informações contidas em outros bancos de dados[536].

O indivíduo deve ser informado caso houver alteração na finalidade, no destino e no compartilhamento, quantas vezes eles ocorrerem.

Adiante, há diversas maneiras de se regulamentar a inteligência artificial, a qual deve ser desenvolvida de acordo com a legislação vigente (*by design*)[537], com ética, com a implementação de boas práticas e com governança por parte daqueles que desenvolvem e operam o sistema.

---

[532] MONTEIRO; CRUZ, 2022, p.188.
[533] MENDES, 2014.
[534] RODOTÀ, 2008.
[535] *Ibidem.*
[536] *Ibidem*, p. 104.
[537] "Em suma, a dinâmica por trás do conceito do *privacy by design* é a perfeita associação entre o direito e tecnologia, de modo a implementar no desenho da arquitetura da rede mecanismos técnicos que possam garantir a efetividade de direitos dos seus usuários, por padrão, em benefício do ser humano. Como consequência, o ambiente digital se tornaria espontaneamente mais seguro, ético e saudável, consolidando uma cultura de proteção de dados". JIMENE, Camilla do Vale. **Capítulo VII, da segurança e das boas práticas**. *In*: MALDONADO**,** Viviane Nóbrega; BLUM, Renato Opice (**c**oord.). LGPD**: Lei Geral de Proteção de Dados comentada.** 2**.** ed. São Paulo: Thomson Reuters Brasil, 2019. p. RL-1.14.

Nesse sentido, o titular de dados tem direito à oposição, à informação e à revisão da decisão automatizada. A proteção de dados tem aspecto negativo, positivo e dinâmico[538], pois há a possibilidade de se acompanhar como o dado tem sido utilizado. Além disso, há diversos meios de proteção, seja pelo indivíduo, pelas instituições privadas e por órgãos públicos que têm o dever de evitar violação de direitos ou de discriminações.

Dentro do sistema europeu, a decisão automatizada[539] ocorre em situações específicas e quando não afeta significativamente e atinge a esfera jurídica[540] do sujeito, não sendo esse obrigado a submeter-se a ela. É possível, nas hipóteses do art. 22, n. 2 do RGPD, que cada Estado-membro legisle sobre a utilização das decisões automatizadas. No entanto, o direito à explicação consta somente do considerando 71 do RGPD, que não tem força normativa. Por isso, houve muita discussão sobre a existência desse direito no sistema europeu. Na União Europeia (RGPD) o direito à oposição pode ser exercido via judicial ou extrajudicial[541], assim como o titular dos dados tem a possibilidade de:

> Logo que o titular dos dados exerça esse direito, o responsável pelo tratamento tem de interromper (ou evitar que seja iniciado) o processo de definição de perfis, a não ser que possa apresentar razões imperiosas e legítimas que prevaleçam sobre os interesses, os direitos

---

[538] RODOTÀ, 2008.

[539] O Regulamento Geral sobre a Proteção de Dados (RGPD), em seu art. 22, é mais detalhista sobre as decisões automatizadas: "O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.2. O n. 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados.3. Nos casos a que se referem o n. 2, alíneas a e c, o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.4. As decisões a que se refere o n. 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, n. 1, a não ser que o n. 2, alínea a ou g, do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular".

[540] SOUZA; PERRONE; MAGRANI, 2020.

[541] VERONESE, Alexandre. Os direitos de explicação e oposição diante das decisões automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

> e as liberdades do titular dos dados. O responsável pelo tratamento poderá igualmente ter de apagar os dados pessoais em causa[542].

A LCP estabelece expressamente que o legislador optou pelo *opt in*. Diante disso, a pessoa poderá solicitar a sua retirada do cadastramento depois que tiver sido criado. Como mencionado, diferentemente da RGPD[543], para o qual o titular tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, a LGPD parte do pressuposto que podem ser tomadas decisões unicamente automatizadas.

As expressões que são utilizadas para designar um desenvolvimento da tecnologia que observa os princípios previstos na LGPD são *by default*[544] ou *by design*[545]. Portanto, os princípios devem ser observados no processo de desenvolvimento do sistema[546].

Uma das técnicas utilizadas pela inteligência artificial busca "[...] identificar padrões a partir da análise de dados por meio de uma lógica matemática (algoritmo) e o aprendizado de máquina (*machine learning*)"[547]. Neste capítulo, abordar-se-ão as decisões automatizadas tomadas pelas máquinas, ou seja, programas de computador a partir dos dados inseridos (*inputs*), os quais são tratados e apresentam resultados, e das decisões (*outputs*), por meio de processos dedutivos e análises estatísticas, além dos resultados decorrentes das correlações realizadas pela inteligência artificial[548].

No entanto, como já mencionado, a linguagem e as rações utilizadas pela máquina e as utilizadas pelo ser humano para a tomada de decisão são distintas, haja vista que "[...] matemática que privilegia padrões e correlações – mas não

---

[542] GRUPO…., 2017, p. 20.
[543] RGPD, art. 22, n. 1: "O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar."
[544] "O art. 25 (2) do RGPD prevê, inclusive, que o controlador deverá aplicar medidas técnicas e organizacionais para assegurar que, por padrão (*privacy by default*), só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento, de acordo com a quantidade de dados pessoais coletados, à extensão do seu tratamento, o prazo de armazenamento e à sua acessibilidade. Em especial que, por padrão, dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas" (MAGRANI, 2019, p. 127).
[545] MALDONADO; BLUM, 2019.
[546] MAGRANI, 2019.
[547] BIONI; LUCIANO, 2019, p. RB-11.1.
[548] MULHOLLAND; FRAJHOF, 2019.

causalidades, não pode levar a explicações racionais, inteligíveis e convincentes”[549]. Por isso, tem-se sustentado que, diante dessa distinção, espera-se que os algoritmos sejam opacos. Além do mais, só a análise dos dados utilizados, ou seja, inseridos (*inputs*), não é suficiente para aferir como ocorreu o resultado apresentado[550].

O mais indicado, então, seria a análise do resultado da decisão da tomada da máquina para se investigar a decisão e se houve discriminação[551]. No entanto, como ficou evidente no Capítulo 2, existem a LGPD, o CDC e a LCP, que abordam como e quais dados podem ser coletados e por quanto tempo, normas que também devem ser observadas para o *input*. Mas novos estudos têm se voltado para o resultado da decisão automatizada[552].

> A partir dessa constatação, os autores demonstram a insuficiência da tutela tradicionalmente dedicada à proteção de dados diante dos recentes avanços tecnológicos e propõem um “direito a inferências razoáveis” (*right to reasonable inferences*) como resposta[553].

Nessa esteira, Junqueira[554] entende que, desde a modelagem, treinamento do sistema de inteligência artificial e o resultado, o agente de tratamento deve atuar proativamente a fim de evitar enviesamentos. Para isso, deve ser feito o “[...] fuso de métricas tradicionais de exame de performance dos algoritmos com outras de equidade”[555], o que tornará possível verificar as taxas de falso positivo e falso negativo entre diferentes grupos demográficos[556], por exemplo.

Os agentes de tratamentos de dados devem observar as restrições que as leis impõem para coleta de dados (*inputs*), assim como observar a decisão dada pela máquina para verificar se não houve abusos ou decisões discriminatórias não toleradas. Também é possível que observem quais

---

[549] FRAZÃO, 2021.
[550] *Ibidem*.
[551] *Ibidem*.
[552] JUNQUEIRA, 2020a.
[553] *Ibidem*, p. RB-3.4.
[554] *Ibidem*.
[555] *Ibidem*, p. RB-3.1.
[556] JUNQUEIRA, 2020a.

inferências puderam ser extraídas a partir dos dados[557]. Entende-se por inferências razoáveis o direito de ser avaliado de forma razoável — ideias propostas por Sandra Wachter e Brent Mittelstadt. Trata-se de um dos métodos possíveis para se analisar as decisões automatizadas[558]. No entanto, para Junqueira, essa teoria de inferência razoável não enfrenta o problema das discriminações indiretas[559].

Entende-se que o princípio da não discriminação fundamenta a proteção dos dados sensíveis, que contribuem para o acesso aos direitos sociais, o direito à saúde, ao crédito, à moradia[560].

Há diversos direitos previstos para tutelar a proteção de dados pessoais previstos na LGPD, no CDC e na LCP, haja vista que, entre os problemas enfrentados pelo titular dos dados, estão: não saber quais dados pessoais foram utilizados, a procedência deles, se estão atualizados, por exemplo[561]. Outra problemática é de que maneira o algoritmo chega a determinado resultado e, por fim, para qual finalidade esse será utilizado[562]. As legislações estudadas até aqui definem os seguintes direitos aplicáveis à decisão automatizada:

i) direito geral de informação;
ii) direito de acesso;
iii) direto de notificação;
iv) direito de retificação, cancelamento e bloqueio dos dados; e
v) direto de não se ficar sujeito a uma decisão individual automatizada[563].

O direito à informação compreende saber da existência de banco de dados com as suas informações e de quais os objetivos com a utilização deles — conteúdo que se expressa pela transparência[564]. O consumidor deve também

[557] *Ibidem*.
[558] *Ibidem*.
[559] *Ibidem*.
[560] MULHOLLAND; FRAJHOF, 2019.
[561] MONTEIRO; CRUZ, 2022.
[562] *Ibidem*.
[563] MENDES, 2014, p. 65-66.
[564] MENDES, 2014.

saber quais são os seus direitos, quem são os agentes de tratamento e se há transferência dos seus dados[565].

O direito de acesso assegura que se saiba quais são os dados que constam do banco de dados, o que será feito mediante requisição e em qual banco de dados ficarão armazenados os dados[566]. O direito de notificação corresponde à comunicação ao consumidor de que houve a coleta de seus dados, possibilitando o conhecimento sobre quem a fez e a notificação de em caso de transferência[567] (LCP, art. 4, §4º e CDC, art. 43, §2º).

Por seu turno, o direito à retificação dos dados ocorre quando eles não correspondem à verdade — pode-se solicitar o cancelamento, isto é, a exclusão deles, se já houve o cumprimento da finalidade, por exemplo. Todos que tenham recebido os dados deverão ser informados como poderão exercer os seus direitos[568]. Quanto ao direito de não se ficar sujeito a uma decisão individual automatizada, Mendes explica que:

> Tal direito consiste, na realidade, em uma regra de justiça, que visa assegurar a possibilidade de defesa do titular e a mínima participação do titular em um processo de decisão tomado com base em seus dados e que afetará de forma significativa as suas oportunidades de vida[569].

Caitlin Mulholland e Isabella Z. Frakjhof defendem que o direito à informação abrange a explicação sobre: "(i) o algoritmo em si e sua forma de funcionamento; (ii) o racional do algoritmo para a tomada de decisão; ou (iii) o momento no qual poderá o titular pleitear tal direito, se antes ou depois da tomada de decisão automatizada"[570].

Convém mencionar que o art. 18 da LGPD elenca, entre os direitos dos titulares[571], o de requisitar acesso aos dados que estão sendo tratados. Além

---

565 *Ibidem*.
566 *Ibidem*.
567 *Ibidem*.
568 *Ibidem*.
569 MENDES, 2014, p. 68.
570 FRAZÃO; MULHOLLAND, 2019, RB –13.2.
571 LGPD: "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos

disso, os titulares poderão requerer a correção de dados incompletos, inexatos ou desatualizados, bem como a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto. Nota-se, nesse dispositivo, a possibilidade de retificar os dados bem como de o titular ser informado sobre o tratamento de dados, ou seja, o agente de tratamento de dados não pode se abster dessas atitudes.

Esses direitos garantem a efetividade do procedimento para a proteção dos dados. Para esse propósito, deverá ser estabelecida regulamentação específica. Devem ser definidos procedimentos e prazos para que que as solicitações feitas pelo titular possam ser atendidas em casos de uso de decisões automatizadas[572].

Como se nota, a LGPD é, como o próprio nome diz, “Geral”. Portanto, trata-se de uma norma principiológica, não estabelecendo um procedimento específico[573] a ser seguido, como a RGPD. Isso ocorre até porque, a depender da espécie de relação, haverá a necessidade de regulamentação especial, como em situações que envolvem dados e informações sobre a saúde do cliente. Nesse sentido, essa regulamentação também competirá a Autoridade Nacional de Proteção de Dados (ANPD).

Entre os direitos garantidos pela Lei do Cadastro Positivo está o de acesso às informações que constem dos bancos de dados sem a necessidade de justificar o requerimento (art. 5º, inciso II):

---

dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional”.

[572] ABILIO, Vivianne da Silveira; FRAZÃO, Ana; OLIVA, Milena Donato. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 672.

[573] BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeamento convergência na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

> [...] acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado;

O acesso à informação contribui para a transparência e para o direito à informação, assim como para a redistribuição de poder[574]. Além disso, atende ao interesse e funcionamento do mercado em se ter informações corretas dos titulares de dados[575]. Como já mencionado, há uma assimetria entre quem administra o banco de dados ou tem acesso a eles em relação aos consumidores.

Para o exercício do acesso à informação, o art. 9º, incisos I e II da LGPD, garante ao titular poder saber sobre a finalidade específica do tratamento e a forma e a duração do tratamento, observados os segredos comercial e industrial; assim como o titular tem direito a obter do controlador, em relação aos dados tratados, a qualquer momento e mediante requisição, confirmação da existência de tratamento e acesso aos dados (LGPD, art. 18, incisos I e II).

No art. 19, inciso II, consta, ainda, como direito a requisição do titular sobre quais "[...] os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular". Isso pode significar que está a:

> [...] se referir aos parâmetros utilizados para a tomada de decisão, ainda que a alusão a procedimentos na regulação brasileira permita uma interpretação de que o controlador deve informar mais sobre o modo como o algoritmo opera e sua funcionalidade[576].

Esse artigo não é exaustivo. Além disso, o § 4º prescreve que a ANPD poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do *caput*, para os setores específicos.

Por isso, Mendes[577] defende que o consumidor tem direito de saber qual é a sua pontuação (nota), como também a lógica do *scoring*, ou seja, os dados

---

[574] RODOTÀ, 2008.
[575] *Ibidem*.
[576] SOUZA; PERRONE; MAGRANI, 2020, p. 275.
[577] MENDES, 2014.

levados em consideração e quais os fatores que influenciaram o valor de forma positiva ou negativa.

A retificação dos dados é importante, pois a projeção digital sobre a pessoa pode afetá-la, como foi visto no capítulo anterior. Dessa maneira:

> Além do princípio da qualidade dos dados, o direito de correção é uma construção que deriva da perspectiva da identidade do sujeito e não do direito à privacidade. É o primeiro direito de personalidade que determina a necessidade de haver uma correspondência fidedigna entre a pessoa e seus dados pessoais. A esfera do que é público ou privado revela-se incompleta para dar vazão a esse tipo de dinâmica normativa[578].

Ademais, a limitação temporal para a utilização de dados coletados e tratados significa que esses poderão ser utilizados dentro de um determinado período. Mas, conforme foi visto no capítulo anterior, há distinção de prazos entre o CDC e LCP, embora a LGPD não trate desse tema. Mendes[579] afirma que a limitação temporal também deve ser observada na transferência de dados pessoais. A limitação temporal tem correlação com o princípio da finalidade[580]:

> Como regra geral, entende-se que os dados não devem ser armazenados por um período superior ao tempo necessário para atender à finalidade pela qual eles foram coletados. Ademais, uma avaliação de risco também é relevante para determinar o prazo de armazenamento e processamento. Isto é, quanto maiores os riscos e a probabilidade de efeitos negativos para o consumidor, menor deve ser o tempo de armazenamento[581].

Além do direito à informação, deve-se levar em consideração o direito à autodeterminação informativa (LGPD, art. 2, inciso II), haja vista que o direito fundamental à proteção de dados pessoais abarca o controle dos dados[582].

Embora a nova redação aparente ser uma tentativa de restrição à contestação à decisão automatizada, ao se analisar a Constituição da República de 1988, a LGPD, o CDC, o MCI, a LCP, os princípios e os direitos fundamentais, de fato, parece ter sido essa mesmo a tentativa. No entanto, ao se levar em conta

---

[578] BIONI, 2020a, p. 58.
[579] MENDES, 2014.
[580] *Ibidem*.
[581] *Ibidem*, p. 220.
[582] MENDES, 2014.

o ordenamento jurídico, isso pode ser afastado, porque é possível se estabelecer os mecanismos adequados. A legislação brasileira menciona diversas vezes o direito ao segredo comercial ou industrial, mas deve haver a compatibilização, a harmonização com os direitos fundamentais. A RGPD, em seus artigos 21 e 22, não dispõe sobre essa restrição; o Considerando 71 também trata desse tema[583].

Ademais, Zanatta entende que a criação de um perfil acarreta obrigações de informação, uma obrigação antidiscriminatória e uma dialógica. Portanto, ao

---

[583] "ARTIGO 21. O Direito de oposição **"**O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.o, n.º 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim. O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se referem os n. 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações. No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas. Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.º 1, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público. ARTIGO 22.O Decisões individuais automatizadas, incluindo definição de perfis - O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. O n.º 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. Nos casos a que se referem o n.º 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. As decisões a que se refere o n.º 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.o, n.º 1, a não ser que o n.º 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular". UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas, Bélgica: Parlamento Europeu, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 25 ago. 2022.

ser realizada a perfilização por meio de uma decisão automatizada, haverá uma relação entre o titular dos dados e o controlador[584], ou seja, um processo dialógico, com fundamento no princípio da transparência (LGPD, art. 6º, inciso VI):

> [...] não basta um sistema unidirecional e não dialógico no provimento das informações. Esse é o antigo modelo da década de 1990, sob o qual o Código de Defesa do Consumidor inicialmente se estruturou. Uma leitura "dialógica" do princípio da transparência nos leva a um outro patamar quando se trata de processos de comunicação e de aprendizagem. Como sustentam Andrew Selbst, do Data & Society *Research Institute*, e Julia Powles, da Cornell Tech, existe sim um direito à "informação significativa sobre a lógica envolvida em decisões automatizadas"[585].

Portanto, o processo dialógico de explicação consiste "[...] em uma ação relacional e 'construção conjunta do conhecimento'"[586]. Para isso as informações devem ser claras, precisas e facilmente acessíveis.

Pode-se dizer que há uma diferença entre a visão nos Estados Unidos, fundada no devido processo legal que se baseia em um regime de transparência na tomada das decisões automatizadas[587]; e na Europa, em que se utiliza a RGPD, segundo a qual as soluções para as decisões tomadas pela máquina seriam o acesso à informação, a transparência, o direito à explicação, com os quais o titular poderá exercer o controle quanto ao uso de seus dados[588].

Além disso, parece ser mais indicada a utilização de diversas técnicas ao longo do processamento dos dados até a tomada de decisão pelo sistema de IA, as quais poderão evitar discriminações:

> i) anteriores ao processamento de dados (pré-processamento), ii) ao longo do seu processamento (in-processamento) e iii) após o seu processamento (pós-processamento). A despeito de seguirem estratégias distintas, elas se encaixam na referida metodologia da "equidade por *design*"[589].

---

[584] LGPD: "Art. 5º, inciso VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".
[585] ZANATTA, 2020, p. 541.
[586] *Idem*.
[587] SOUZA; PERRONE; MAGRANI, 2020.
[588] *Ibidem*.
[589] JUNQUEIRA, 2020a, p. RB-3.3.

Não obstante isso, desde os testes feitos para o desenvolvimento da inteligência artificial, deve haver diversidade, a fim de que grupos vulneráveis, para quem a tecnologia está a ser desenvolvida, sejam levados em consideração. Por isso, advoga-se pela inclusão das pessoas na participação na criação desses sistemas, pela educação tecnológica e pela discussão ampla e geral sobre tecnologia em si[590] — e, mais especificamente, sobre os limites aplicados à tecnologia e à orientação ética. Pode-se, nesse sentido, mencionar como mecanismos de proteção os relatórios de impactos, os códigos de boa conduta das empresas e dos desenvolvedores dos programas de computador.

O art. 18 da LGPD e o art. 9º e o seu §3º garantem ao titular o acesso facilitado às informações[591] sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.

Também o art. 9, §3º, assegura ao titular o direito de ser informado com destaque sobre a situação em que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito. Ademais, deverá ser informado sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 da LGPD. Portanto, esses dispositivos devem ser empregados a fim de que as pessoas sejam informadas previamente sobre a coleta e tratamento de dados, e também de que serão tomadas decisões automatizadas a partir dos seus dados.

Como o objetivo deste estudo é discutir como se pode evitar discriminações e refletir sobre a revisão da decisão automatizada, deve-se

---

[590] EXPLICABILIDADE..., 2022.

[591] LGPD: “Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador ;V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei”.

demonstrar de que maneira o titular dos dados pode contestar as decisões automatizadas. Para tanto, ele deve ter acesso à informação, para propiciar o exercício dos seus direitos.

3.1 DIREITO À TRANSPARÊNCIA

O princípio da transparência previsto no art. 6º, inciso VI, consiste na "[...] garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e sobre os respectivos agentes de tratamento, observados os segredos comercial e industrial". A transparência a ser observada deve ser "[...] diretamente proporcional ao poder do tratamento dos dados pessoais (qualitativo e quantitativo) e à capacidade de assimilação dos titulares dos novos e dinâmicos produtos e serviços apresentados para o seu uso"[592]. A transparência se coaduna com o direito à informação previsto no art. 6º, inciso III do CDC:

> i) quais os dados pessoais são tratados e para quais finalidade;
> ii) se os dados pessoais são transmitidos para terceiros;
> iii) para quais países os dados pessoais são transmitidos, se for o caso;
> iv) qual é o período de conservação de dados;
> v) quais os mecanismos de segurança utilizados para garantir a segurança dos dados pessoais[593].

A transparência exige que o consumidor seja esclarecido sobre quais os dados utilizados na decisão automatizada, ou seja, que contribuíram para a análise (cálculo) do risco[594]. Ela deve ser entendida como um caminho a ser percorrido, para que seja possível entender a decisão automatizada[595], desde o direito de ser informado sobre a coleta e tratamento de dados. Para isso, deve-se fornecer ao consumidor informações sobre o momento em que os seus dados foram recolhidos, se foram fornecidos diretamente pelos consumidores, ou

[592] MALDONADO; BLUM, 2019.
[593] MENDES, 2014, p. 215.
[594] MONTEIRO; CRUZ, 2022.
[595] PASQUALE, 2014, p. 08.

obtidos de maneira indireta, por um aplicativo, ou inferidos a partir de um perfil anteriormente existente[596].

Em relação à transparência, pode-se apontar críticas apresentadas por Filipe Medon[597], no sentido de que há limites nessa solução. Assim, haveria a possibilidade de manipulações dos algoritmos. Além disso, o segredo comercial é tido como uma limitação. O autor também se atenta para as situações em que se usa o aprendizado profundo da máquina, inviabilizando a transparência, pois não haveria como tecnicamente se revelar como o programa tomou determinada decisão[598]. Aponta a seguinte solução Filipe Medon:

> À luz da alteração, a revisão por pessoa natural passaria a depender da regulamentação da ANPD, que deveria levar em consideração dois critérios básicos: (i) a natureza e o porte da entidade; ou (ii) o volume de operações de tratamento de dados. Tais critérios foram incluídos na lei como uma solução compromissória para atender aos anseios daqueles que, durante o processo legislativo, manifestaram a preocupação de que a revisão por pessoa natural pudesse inviabilizar estratégias e modelos de negócio inovadores, como *startups* e *fintechs* (sociedades empresárias que utilizam inovações tecnológicas para aperfeiçoar o mercado financeiro)[599].

Para a concretização desse princípio, a LGPD (art. 9, §3º) determina que o titular dos dados seja informado sobre o tratamento dos dados pessoais de maneira destacada e sobre como poderá exercer os seus direitos previstos no art. 18[600]. Essa prática consiste em um direito anterior (*ex ante*) de ser informado sobre o tratamento de seus dados quando ele for condição para o fornecimento do serviço, e um direito posterior (*ex post*) de acesso aos dados tratados pelo agente de tratamento, ou seja, o controlador[601].

A LGPD garante que se possa ter confirmação de existência ou o acesso a dados pessoais, o que poderá ser feito mediante requisição em formato simplificado ou por meio de declaração clara e completa, que indique a origem

---

596 GRUPO…, 2017.
597 MEDON, 2020.
598 MEDON, 2020.
599 *Ibidem*, p. RB-17.4.
600 LGPD: "Art. 9º, § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei".
601 JUNQUEIRA, 2020a, p. RB-2.3.

dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento[602]. A partir do requerimento, o controlador tem até 15 (quinze) dias de prazo para responder. Ademais, os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. A recusa em oferecer a informação implica a realização de uma auditoria pela ANPD.

Isabella Frajhof[603], por seu turno, defende que o início dessa discussão deveria ser exatamente quais seriam as informações a que se deve ter acesso, e quais as pessoas, entidades ou grupos deteriam esse direito. Também questiona o argumento sobre o segredo do negócio, uma vez que esse é um assunto diferente do direito fundamental à proteção de dados pessoais, portanto, não haveria pertinência de ambos estarem envolvidos nesse tema[604] — por serem assuntos diferentes, não haveria pertinência de se alegar uma questão do direito concorrencial com o direito fundamental à proteção de dados pessoais.

3.1.1 DIREITO À INFORMAÇÃO

O direito à informação está presente na Constituição da República no art.5º, inciso XIV, no qual consta que "[...] é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional". De acordo com José Afonso da Silva[605], o direito à informação tem uma dimensão e função coletiva.

No Código de Defesa do Consumidor é um princípio previsto no art. 4º, inciso IV: "[...] educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo". É também um direito básico previsto no art. 6º, inciso III: "[...] a informação adequada e clara sobre os diferentes produtos e serviços, com especificação

---

602 LGPD: "Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simplificado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular".
603 EXPLICABILIDADE..., 2022.
604 *Ibidem*.
605 SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 23. ed. rev. atual. São Paulo, 2004.

correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem".

Além disso, também é tratado no art. 46 do CDC, pois os contratos que regulam as relações de consumo, para poderem obrigar os consumidores, deverão dar a eles a oportunidade de tomarem conhecimento prévio de seu conteúdo, portanto, devem ser redigidos de modo a não dificultar a compreensão de seu sentido e alcance.

Não faz sentido restringir o direito à explicação somente às decisões tomadas unicamente com base em tratamento automatizado ante a existência do *habeas data*, do Código de Defesa do Consumidor. Além disso, há na Constituição da República o direito à informação, no art. 5, "§ 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata. § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte".

A crítica[606] apresentada à Lei n. 9.507/1997, que regulamenta o direito de acesso a informações e o rito processual do *habeas data*, diz respeito à necessidade de a petição ser instruída com prova:

> Art. 8º, parágrafo único. A petição inicial deverá ser instruída com prova:
> I - da recusa ao acesso às informações ou do decurso de mais de dez dias sem decisão;
> II - da recusa em fazer-se a retificação ou do decurso de mais de quinze dias, sem decisão; ou
> III - da recusa em fazer-se a anotação a que se refere o § 2° do art. 4° ou do decurso de mais de quinze dias sem decisão.

Isso significa que deve haver recusa administrativa para que a pessoa ingresse no Poder Judiciário, tema esse que não será aprofundado neste estudo. Ademais, o CDC, em seu art. 43, também assegura o direito à informação e o direito de saber quais as informações contêm os cadastros, assim como sobre quais são as suas respectivas fontes.

---

[606] DONEDA, 2020a.

No âmbito da RGPD, entende-se que os responsáveis pelo tratamento dos dados terão que "[...] imperativamente explicar às pessoas em causa, de forma clara e simples, o funcionamento do processo de definição de perfis ou de decisão automatizada"[607].

A Autoridade Nacional de Proteção de Dados (ANPD), por sua vez, pode ser solicitada a atuar nas situações em que (art. 20, §2º) não for oferecida informações de que trata o § 1º desse artigo, com base na observância de segredo comercial e industrial. Diante disso, poderá a autoridade nacional realizar auditoria para verificar aspectos discriminatórios em tratamento automatizado de dados pessoais. Caitlin Mulholland e Isabella Frajhof[608] apontam que se trata de uma discricionariedade da Autoridade Nacional de Proteção de Dados realizar ou não a auditoria.

Pode-se dizer, ainda, que há situações que poderiam ser auditadas para "[...] investigar a veracidade da explicação fornecida pelo controlador ou a legitimidade e a legalidade da recusa em alterar a decisão automatizada"[609]. Contudo, diante dos direitos fundamentais envolvidos e dos inúmeros exemplos de discriminações já vistos e discutidos pela doutrina[610], esse artigo não poderia ser interpretado restritivamente.

Além disso, essa legislação europeia permite que a pessoa não se submeta à decisão automatizada[611], mas a LGPD, por outro lado, dispõe direitos

---

[607] GRUPO, 2017, p. 18.

[608] MULHOLLAND; FRAJHOF, 2019.

[609] SÁ, Maria de Fátima Freire de; LIMA, Taisa Maria Macena de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 26, n. 04, p. 227-246, out./dez. 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584. Acesso em: 5 ago. 2022. p. 236.

[610] "O Google Fotos é um serviço de compartilhamento e armazenamento de fotos desenvolvido pela Google, empresa de serviços *on-line* e *software*, que tem a capacidade de organizar e marcar com *tags* (espécie de etiqueta digital) fotos semelhantes e reuni-las em um mesmo álbum. Mediante um sistema de reconhecimento de imagens, cada foto armazenada é qualificada, gerando diversas *tags*. No mesmo ano em que esse recurso foi disponibilizado (2015), um incidente constrangedor revelou uma falha grave do aplicativo. Um usuário do app Google Fotos fez o upload de algumas de suas fotos tiradas com sua amiga para o armazenamento da empresa. Posteriormente, ao acessar esses arquivos, constatou que as suas imagens estavam organizadas em um álbum intitulado 'Gorilas'. Um detalhe a considerar: este usuário e sua amiga são pessoas negras. Instada a manifestar-se, a empresa Google se disse 'triste e constrangida' e declarou estar tomando medidas para que este tipo de resultado não voltasse a aparecer" (SÁ; LIMA, 2021, p. 228).

[611] "A lei da proteção de dados estipula que uma pessoa tem o **direito a não ser sujeita a decisões baseadas exclusivamente em meios automatizados,** se a decisão produzir efeitos

ao titular quando realizada a perfilização[612]. Além disso, dispõe que serão considerados dados pessoais aqueles que forem utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (LGPD, art. 12, §2º).

Nesse contexto, o controlador[613] é figura que terá papel de destaque tanto nas decisões automatizadas como nas revisões delas. Para Souza, Perrone e Magrani[614], os controladores podem indicar em quais casos poderá ser feita a revisão das decisões por intermédio de uma pessoa natural.

A LGPD admite o tratamento de dados pessoais sensíveis com base no "[...] legítimo interesse do próprio controlador ou mesmo de terceiro, inclusive nos casos de tratamento de dados realizados por sistema de inteligência artificial"[615]. Devido ao cuidado que se deve ter com os dados pessoais sensíveis, o direito à explicação é considerado um instrumento eficiente para avaliar a legitimidade dos controladores[616].

A responsabilidade civil do controlador e do operador é solidária, e esses devem agir com diligência, pois podem ser responsabilizados se causarem danos no exercício de suas atividades, seja patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, sendo obrigados a repará-los (art. 42, LGPD).

Ademais, embora a responsabilidade seja objetiva, há situações em que controlador e operador podem se eximir se provarem, conforme o art. 43, que: não realizaram o tratamento de dados pessoais que lhes é atribuído; embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não

---

jurídicos respeitantes à pessoa ou que a afetem significativamente de maneira similar. Uma decisão produz efeitos jurídicos quando os seus direitos jurídicos são afetados (como o direito de voto). Além disso, o tratamento pode afetar significativamente um indivíduo se influenciar as suas circunstâncias, comportamentos ou escolhas. Por exemplo, o tratamento automatizado pode levar à recusa de um pedido de crédito em linha" (COMISSÃO EUROPEIA, [20--], grifos do autor).

612 ZANATTA, 2020.

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

614 SOUZA; PERRONE; MAGRANI, 2020.

615 SÁ; LIMA, 2021, p. 235.

616 *Ibidem*.

houve violação à legislação de proteção de dados; o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Diante disso, cabe ao controlador fornecer informações sobre o tratamento de dados quando solicitado pelo titular dos dados, ou seja, exercer os seus direitos previstos a partir do art. 18 da LGPD. Considerar-se-á irregular o tratamento de dados pessoais (art. 44) quando não se observar a legislação ou quando não se fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Diante disso, se ficar demonstrado que houve dano e ainda que não seja fornecida explicação, o controlador será passível de ressarcimento de danos materiais ou morais ao titular dos dados[617]. Ademais, a proteção do segredo comercial ou industrial não pode ser obstáculo para a proteção de direitos fundamentais e para se eximir a responsabilidade civil[618].

Não se pode apoiar as decisões da máquina num contexto de pseudoconsentimento[619]. Deve-se existir mecanismos que permitam que as pessoas possam consentir e exercer a autodeterminação informativa. Por outro lado, deve-se ressaltar que o consentimento do titular dos dados e o exercício da autodeterminação informativa apresentam dificuldades práticas para serem exercidos individualmente, em uma multiplicidade de situações do cotidiano. É o que se tem chamado do mito do consentimento:

> O consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade. Sua utilização como instrumento paradigmático para a tutela dos dados pessoais deve ser observada a partir de seus efeitos na sua

[617] SÁ; LIMA, 2021.
[618] *Ibidem*.
[619] CAMURÇA; MATIAS, 2021.

> concreta aplicação ao caso dos dados pessoais e seus efeitos — o que já foi denominado como *mito do consentimento*[620].

O regulamento da União Europeia 2016/679, do Parlamento e do Conselho[621], assegura a intervenção humana a fim de que se obtenha explicação quanto a uma decisão tomada por uma máquina sobre os seus dados. O considerando 71 da GDPR não tem força normativa, mas é uma diretriz interpretativa.

Para a Comissão Europeia[622], há possibilidade de uma pessoa estar sujeita a uma decisão automatizada. Porém a regra é que não deva ser sujeita

---

[620] DONEDA, 2020a, p. RB-4.6.

[621] O direito à explicação na GDPR está previsto no artigo 22, que dispõe sobre as decisões individuais automatizadas, o *profiling* – e o Considerando 71 (preâmbulo desse documento). Art. 12 e 13, considerando 60-62 e art. 15 e considerando 63: "(71) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou que o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança. A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas".

[622] COMISSÃO EUROPEIA, [20--].

a uma decisão baseada exclusivamente em tratamento automatizado, portanto, trata-se de uma exceção[623]. Além disso, deve haver previsão legal e serem garantidas as salvaguardas adequadas[624]. As decisões automatizadas serão permitidas quando: "[...] a decisão é necessária, ou seja, não pode existir outra forma de alcançar o mesmo objetivo, para celebrar ou executar um contrato com a pessoa em questão; a pessoa deu o seu consentimento expresso".

Nesses dois casos, a decisão tomada tem de proteger os direitos e liberdades por meio de salvaguardas adequadas. A empresa ou organização deve, pelo menos, informá-lo do seu direito de obter intervenção humana e de tomar as medidas procedimentais necessárias. Também deve permitir a manifestação do seu ponto de vista e deve informá-lo de que pode contestar a decisão.[625] Contudo, segundo a Comissão Europeia, as decisões automatizadas não poderão utilizar categorias especiais de dados, somente poderão fazê-lo se houver consentimento do titular ou se o tratamento for permitido pelo direito da União Europeia ou pelo direito nacional[626].

Para a utilização do aprendizado da máquina, os dados devem ser confiáveis e deve-se verificar se há dados suficientes e se esses estão atualizados[627]. Além disso, deve-se observar se existe o objetivo de solução de problemas específicos e que foram testados anteriormente.

Se houver algum problema na saída, ou seja, no resultado apresentado, não necessariamente se desenvolverá um novo sistema ou se poderá solucionar, senão fazer ajustes e aplicar novos testes[628]. Esse é um dos pontos de maiores preocupações, pois aqueles que desenvolvem os sistemas também podem não ter soluções práticas para resolver os resultados que apresentem vieses discriminatórios. A máquina reflete os dados passados, reproduz as percepções e preconceitos existentes.

---

623 *Ibidem*.
624 *Ibidem*.
625 *Ibidem*.
626 COMISSÃO EUROPEIA, [20--].
627 SILVA, Nilton Correia da. Compreensão da inteligência artificial e dos seus pressupostos de controle e regulação. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019, p. R.B -3.4.
628 SILVA, 2019.

Italo Vega[629] explica que a decisão deve ser lógica e consistente, pois as deduções computacionais utilizam um sistema lógico codificado na forma de programa, mas se forem usados diversos sistemas lógicos, não há como se garantir que a decisão será racional[630]. Em razão disso, faz-se necessária a presença de agentes externos para a tomada da decisão final, os quais lidarão com situações conflitantes[631].

Andriei Gutierrez[632] aponta que uma das soluções para a revisão das decisões automatizadas seria que ela estivesse condicionada a situações muito específicas, e apenas em última instância ser precedida por revisões automatizadas, a fim de combinar a proteção de direitos e o desenvolvimento econômico movido por dados e sistemas de IA. Além disso, afirma que é necessário que as revisões automatizadas devam ter relativo grau de confiança[633].

Fabro Steibel, Victor Freitas Vicente e Diego Santos Vieira de Jesus[634], por sua vez, afirmam que as pessoas deverão estar constantemente atualizadas nas suas funções e habilidades a fim de monitorar as máquinas e as suas decisões autônomas que possam resultar em questões jurídicas e éticas negativas. Uma das sanções aplicadas àqueles que utilizam a decisão automatizada pode ser receber a desconfiança do consumidor e da população em geral, sendo assim afetada a sua reputação no mercado. Diante disso, devem ser adotadas medidas preventivas[635].

Contudo, deve-se levar em consideração que, embora os consumidores possam deixar de contratar determinados fornecedores, isso pode ser um fardo, porque em toda contratação terá que analisar como os seus dados serão

---

[629] VEGA, Italo S. Inteligência artificial e tomada de decisão – a necessidade de agentes externos. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.
[630] *Ibidem*.
[631] *Ibidem*.
[632] GUTIERREZ, 2019.
[633] GUTIERREZ, 2019.
[634] STEIBEL, Fabro; VICENTE, Victor Freitas; JESUS, Diego Santos Vieira de. Possibilidade e potenciais da utilização da inteligência artificial. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.
[635] STEIBEL; VICENTE; JESUS, 2019.

tratados, ou mesmo se terá acesso a isso. Além do mais, os perfis criados têm um aspecto coletivo, ou seja, afetam grupos de pessoas. Em virtude disso, a atuação de outros agentes na prevenção de danos, sejam públicos ou privados, é mais recomendada, assim como a aplicação de técnicas como *privacy by design* e *default by design*, a observação das leis vigentes, e a ação ética, parecem ser mais relevantes e eficazes nesse processo.

Bruno Bioni e Maria Luciano[636] defendem a aplicação do princípio da precaução nas decisões automatizadas, pois deve-se levar em consideração o grau do risco apresentado (forte, fraco ou moderado), a possibilidade de reversibilidade ou não e a utilização dos relatórios de impacto à proteção de dados pessoais. Os autores explicam que há uma relação entre o princípio da precaução e da *accountability* para aferir se cabe ou não a aplicação de uma decisão automatizada:

> Na medida em que boa parte dos processos de decisões automatizadas com o emprego de IA envolverá o processamento de dados pessoais, leis gerais de proteção de dados, talhadas com base em uma mentalidade de regulação de risco e no princípio da *accountability*, são vetores de democratização do próprio processo de regulação de tal tecnologia. Tais leis apresentam-se como um feixe de entrada para a aplicação do princípio da precaução, em sua conotação de deliberação pública, acerca da adoção ou não de IA em vista da definição do tipo de riscos que lhes são subjacentes[637].

Para a LGPD o princípio da *accountability* pode ser extraído do art. 6º, que enumera os seus princípios, mais especificamente o inciso X: "[...] responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

A *accountability* também se relaciona com o devido processo informacional e com o exercício dele, uma vez que, para que se possar exercer a autodeterminação informativa, faz-se necessário que se tenha acesso a diversas informações, assim como à explicação de como se deu a decisão

[636] BIONI; LUCIANO, 2019.
[637] BIONI; LUCIANO, 2019, p. RB -11.3.

automatizada. No entanto, para a prestação de contas, faz-se necessária a documentação sobre a coleta dos dados que demonstre, pelo agente de tratamento, a adoção de medidas que sejam eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas. Esse tema será retomado novamente quando forem abordadas as medidas que devem ser adotadas pelos agentes de tratamento.

Entre as novidades trazidas pela LGPD está a tutela dos titulares com a "[...] demonstração e prestação de contas (*accountability*); são considerados elementos que levam em conta o risco em atividades de tratamento de dados pessoais e muitas outras"[638]. Não há uma tradução exata para o português de "*accountability*". Trata-se de uma expressão que indica algo como a ética, a obrigação, a transparência, a prestação de contas[639]. Além disso: "Remete à necessidade de governança e, em alguns casos, até de responsabilidade civil. Não é à toa que o tema da IA tem chamado a atenção de empresas, governos e organizações nacionais e internacionais"[640].

Sobre a inteligência artificial, ao se discutir como um sistema deve ser, recomenda-se os seguintes princípios para que esse seja considerado confiável: a transparência e a explicabilidade; a inclusão, bem-estar e crescimento sustentável; valores e justiça antropocêntricos, segurança e robustez; e *accountability*[641].

Segundo a doutrina, o princípio de *accountability* não tem correspondência na língua portuguesa. Esse termo engloba a "[...] responsabilidade com ética, a obrigação, a busca por transparência, a prestação de contas"[642]. Esse princípio está em consonância com o devido processo informacional e o direito à explicação, pois contribui para elucidar como foi tomada a decisão, bem como se os agentes de tratamento atuaram de acordo com a legislação existente.

---

[638] DONEDA, 2020b, p. 37.
[639] GUTIERREZ, 2019.
[640] GUTIERREZ, 2019, p. RB-6.3.
[641] GUTIERREZ, 2019.
[642] GUTIERREZ, 2019, p. RB-6.3.

3.2 DIREITO À EXPLICAÇÃO

Na LGPD está expresso o direito à revisão da decisão automatizada (art. 20) quando a decisão tiver sido tomada unicamente por meio de um tratamento de dados automatizado[643]. Ana Frazão[644] sustenta que o direto à revisão abrange o direto à explicação e à oposição, ainda que tenha sido excluída da legislação a revisão da decisão por pessoa humana. Além disso, não basta que as informações sejam claras e adequadas[645]:

> O dever do controlador é fornecer subsídios que tornem compreensível a passagem dos seus objetivos, consolidados no artefato algorítmico em critérios matemáticos, até a decisão automatizada. Não se torna imperativo que as minúcias técnicas da decisão sejam reveladas, protegido assim o segredo comercial e industrial; mas deve o controlador demonstrar, em linguagem natural, por que ele mesmo acredita que a decisão automatizada é a que melhor atende suas pretensões[646].

Devido à complexidade da decisão automatizada, para que alguém possa se opor a ela deve antes ter acesso às informações, ou seja, entender o que ocorreu, o que demanda transparência. Em suma, "[...] com efeito, corolário lógico do direito de revisão de decisões automatizadas é o direito à explicação"[647].

Nessa esteira, Miriam Wimmer e Danilo Doneda[648] entendem que o direito à explicação tem um componente informativo, pois para que possa haver a revisão, torna-se necessário que se conheça os critérios e os vetores que resultaram em uma decisão, ou seja, que se saiba sobre a sua *ratio*. Além disso,

---

643 TONIAZZO, Daniela Wendt; BARBOSA, Tales Schmidke; RUARO, Regina Linden. O direito à explicação nas decisões automatizadas: uma abordagem comparativa entre o ordenamento brasileiro e o europeu. **Revista Internacional Consinter de Direito**, Porto, Portugal, v. 7, n. 13, p. 55-69, 2021. Disponível em: https://revistaconsinter.com/index.php/ojs/article/view/63/106. Acesso em: 10 fev. 2023.

644 FRAZÃO, 2020.

645 *Ibidem*.

646 *Ibidem*, p. RB-3.5.

647 FRAZÃO, 2021.

648 WIMMER, Miriam; DONEDA, Danilo. "Falhas de IA" e a intervenção humana em decisões automatizadas: parâmetros para a legitimação pela humanização. **Direito Público**, Brasília, v. 18, n. 100, p. 374-406, 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6119. Acesso em: 11 fev. 2023.

Monteiro afirma que o direito à explicação decorre do princípio da transparência e que a LGPD tem como característica ter sido elaborada de forma multissetorial e transversal[649].

A LGPD, no art. 20, §§ 1º e 2 º, assegura o direito à informação para que se possa solicitar a revisão:

> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Portanto, do artigo 20 da LGPD pode-se extrair a existência de um direito à explicação e do direito à revisão da decisão automatizada. Há, ainda, o direito à petição à Autoridade Nacional de Proteção de Dados (ANPD), a fim de que seja realizada auditoria se não forem prestadas as informações solicitadas[650]. Todavia, Daniela Toniazzo, Tales Barbosa e Regina Ruaro, por outro lado, entendem que:

> Por fim, como resultado do presente estudo, conclui-se que não há expressamente, no direito brasileiro, o direito à explicação da decisão automatizada, como ocorre no direito europeu, mas apenas a possibilidade de revisão, não humana, da decisão tomada unicamente com base em tratamento automatizado de dados pessoais[651].

Também é possível que esse direito à explicação possa ocorrer em qualquer momento do tratamento de dados, tendo em vista o §1º do art. 20, que contém a expressão “sempre que solicitadas” o controlador deve fornecer informação[652].

---

[649] MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Revista Instituto Igarapé**, Rio de Janeiro, Artigo Estratégico 39, p. 1-27, dez. 2018. 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 em: 08 fev. 2023.
[650] FRAZÃO, 2018a.
[651] TONIAZZO; BARBOSA; RUARO, 2021, p. 68.
[652] SOUZA; PERRONE; MAGRANI, 2020.

No entanto, no Direito brasileiro, a pessoa não pode escolher não se submeter à decisão automatizada, como previsto no RGPD, art. 22, n. 1, em que "[...] direito a não ser submetido à decisão exclusivamente automatizada, incluindo as definições de perfil"[653]. Portanto, a referida proibição independe de o titular dos dados adotar uma medida relativa ao tratamento dos seus dados pessoais[654]. Ana Frazão entende que da LGPD, art. 20 e parágrafos, pode-se extrair os seguintes direitos:

> (i) o direito de acesso e informação em relação a respeito dos critérios e procedimentos utilizados para a decisão automatizada, (ii) o direito de oposição quanto à decisão automatizada e de manifestar o seu ponto de vista, (iii) o direito de obtenção da revisão da decisão automatizada por uma pessoa natural e (iv) o direito de petição à autoridade nacional para a realização de auditoria, em caso da não prestação das informações[655].

Thiago Junqueira apresenta a seguinte crítica sobre as disposições do art. 20 da LGPD:

> Nesse sentido, a ambiguidade do art. 20 da LGPD e as incertezas que circundam os direitos à explicação e à revisão das decisões automatizadas acabam por não acomodar apropriadamente o elo entre a proteção de dados e o combate à discriminação. A desnecessidade de revisão humana de tais decisões, bem como o caráter optativo do relatório de impacto à proteção de dados e da realização de auditoria pela ANPD, também colocam em xeque o potencial de prevenção e combate à discriminação. A tudo isso, soma-se mais um elemento: paradoxalmente, em alguns casos a *proteção da privacidade pode causar o efeito perverso de ampliar a discriminação algorítmica*[656].

A leitura restritiva desse artigo não contribui para o enfrentamento das implicações negativas do avanço da inteligência artificial e da técnica denominada de aprendizado da máquina, ainda mais com a potencialidade de se obter dados pessoais sensíveis de maneira indireta. Decorre daí a importância do direito à explicação, uma vez que esse direito pode contribuir para se verificar a necessidade de intervenção humana. Porém, a depender do resultado obtido,

---

653 TONIAZZO; BARBOSA; RUARO, 2021, p. 64.
654 GRUPO..., 2017.
655 FRAZÃO, 2018a.
656 SILVA; TEPEDINO, 2020, RB-14.3.

a explicação pode ser desaconselhável, como nos casos em que a decisão é irreversível[657]:

> Nesse sentido, a irreversibilidade dos efeitos da decisão automatizada certamente é elemento central a ser considerado, pois, embora um direito à explicação pudesse eventualmente apoiar demandas de reparação por danos experimentados, pouco sentido haveria em prever o direito à revisão de uma decisão cujos efeitos são irreversíveis[658].

A Lei n. 12.414/2011 (Lei do Cadastro Positivo), art. 5º, inciso VI, estabelece o direito do cadastrado de "[...] solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados". Para isso deve conhecer os elementos e os critérios utilizados para a análise do risco e para a elaboração de sua pontuação[659]. Esse conjunto de direitos pode ser considerado uma versão do direito à explicação[660].

Essa mesma Lei contém um sistema administrativo[661] para controle da atividade de processamento de dados, quando o cadastrado for consumidor (CDC). Ademais, para Monteiro[662], alguns desses direitos, como a transparência e a explicação, estavam garantidos para as decisões automatizadas no CDC e na LCP, o que já tinha sido reconhecido pelo STJ[663]. Diante disso, há esse

---

[657] WIMMER; DONEDA, 2022.
[658] *Ibidem*, p. 396.
[659] MENDES, 2014.
[660] SOUZA; PERRONE; MAGRANI, 2020.
[661] LCP: "Art. 17. Nas situações em que o cadastrado for consumidor, caracterizado conforme a Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor, aplicam-se as sanções e penas nela previstas e o disposto no § 2º. § 1º Nos casos previstos *no caput* , a fiscalização e a aplicação das sanções serão exercidas concorrentemente pelos órgãos de proteção e defesa do consumidor da União, dos Estados, do Distrito Federal e dos Municípios, nas respectivas áreas de atuação administrativa. § 2º Sem prejuízo do disposto *no caput e* no § 1º deste artigo, os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas e estabelecer aos bancos de dados que descumprirem o previsto nesta Lei a obrigação de excluir do cadastro informações incorretas, no prazo de 10 (dez) dias, bem como de cancelar os cadastros de pessoas que solicitaram o cancelamento, conforme disposto no inciso I do caput do art. 5º desta Lei".
[662] MONTEIRO, 2018.
[663] "Posteriormente, o tribunal julgou se o direito de acesso às fontes dos dados e a explicação da lógica do seu tratamento encontravam algum fator limitador. Concluiu que existe interesse de agir do consumidor que deseja conhecer os principais elementos e critérios considerados para a análise do seu histórico e as informações pessoais utilizadas — respeitado o segredo empresarial, — desde que tenha sido atingido por tais critérios quando tentou obter crédito no mercado, p.ex., deixou de conseguir crédito devido à pontuação que lhe foi atribuído. O STJ estabeleceu, assim, um critério que até então não encontrava respaldo na lei, possibilitando reconhecer a existência do direito à explicação de decisões totalmente automatizadas, desde

respaldo para o exercício desses direitos em situações que envolvem a concessão de crédito e o cálculo de risco de inadimplência. Toma-se como exemplo o art. 5º, incisos IV a VII, da LCP[664]:

> Estes quatro direitos se originam a partir do direito à transparência e não discriminação e formam a espinha dorsal do direito à explicação de decisões automatizadas em relações de consumo. Eles exigem que o consumidor seja esclarecido sobre as fontes de dados utilizadas e as informações pessoais consideradas para o cálculo do risco de inadimplência na concessão ou não de crédito. A Lei também tenta limitar os tipos de dados que podem ser utilizados para cálculo do risco de crédito, vedando o uso de dados não relacionados com a análise do risco de crédito do consumidor, assim como dados pessoais sensíveis e os pertinentes "à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas"[665].

Contudo, como afirma Monteiro[666], essa proteção é insuficiente por ser setorial, haja vista as inúmeras possibilidades de aplicação de decisões automatizadas. Por isso:

> O princípio da transparência deve reger toda e qualquer relação do responsável pelo tratamento de dados pessoais com o titular dos dados, garantindo a este o direito de acesso aos seus dados pessoais. Esse princípio também pressupõe o dever de informar os critérios de tratamentos utilizados para finalidades informadas ao titular[667].

A fiscalização e a aplicação de sanções serão feitas de maneira concorrente pelos órgãos de proteção e de defesa do consumidor da União, dos estados, do Distrito Federal e dos municípios, nas respectivas áreas de atuação administrativa. Além disso, os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas aos bancos de dados que descumprirem o previsto nessa lei. Caso haja descumprimento, há a obrigação de excluir do

---

que tais decisões tenham um impacto específico na vida das pessoas" (MONTEIRO, 2018, p. 08).

664 LCP: "Art. 5º: IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial; V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais; VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados".

665 MONTEIRO, 2018, p. 08.

666 *Ibidem*.

667 *Ibidem*, p. 10.

cadastro informações incorretas, no prazo de 10 (dez) dias, e de cancelar os cadastros de pessoas que assim solicitarem, conforme o disposto no inciso I do caput do art. 5º dessa Lei. Dessa forma, há um sistema de fiscalização, coexistente com o sistema judicial[668], que pode contribuir para solucionar conflitos.

Bruno Bioni e Maria Luciano[669] explicam que o direito à explicação decorre do princípio da transparência, o qual está previsto na LGPD, no 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". Ensinam que o direito à explicação das decisões automatizadas também está previsto desde a Lei n. 12.414/2011 (Lei do Cadastro Positivo), no art. 8º, inciso VI, o qual determina a obrigação de "[...] fornecer informações sobre o cadastrado, em bases não discriminatórias, a todos os gestores de bancos de dados que as solicitarem, no mesmo formato e contendo as mesmas informações fornecidas a outros bancos de dados". Nessa esteira, Toniazzo, Barbosa e Ruaro afirmam que o princípio da explicação se coaduna com o princípio da transparência, que deve ser:

> [...] garantida *ex ante* (quanto trata da funcionalidade do sistema) e também *ex post* (ao versar sobre os fundamentos da decisão). A explicabilidade garante a revelação dos motivos da decisão algorítmica, significando um requisito de efetividade da contestação e do recurso contra a decisão artificial suspeita de afrontar os princípios e valores fundamentais. É garantia do princípio da motivação explícita, clara e congruente[670].

Portanto, a explicação e a transparência podem ser solicitadas em todas as fases do procedimento de decisão automatizada ao se fazer uma interpretação das diversas leis existentes e aplicáveis nessas relações. Taisa Lima e Maria de Sá[671] asseveram que a LGPD foi tímida nesse aspecto, uma vez que os processos decisórios complexos podem ter fases que são

---

[668] MENDES, 2014.
[669] BIONI; LUCIANO, 2019.
[670] TONIAZZO; BARBOSA; RUARO, 2021, p. 65.
[671] SÁ; LIMA, 2021.

automatizadas e outras que são implementadas com as decisões humanas — em razão disso, essas decisões devem ter igual cobertura legal, ou seja, serem abrangidas pelo direito à explicação.

Defende-se que o direito à explicação pode ser exercido anteriormente ou posteriormente à tomada de decisão, e que as informações devem dizer respeito ao sistema ou às razões que levaram à tomada de decisão[672], assim como aos perfis criados (*profiling*) dos titulares de dados[673].

Para Renato Monteiro, a LGPD foi mais adiante do que a RGPD no que diz respeito ao direito à explicação. Ademais, há a necessidade de dois novos direitos distintos para proteger o titular dos dados: o primeiro é o direto à explicação, que consiste no direito de o titular receber informações que sejam suficientes e inteligíveis para que possa entender a lógica e os critérios utilizados para o tratamento de dados pessoais[674]. E o segundo direito é o de requerer uma revisão feita por uma pessoa humana em caso de revisão automatizada de uma decisão totalmente automatizada, quando houver "[...] uma decisão totalmente automatizada que possa ter um impacto nos seus interesses, principalmente os relacionados à definição do seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade"[675].

Monteiro[676] sintetiza as garantias previstas na LGPD ao titular dos dados pessoais da seguinte maneira:

> i. Ter acesso aos tipos de dados e a quais de seus dados pessoais são utilizados para alimentar algoritmos responsáveis por processos de decisões automatizadas; ii. Caso o processo automatizado tenha por finalidade formar um perfil comportamental, ou se valha de um perfil comportamental para tomar uma decisão subsequente, o direito de acesso aos dados poderá incluir, também, os dados anonimizados utilizados para enriquecer tais perfis; iii. Esse direito inclui o de receber explicações sobre os critérios utilizados para tomar a decisão automatizada, observados os segredos comercial e industrial, que deve ser analisados caso-a-caso, uma vez que tais conceitos não encontram subsídio na Lei; e iv. Caso tais decisões tenham impacto nos interesses dos titulares, o que se presume, no caso de perfis comportamentais, é um direito requisitar que haja revisão por uma

672 MULHOLLAND; FRAJHOF, 2019.
673 *Ibidem*.
674 MONTEIRO, 2018.
675 *Ibidem*, p. 04.
676 *Ibidem*.

> pessoa natural, a qual deverá observar o princípio da transparência, devendo deixar claro os critérios utilizados para tomar sua decisão[677].

Assim, está previsto no âmbito da RGPR que o titular dos dados tem o direito de acesso, que consiste na possibilidade "[...] de obter informações acerca de quaisquer dados pessoais utilizados na definição de perfis, incluindo a categoria dos dados utilizados para criar um perfil"[678]. Além disso, tem direito de ter acesso às informações genéricas sobre o tratamento dos dados e de "[...] saber quais os dados utilizados como dados de entrada para criar o perfil, bem como facultar acesso a informações sobre o perfil e sobre os segmentos onde o titular dos dados foi inserido"[679].

Outro ponto a ser levado em consideração é a utilização de informação que é pública, e que por sua natureza não tem sigilo, como a participação em sindicatos, em manifestações, ação movida contra o seu empregador, processos sem sigilo. Informações como essas, que não tenham relevância para determinado tratamento de dados, não podem ser consideradas, pois podem prejudicar indivíduos e grupos de pessoas. Como já mencionado, deve-se observar os princípios para o tratamento dos dados, verificar se há relevância para o caso ou se apenas se induz à discriminação. Por isso, Rodotà ensina que há informações que não têm vocação para o sigilo e estão públicas, o que ele denomina de paradoxo da privacidade[680].

Por outro lado, a LGPD, no art. 7º, § 4º, aduz que é dispensado o consentimento para dados tornados manifestamente públicos pelo titular; não obstante isso, assegura os direitos do titular e os princípios previstos nesta lei. Além disso, a utilização de informação sobre o exercício regular de um direito[681] não pode ser considerada em prejuízo da pontuação (*scoring*); se o fizer, considerar-se-á a prática ilícita[682].

---

[677] MONTEIRO, 2018, p. 13.
[678] GRUPO..., 2017, p. 18.
[679] *Ibidem*, p. 18-19.
[680] RODOTÀ, 2008.
[681] LGPD: "Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo".
[682] OLIVA; VIÉGAS, 2020.

Apesar disso, deve-se observar os princípios elencados no art. 6º, especialmente quanto ao mínimo essencial[683], que são os princípios da finalidade, da adequação e da necessidade[684]. Diante disso, os dados que naturalmente sejam públicos e potencialmente sensíveis, ou que possam causar discriminação, devem ser ponderados dentro de um contexto para se verificar a aplicação desses princípios.

Há também informações que, por força de lei, são públicas, com fundamento no interesse público e no princípio da publicidade, como as informações sobre acesso a políticas públicas ou rendimentos dos servidores públicos[685], cuja divulgação é constitucional. Contudo, a utilização de tais informações deve observar o princípio da finalidade, pois apesar de serem públicas não podem se desviar da sua finalidade, ou seja, não devem ser utilizadas com um outro propósito. A Lei de Acesso à Informação também apresenta disposições sobre esse tema no art. 31: "O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais"[686].

---

683 TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais**: comentada artigo por artigo. 2. ed. rev. atual. e ampl. Salvador: Editora JusPodvm, 2020.

684 LGPD: "Art. 6º, incisos: III - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

685 BRASIL. Supremo Tribunal Federal (plenário). **Recurso Extraordinário com Agravo 652.777/SP**. Constitucional. Publicação, em sítio eletrônico mantido pelo município de São Paulo, do nome de seus servidores e do valor dos correspondentes vencimentos. Legitimidade. 1. É legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias. 2. Recurso extraordinário conhecido e provido. Relator: Teori Zavascki, 23 abr. 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8831570. Acesso em: 30 jan. 2023.

686 BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a lei nº 8.112, de 11 de dezembro de 1990; revoga a lei nº 11.111, de 5 de maio de 2005, e dispositivos da lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2011]. Disponível em:

Houve divergência sobre a existência ou não desse princípio no âmbito da União Europeia, pois se esse direito não estava expresso, não poderia ser exercido, o que foi defendido por Wachter, Mittelstadt e Floridi[687]. Contudo, Wachter e Russel[688] mudaram de entendimento posteriormente[689].

Não parece existir, porém, divergência no direito brasileiro acerca da existência desse direito, haja vista que a LGPD garante o direito à revisão e que o controlador deve fornecer informações — se não o fizer, a ANPD poderá realizar auditoria. Parece ser mais relevante discutir como esse direito poderá ser exercido e como enfrentar a negativa em razão do segredo do negócio ou industrial, haja vista que o legislador fez menção disso por diversas vezes. Ademais, a Lei do Cadastro Positivo garante o direito à informação no art. 8º,

---

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 30 jan. 2023.

[687] WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, [*s. l.*], 25 fev. 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469. Acesso em: 25 ago. 2022.

[688] MULHOLLAND; FRAJHOF, 2019.

[689] "Para compreender o que é esta explicação do dia-a-dia, os autores retomam a estudos de outras áreas do conhecimento (filosofia, psicologia e ciências cognitivas) para entender como é descrita a forma com que os seres humanos dão e recebem explicações. Três principais características foram destacadas. A primeira delas é o fato de que explicações são contrafactuais e contrastantes, ou seja, as pessoas não pedem explicações do por que dado evento ocorreu (P), mas por que (P) ocorreu no lugar de (Q). Isto acontece, pois os seres humanos preferem psicologicamente explicações contrastantes a explicações em cadeia. A segunda característica das explicações humanas é que elas são seletivas. As pessoas não esperam uma explicação completa e encadeada para compreender um evento, elas selecionam uma ou duas causas de um número de causas finitas para compreendê-lo, de acordo com seus interesses subjetivos e o contexto no qual ela se encontra inserida. A terceira característica é que as explicações humanas são sociais, e envolvem interação e comunicação entre o emitente e o receptor. A sugestão dos autores é que, tanto para as explicações que tratam sobre as funcionalidades do modelo de aprendizado de máquina e suas diversas camadas, relacionadas à transparência dos algoritmos e sua forma de trabalho, assim como aquelas relacionadas à decisão *post-hoc* para explicar o modelo e as decisões, devem ser levadas em consideração a forma e qualidade que se dão estas explicações, devendo ser levada em consideração a maneira como seres humanos lidam com elas. No entanto, as três características acima destacadas da explicação humana não vão sem críticas, mas o conhecimento sobre os seus problemas auxiliará desenvolvedores a se resguardarem, implementando *features* que ao menos mitiguem estes riscos. Uma das formas de evitá-los é permitir a troca de informação entre usuários e desenvolvedores. É neste sentido que eles caminham para a defesa de uma 'teoria de explicações de todo o dia', que consiste na capacidade de desenvolver explicações que reflitam não apenas a transferência de informação ou argumentos causais para o titular de dados, mas que estas se deem a partir de um suporte argumentativo para estas causas que deverá ocorrer por intermédio da interação entre usuário e desenvolvedor (MITTELSTADT *et al*., 2019, p. 7). A recomendação é que pesquisadores da área de *explainable AI* devam se voltar para o desenvolvimento de métodos que produzam explicações que incorporem estas características, tanto quando forem dadas explicações contratantes, quanto por aproximação" (MULHOLLAND; FRAJHOF, 2019, p. RB-13.4).

inciso VI, devendo, desse modo, ser feita uma interpretação do ordenamento como um todo.

A explicação garante a efetividade ao princípio da transparência, a qual deve abranger a funcionalidade do sistema, ou seja, a sua lógica, assim como os fundamentos da decisão[690]. Deve-se ressaltar que o art. 20 da LGPD consagra a "[...] diretriz da explicabilidade e da sua vinculação ao princípio da motivação decisória algorítmica, traduzindo-se também como uma espécie de extensão da fundamentação para o universo das decisões artificiais"[691]. Ademais, a explicação contribui para *accountability* de IA, uma vez que pode explicitar qual a lógica aplicada na decisão e contribuir para determinar a extensão em que determinado *input* foi determinante ou influenciador no resultado obtido[692].

O direito à explicação também deve abranger quais dados são utilizados, pois, se houver dados sensíveis, devem ser observadas as regras específicas para a sua utilização. Para que seja possível viabilizar o direito à explicação, sugere-se que devam ser documentadas as seguintes condutas:

> (i) apresentação de justificativas que motivaram o uso de sistemas de IA para aquele determinado contexto; (ii) indicação de quais tipos de métodos e modelos de interpretação e explicação do resultado do modelo de ML foram considerados e implementados; (iii) registro da origem dos dados utilizados para o treinamento e teste do modelo, (iv) indicação de como foi realizado o pré-processamento dos dados, e como potenciais discriminações foram consideradas; (v) apontamento de quais foram os critérios para a escolha do modelo em relação à capacidade de interpretação e explicação dos seus resultados, e as ferramentas utilizadas para tanto; (vi) apresentação dos resultados da aprendizagem e testagem do modelo; e (vii) indicação de como e qual tipo de explicação está sendo fornecida para o titular de dados[693].

Verifica-se que há uma relação entre o princípio da precaução e da *accountability* e dos relatórios feitos ao longo do processamento de dados pessoais para evitar danos incalculáveis aos indivíduos ou a grupo de pessoas vulneráveis. Diante disso:

---

[690] TONIAZZO; BARBOSA; RUARO, 2021.
[691] *Ibidem*, p. 64.
[692] BIONI; LUCIANO, 2019.
[693] FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022, p. RB-19.4.

> [...] é o princípio da responsabilização e prestação de contas, que impõe aos agentes de tratamento o dever de demonstrar que adotaram medidas eficazes para comprovarem a observância do cumprimento das garantias previstas pela lei, demonstrando essa eficácia. Esse princípio traduz a noção de *accountability* e é complementado por outros deveres mais específicos, como o de adotar medidas de segurança desde a concepção de produtos ou serviços e a elaboração de relatórios de impacto à proteção de dados para atividades que apresentem riscos às liberdades civis e aos direitos fundamentais dos titulares afetados[694].

Esse direito de explicação deve abranger também dados que não são considerados pessoais, mas que influenciaram a decisão[695]. Muito se falou no capítulo anterior da quantidade de dados coletados, por qual período podem ser utilizados, no entanto, há seguros que levam mais em consideração o comportamento do motorista via aplicativo do que outras informações[696].

Convém destacar que Toniazzo, Barbosa e Ruaro defendem a revisão da decisão automatizada por uma pessoa humana para que o direito à explicação tenha eficácia, ainda que não tenha existido falhas no sistema de IA[697]:

> A explicabilidade por meio de revisão humana, em especial destaque, é crucial para se criar e manter a confiança dos utilizadores nos sistemas de inteligência artificial, emanando a transparência dos processos de decisões algorítmicas, visando reprimir preconceitos humanos e sociais capazes de ter seus efeitos multiplicados, quando se tratar de decisões automatizadas. [...]
> O direito à explicação, por meio de revisão humana, parece ser essencial para se vislumbrar com clareza o trajeto das decisões algorítmicas e os potenciais erros presentes no processo de tomada de decisão por inteligência artificial, de modo a possibilitar que a IA se torne cada vez mais segura em suas relações entre máquina e o homem, colaborando para decisões imparciais aptas a serem supervisionadas e alteradas durante o projeto ou funcionamento[698].

---

694 MARTINS, 2022, p. 216.
695 "No seguro de veículos podem ser utilizados "[...] outros dados que auxiliem na interpretação desses, como os atinentes às respectivas condições climáticas e de trânsito, igualmente comporão o perfil de risco em questão e, por isso, deverão ser informados" (JUNQUEIRA, 2020b, RB-2.3).
696 "Os aplicativos que monitoram o comportamento ao volante utilizam o celular, que precisa estar sempre com o motorista. Com os recursos do próprio *smartphone*, o app verifica se o usuário acelera forte, se as frenagens são bruscas, se faz curvas fechadas ou se fala ao celular enquanto dirige" (CARVALHO, 2021).
697 TONIAZZO; BARBOSA; RUARO, 2021.
698 *Ibidem*, p. 67.

O direito à explicação abrange a informação de quais dados são utilizados, se houve a utilização de dados sensíveis. Ademais, devem ser observadas as regras específicas para a sua utilização, como o consentimento em algumas situações, se não decorrer de hipótese prevista em lei. Além disso, esse direito abrange a informação do modo como são coletados os dados pessoais, e se são coletados dados disponíveis em outros locais, seja em ambiente virtual ou não. Isso decorre também do princípio da transparência, trata-se de tema complexo e de difícil controle.

Por isso, também se pode falar em um direito à explicação anteriormente e posteriormente à tomada da decisão (*ex ante e ex post).* Em outras palavras, esse direito pode ser exercido nesses dois momentos[699]*.* Thiago Junqueira faz as seguintes sugestões para a utilização das decisões automatizadas:

> Entre as medidas que se julgam necessárias, podem ser sublinhadas, sem pretensão de exaustão: i) a exigência de que os algoritmos subscritores dos seguros sejam compreensíveis e contem, sempre, com um humano envolvido nos seus processos de treinamento e tomada de decisões; ii) o aumento da transparência e de *accountability* do segurador em relação aos dados coletados e aos modos de sua utilização (controle dos *inputs* e dos *outputs*), exigindo-se o registro de todo o processo de treinamento do algoritmo e a sua adaptação razoável — caso esteja causando um discriminação inadmissível —, e iii) o incentivo de uma maior diversidade nas empresas de tecnologia e nas seguradoras, de modo a se possibilitar um controle interno mais rigoroso por meio dos próprios funcionários membros de grupos minoritários[700].

Dentre as novidades trazidas pela Lei Geral de Proteção de Dados está a tutela dos titulares com as regras de "[...] demonstração e prestação de contas (*accountability*); são considerados elementos que levam em conta o risco em atividades de tratamento de dados pessoais e muitas outras"[701]. Sobre a prestação de contas na ANPD, explica:

> O princípio da responsabilização e prestação de contas (*accountability*) estabelece que os(as) agentes de tratamento devem ser capazes de demonstrar o cumprimento e o respeito à LGPD, apresentando as

[699] SOUZA; PERRONE; MAGRANI, 2020, p. 261.
[700] SILVA; TEPEDINO, 2020, p. RB-14.4.
[701] DONEDA, 2020b, p. 37.

> medidas adotadas e a eficácia delas. Para isso, a lei apresenta uma série de instrumentos que podem ser utilizados[702].

Junqueira elenca as seguintes sugestões para que os agentes de tratamento de dados utilizem nas decisões automatizadas em casos de perfilização:

> [...] registro de todo o processo envolvendo a coleta de dados, escolha dos atributos, rotulagem e toda a fase de treinamento e calibragem do algoritmo, bem como a manutenção de rígida documentação sobre testes internos para a verificação dos *outputs* (em especial, se estão ocasionando alguma discriminação racial), nada impede que ela seja implementada[703].

Segundo Junqueira[704], o que se nota é que a proteção de dados tende a estar mais voltada para a coleta dos dados pessoais (*inputs*) e não para as informações e consequências a partir do aprendizado da máquina, ou seja, as suas decisões (*outputs*).

No estudo feito pelo Instituto de Tecnologia e Sociedade do Rio (ITS), sugeriu-se aos *bureaux* estruturar mecanismos, como uma ouvidoria, para que os titulares possam exercer os seus direitos como acesso, retificação, conhecimento da fonte e das informações pessoais utilizadas em determinado tratamento de suas informações pessoais[705]. Outra sugestão, em contexto de uso de IA, foi:

> a.3. Os procedimentos a serem utilizados na análise dos dados pessoais, seja quanto à mineração destes, seja quanto à inteligência analítica e algoritmos utilizados, deverão ser tornados públicos, de forma que sejam claros e compreensíveis ao titular dos dados os parâmetros principais destas operações e seus possíveis resultados, bem como seus potenciais efeitos para o titular. Eventuais restrições quanto à propriedade intelectual e segredo comercial relacionados à divulgação de algoritmos utilizados, antes que utilizados como justificativas para a opacidade do sistema como um todo, devem fomentar a elaboração de estratégias que permitam ao cidadão ter ciência e segurança quanto aos elementos básicos e fundamentais do funcionamento do sistema de processamento de seus dados para que possa ter ciência das suas consequências e ter elementos para

---

[702] ANPD, 2021, p. 33.
[703] JUNQUEIRA, 2020a, p. RB-3.3.
[704] *Ibidem*.
[705] ITS, 2017.

> identificar e notificar por eventuais abusividades quanto ao tratamento de seus dados e a operação do sistema[706].

O controlador tem um papel de destaque nas decisões automatizadas, ainda que sejam integralmente tomadas pelas máquinas. Por isso, Mulholland e Frajhof[707] sustentam que o controlador terá deveres e ônus de comprovar que a atividade de tratamento não é discriminatória. Ainda que se alegue que, a depender da espécie de tratamento, não seja possível saber como foi tomada a decisão em virtude da opacidade, não se pode admitir a violação de direitos fundamentais e humanos. Nesse sentido, há que se poder ter respostas e responsabilidades para violações de direitos.

Os algoritmos fazem a análise de dados que são cruzados e estruturados e buscam por padrões ou correlações[708]. Portanto, Junqueira explica que pode ser exigido do agente de tratamento, ao utilizar o sistema de decisão automatizada, "[...] o registro dos *inputs*, dos resultados esperados e do processo de treinamento do algoritmo, e a posterior disponibilização deles para auditorias"[709], para maior transparência e para verificar se houve discriminação[710].

Para o exercício da revisão das decisões, será necessária a implementação de diversas medidas para que o titular de dados possa exercer os seus direitos, seja antes da decisão ou posteriormente. Algumas dessas medidas são a governança dos dados e a atuação da ANPD, que serão estudadas a seguir.

3.3 O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS NAS DECISÕES AUTOMATIZADAS

A Autoridade Nacional de Proteção de Dados é uma autarquia de natureza especial, dotada de autonomia técnica e decisória (Art. 55-A, LGPD). Tem a função de "[...] promover na população o conhecimento das normas e das

---

[706] *Ibidem*, p. 50.
[707] MULHOLLAND; FRAJHOF, 2019.
[708] GUTIERREZ, 2019.
[709] JUNQUEIRA, 2020a, p. RB – 2.2.
[710] *Ibidem*.

políticas públicas sobre proteção de dados pessoais e das medidas de segurança" (art. 55-J, inciso VI da LGPD). Deve ser independente tanto para setor privado como para o Estado, pois ambos coletam dados dos cidadãos[711]. Desse modo, a independência da ANPD:

> [...] através da reformulação de sua estrutura organizativa base, ou seja, através de sua transformação em uma autarquia especial, instituição de direito público pertencente à Administração Indireta. Ao assim se proceder, colocar-se-á o Brasil em um cenário de destaque no que diz respeito à proteção de dados pessoais, ao lado dos países que fazem parte da União Europeia[712].

Foi publicado o primeiro planejamento estratégico da Autoridade Nacional de Proteção de Dados, aprovado pelo Conselho Diretor, por meio da Portaria nº 12, de 29 de janeiro de 2021. Ficaram estabelecidos a missão, a visão e os princípios e valores que orientam a atuação da ANPD:

> A missão da ANPD é "Zelar pela proteção dos dados pessoais", e sua visão é "Tornar-se órgão de referência nacional e internacional com relação à Proteção de Dados Pessoais.". A atuação da ANPD baseia-se nos seguintes valores: Ética, Transparência, Integridade, Imparcialidade, Eficácia e Responsabilidade[713].

Além disso, descreve-se que a sua atuação tem como objetivo "[...] proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural"[714]:

> A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão vinculado à Presidência da República, dotada de autonomia técnica e decisória, com jurisdição no território nacional e com sede e foro no Distrito Federal, que tem o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, orientada pelo disposto na Lei nº 13.709, de 14 de agosto de 2018, a LGPD[715].

---

711 SANTIAGO, Mariana Ribeiro; SANTOS, Paulo Jorge. Independência da autoridade fiscalizadora e efetividade da proteção de dados pessoais na sociedade em rede. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 27, n. 2, p. 39-62, 2022. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1711. Acesso em: 9 fev. 2023.
712 *Ibidem*, p. 58.
713 ANPD, 2021.
714 *Ibidem*, p. 06.
715 *Idem*.

Nesse documento também ficaram estabelecidos três objetivos estratégicos. Menciona-se neste estudo dois deles: o primeiro é o de "Promover o fortalecimento da cultura de Proteção de Dados Pessoais"[716], e o segundo consiste em "Estabelecer ambiente normativo eficaz para a Proteção de Dados Pessoais"[717], com o "[...] estabelecimento de prioridades da agenda regulatória, a criação e aprovação dos temas regulatórios e o estabelecimento de procedimentos e mecanismos céleres para o tratamento de incidentes e de reclamações"[718].

Entre os mecanismos de controle das decisões automatizadas está a auditoria a ser realizada pela autoridade nacional de proteção de dados pessoais, em caso de recusa de informações solicitadas, conforme o art. 20, § 2º, LGPD.

Nesse contexto, Alberto Trigo[719] explica que em uma auditoria são verificados os *inputs* e os *outpus* dos dados utilizados. Desse modo não se verifica o funcionamento do programa, mas se foram seguidos os procedimentos e se houve alguma manipulação. Por isso, o autor afirma ser esse controle insuficiente para verificar se há algum defeito no sistema[720]. Junqueira[721], por sua vez, entende que a auditoria é um dos mecanismos mais promissores no controle da discriminação algorítmica e que pode reduzir os riscos envolvidos a um nível aceitável[722].

A auditoria, segundo a LGPD, é de competência da ANPD:

> Art. 55-J: 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

---

716 *Ibidem*, p. 09.
717 *Ibidem*, p. 11.
718 Todos os objetivos resumidamente são: "A ANPD definiu três objetivos estratégicos para a estruturação de seu planejamento, são eles: "Promover o fortalecimento da cultura e Proteção de Dados Pessoais"; "Estabelecer ambiente normativo eficaz para a Proteção de Dados Pessoais"; e "Aprimorar as condições para o cumprimento das competências legais". Este arcabouço resultou em ações estratégicas e indicadores, resumidos na seção "Indicadores e Ações Estratégicas" (ANPD, 2021).
719 TRIGO, Alberto Lucas Albuquerque da Costa. Breves notas sobre o controle das decisões informadas por algoritmos. *In*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O Direito Civil na era da inteligência artificial**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.
720 *Ibidem*.
721 JUNQUEIRA, 2020a.
722 *Ibidem*.

> o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

E o inciso IV desse artigo dispõe ainda que caberá à ANPD fiscalizar e aplicar sanções caso haja o descumprimento à legislação, mediante processo administrativo, no qual será assegurado o contraditório, a ampla defesa e o direito de recurso. Desse modo, a auditoria não precisa se restringir somente às decisões automatizadas, mas ao todas as etapas do processamento dos dados.

Nessa linha, Shea Brown, Jovana Davidovic e Ali Haran[723] propõem uma auditoria algorítmica que tenha aplicação geral, isto é, que não seja específica para reconhecimento facial, ou a autonomia e transparência que rastreia o comportamento na internet. No entanto, uma proposta de auditoria ética do algoritmo foca nos impactos negativos[724].

Isabella Frahjof[725] sugere que sejam estabelecidos procedimentos de controle além do relatório de impacto e certificações, como que padrões devem ser observados para facilitar o entendimento dos algoritmos. No entanto, ao se ler o art. 38 da LGPD, depreende-se que o relatório é uma faculdade — pois utiliza-se o termo “poderá”[726]:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Além da auditoria, pode ser utilizado o relatório de impacto à proteção de dados (RIPDP) em conjunto com a atuação da ANPD. O relatório contém a descrição dos processos de tratamentos de dados pessoais que possam acarretar riscos às liberdades civis ou direitos fundamentais, bem como as

---

[723] BROWN, Shea; DAVIDOVIC, Jovana; HASAN, Ali. The algorithm audit: scoring the algorithms that score us. **Big Data & Society**, [*s. l.*], v. 8, n. 1, jan. 2021. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/2053951720983865. Acesso em: 30 jan. 2023.
[724] BROWN; DAVIDOVIC; HASAN, 2021.
[725] EXPLICABILIDADE..., 2022.
[726] No *Guia orientativo* para o período eleitoral, a ANPD recomendou a elaboração do RIPDP “no contexto eleitoral pode ocorrer o tratamento de um grande volume de dados sensíveis relacionados a opiniões e filiações políticas, o RIPD se torna um instrumento importante de *accountability*” (ANPD, 2021 p. 35).

medidas, salvaguardas e mecanismos de mitigação de risco[727]. Em suma, o relatório consiste na documentação feita pelo controlador a fim de registrar processos de tratamento de dados e as respectivas medidas adotadas para mitigar riscos aos direitos dos titulares dos dados[728]. No entanto, há exceções como segredos comercial e industrial, por exemplo:

> Art. 10, §3º - A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Portanto, esse dispositivo também trata do relatório como uma possibilidade de ser solicitado pela ANPD, e não como uma obrigação[729]. Embora o art. 50, §2º, inciso I alínea "d", determine que sejam feitas "[...] políticas e salvaguardas adequadas com base em processo de avalição sistemática de impactos e riscos à privacidade", ele não deixa claro se haverá sanções ou alguma consequência se não for realizada[730]. O RIPDP é uma medida que pode ser tomada antes da aplicação da decisão automatizada (*ex ante*)[731]. Trata-se de uma documentação feita pelo controlador que deve conter:

> LGPD, Art. 5º inciso XVII - documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

---

[727] LGPD: "Art. 5º, inciso "XVII – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

[728] "[...] controlador – quem tem poder de tomada decisão na cadeia de tratamento de dados" (BIONI; LUCIANO, 2019, p. RB-11.4).

[729] JUNQUEIRA, 2020a.

[730] FRAZÃO, Ana. Nova LGPD: ainda sobre a eficácia do direito à explicação e à oposição. **JOTA**, [*s. l.*], 26 dez. 2018b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-ainda-sobre-a-eficacia-do-direito-a-explicacao-e-a-oposicao-26122018. Acesso em: 30 jan. 2023.

[731] FRAJHO, Isabella Z. O papel dos mecanismos de *compliance* para a operacionalização do direito à explicação de decisões totalmente automatizadas. *In***:** FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022.

Tem-se sugerido que, no treinamento da máquina, se usem dados sensíveis, como raça, para prevenir a discriminação[732], mas que esses não deveriam ser utilizados para a tomada de decisão[733].

> Quiçá, poder-se-ia alegar que o "cumprimento de obrigação legal ou regulatória pelo controlador" (art. 11, inc. II, alínea "a") permitiria o tratamento de dados sensíveis para fins de prevenção à discriminação pelo segurador, uma vez que, nos termos da já referida Circular Susep nº 251/2004, a recusa da contratação de seguro deve ser justificada. É claro que uma tal conclusão teria de passar por rigoroso exame de proporcionalidade à luz da situação fática concreta. O melhor caminho, entretanto, seria uma atuação regulatória da ANPD ou da SUSEP, levando em conta as especificidades de cada modalidade securitária e o desenvolvimento de novas técnicas para a solução do problema da discriminação tarifária no seguro.
> Caso se concluísse que seria mesmo necessário o uso de determinado dado sensível pelo segurador, como a raça, dever-se-iam inventar formas de se permitir fazê-lo sem a solicitação direta ao titular — o que por si só poderia gerar um dano — e de se fiscalizar rigorosamente a sua utilização. Conforme se deu nota anteriormente, uma das maneiras sugeridas até o momento é a estipulação de um terceiro altamente confiável que manteria os dados sensíveis e poderia intervir tanto na fase de treinamento dos dados como na verificação de efeitos discriminatórios[734].

No que diz respeito ao momento da realização da auditoria, há uma cláusula de não-divulgação (*non-disclosure*) e de se manter sigilo de informações estratégicas[735]. Para que a auditoria seja feita pela ANPD, Zanatta[736] entende que dependerá de ser solicitada pela sociedade civil. Para o autor, essa atuação da sociedade civil poderá ocorrer de pelo menos três formas:

> (i) a incidência direta no Conselho Nacional de Proteção de Dados Pessoais, que possui representação da sociedade civil organizada,
> (ii) o uso estratégico do regimento interno da Autoridade Nacional de Proteção de Dados Pessoais e pressão para que a Autoridade inicie processos de auditoria, que ainda não se encontram regulamentados, e
> (iii) a colaboração na construção das normas de fiscalização e poder sancionatório, criando mecanismos participativos de denúncia que possam dar início a um processo formal de auditoria[737].

---

[732] SILVA; TEPEDINO, 2020.
[733] *Ibidem*.
[734] SILVA; TEPEDINO, 2020, p. RB-14.3.
[735] ZANATTA, 2022.
[736] *Ibidem*.
[737] *Ibidem*, 269.

Oliva e Viégas catalogam as seguintes atuações da ANPD no âmbito da pontuação de crédito:

> [...] implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD, fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados e privacidade, estimular a adoção de padrões para serviços e produtos que facilitem o exercício e controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades, bem como o porte dos controladores, entre outras (LGPD, art. 55-J)[738].

Novamente, o legislador faz menção a segredos comercial e industrial e determina que a ANPD deve "[...] zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei" (LGPD, art. 55-J, inciso II).

Entre as responsabilidades do controlador está o ônus da prova de demonstrar a legitimidade do tratamento totalmente automatizado, assim como:

> [...] (i) os dados que são coletados, de que fonte e de que maneira, (ii) quais as linhas gerais de programação dos algoritmos e seus objetivos, (iii) como se deu a programação e o desenvolvimento do algoritmo, (iv) se o algoritmo pode ou não modificar seu próprio código, (v) se tais modificações são previsíveis ou ao menos verificáveis, (vi) quais as categorias relevantes dos perfis e os critérios para cada uma delas, (vii) quais são os *outputs* do processo decisório e como avaliar a sua adequação e acurácia, (viii) se há mecanismos de *feedback*, (viii) se há intervenção humana e em que nível, (ix) quais são os principais impactos e riscos para os titulares de danos, (x) que medidas foram tomadas para conter tais riscos[739].

A realização contínua de auditorias, a atualização dos programas de computador e os relatórios dos procedimentos são mecanismos que contribuem para a transparência[740]. Esse cuidado está em consonância com a segurança dos dados pessoais para evitar os riscos de destruição, alteração, divulgação e

[738] OLIVA; VIÉGAS, 2020, p. 592.
[739] FRAZÃO, 2018b.
[740] LORENZETTO; TEIXEIRA FILHO, 2020.

acesso indevido aos dados pessoais[741]. Para a proteção dos dados devem ser adotadas as seguintes condutas:

> [...] dever do fornecedor de manter sistemas seguros, que protejam os dados pessoais em relação a sua confidencialidade, integridade e disponibilidade. Esses são os objetivos clássicos da segurança da informação, conforme definido por normas técnicas internacionais. Enquanto a confidencialidade refere-se à segurança dos dados contra o acesso não autorizado, a integridade diz respeito à proteção contra a manipulação dos dados e dos respectivos sistemas de informação. Já a disponibilidade denota a necessidade de que os dados estejam acessíveis e visa à proteção contra a perda de dados[742].

A atualização dos programas se coaduna com a segurança e também com a necessidade do monitoramento contínuo, assim como a possibilidade de avaliações retrospectivas de impacto[743]. Devem existir também programas de treinamentos dos sistemas de aprendizagem[744].

3.4 A GOVERNANÇA DOS DADOS PESSOAIS NO ÂMBITO DAS DECISÕES AUTOMATIZADAS

Devido à importância do direito fundamental à proteção de dados pessoais e à potencialidade dos danos, como discriminações e cerceamento de direitos, os programas de governança podem colaborar para a aplicação do princípio da prevenção, previsto no art. 6º da LGPD, inciso VIII, que consiste na prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Esse princípio engloba também questões técnicas, como de segurança dos dados[745], de treinamento do sistema e da criação do programa para tomar decisões automatizadas.

---

[741] MENDES, 2014.
[742] *Ibidem*, p. 218.
[743] HOFFMANN-RIEM, 2020.
[744] *Ibidem*.
[745] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, p. 13-14, nov. 2019. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 30 jan. 2023.

Como tem sido visto, a proteção desse direito fundamental se inicia desde o desenvolvimento dos programas de IA e devem percorrer até o tratamento dos dados, como também nas decisões automatizadas. Para atingir esse objetivo:

> [...] a LGPD prevê que os agentes poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais[4], considerando a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento[746].

Tem-se como objetivo a mudança de cultura[747] dos agentes de tratamento para que adotem boas práticas ao longo do seu trabalho. Portanto, pode-se dizer que *compliance* consiste em:

> [...] um conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade[748].

Outra maneira de conceituar *compliance* é a seguinte: "[...] a adesão dos agentes de tratamento de dados pessoais a padrões e normas, oriundas de leis, do mercado e das próprias organizações, aos princípios de boa governança e aos padrões éticos e sociais comumente aceitos"[749].

Além disso, a governança e o código de boas práticas têm como objetivo estabelecer questões operacionais no que diz respeito ao processamento de dados, definição de padrões técnicos e de quais mecanismos serão utilizados na estruturação do sistema[750].

---

[746] VAINZOF, Rony. Capítulo I, Disposições preliminares. *In*: MALDONADO; Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. RL-1.2

[747] *Ibidem*.

[748] FRAZÃO; CUEVA, 2022, p. RB-1.2.

[749] MULHOLLAND, Caitlin; GOMES, Rodrigo D. P. Inteligência artificial e seus principais desafios para os programas de *compliance* e as políticas de proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022. p. RB-6.1.

[750] FRAZÃO; CUEVA, 2022.

A LGPD, no art. 50, traz disposições sobre as boas práticas e a governança, com o objetivo de que os agentes de tratamento se autorregulem, ou seja, formulem as suas próprias regras[751]. Esse artigo enumera requisitos mínimos para o programa de governança[752]. Afinal, cada setor terá as suas próprias necessidades quanto às normas de segurança e de padrões técnicos[753]. Esses programas podem ser denominados de programas de conformidade, integridade ou *compliance*[754].

A autorregulação ou a corregulação contribuem para a efetividade da autovigilância, pois terão regras próprias e boas práticas que atendam à atividade desempenhada e os riscos assumidos[755]. As boas práticas podem se concretizar com a edição de cartilhas explicativas[756].

A adoção de boas práticas contribui para evitar violações de direitos, bem como para orientar os agentes de tratamento[757]. Há, portanto, o *compliance* específico denominado de "*compliance* de dados", o qual tem como objetivo dar efetividade aos direitos do titular de dados pessoais[758].

Esses são alguns dos parâmetros a serem aplicados e atendidos pela governança dos algoritmos, pois cada setor específico que envolva o consumidor terá delineamentos e legislações próprias, como os setores de planos de saúde e de seguradoras, os quais não cabe abordar detalhadamente neste estudo. A LGPD prescreve que:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como

---

751 JIMENE, 2019.
752 MIRAGEM, 2019.
753 JIMENE, *op. cit.*
754 CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020, p. 371-384.
755 ABILIO; FRAZÃO; OLIVA, 2020.
756 TEIXEIRA; ARMELIN, 2020.
757 ABILIO; FRAZÃO; OLIVA, 2020.
758 FRAZÃO; CUEVA, 2022.

> considerem os devidos padrões éticos relacionados a estudos e pesquisas.
> § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

Para a proteção dos dados deve-se avaliar[759]:

> (i) em que momentos há a utilização de dados pessoais;
> (ii) que dados são esses;
> (iii) como e por quem esses dados foram coletados;
> (iv) como a utilização a utilização desses dados se relaciona com a atividade desenvolvida;
> (v) o que ocorre com esses dados, uma vez que ingressam e, por fim,
> (vi) se e como saem do controle da organização[760].

A partir dessa análise, será possível verificar se os dados foram excluídos, anonimizados, por exemplo, ou se eles são essenciais para a atividade ou serviço prestado[761]. As atuações enumeradas no art. 50, *caput* da LGPD, são considerados requisitos mínimos. O art. 51 estabelece que a ADPD estimulará a adoção de padrões técnicos, os quais serão controlados pelos titulares dos dados pessoais. Isso significa que:

> A participação do titular deverá influenciar na valoração positiva das normas de *compliance* pela ANPD, de modo que o envolvimento da sociedade civil na própria construção das normas corporativas e revisão da política de privacidade pode ser um relevante indício da robustez do programa[762].

Entre as diversas condutas a serem adotadas que podem ser incluídas na governança e nas boas práticas está o código de conduta. As ações tomadas após a tomada da decisão (*ex post*) podem ser a documentação sobre o desenvolvimento do sistema para que tanto os desenvolvedores como os titulares dos dados possam compreender como ele funciona. Uma das opções é:

---

[759] ABILIO; FRAZÃO; OLIVA, 2020.
[760] *Ibidem*, p. 691.
[761] *Ibidem*.
[762] *Ibidem*, p. 696.

> O *model card* é uma carta que reúne diversas informações sobre o modelo de ML, tais como: resultados do seu comportamento (*performance*), os casos para os quais ele foi desenvolvido, o contexto em que será aplicado e seus potenciais riscos, métricas para avaliar vieses e discriminações, resultados dos seus testes, quais foram os dados que foram utilizados, entre outras. O objetivo do *model card* é a propositura de um padrão ético de documentação de modelos de ML, para que as pessoas envolvidas no seu desenvolvimento sejam capazes de estabelecer uma métrica ética para avaliar esses algoritmos, principalmente em relação a potenciais discriminações advindas dos dados utilizados para o aprendizado do modelo. Como consequência, essa documentação fornece maior transparência e conhecimento sobre o artefato para um público mais amplo, como desenvolvedores de *software*, especialistas em ML e IA, reguladores, organizações, e pessoas impactadas, indicando as limitações do modelo, os tipos de erros, as discriminações e injustiças que podem ocorrer[763].

A despeito disso, esse item terá como foco as ações voltadas para o titular dos dados, entre elas está um canal de comunicação. A ouvidoria é esse canal de comunicação com o titular dos dados e tem como objetivo aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências (LGPD, art. 40, §2º, inciso I). Portanto, trata-se do canal de comunicação externo que tem como finalidade atender às requisições do titular dos dados e analisar a pertinência delas[764]. Para isso o titular deve saber quem é o encarregado pelo tratamento dos dados pessoais que será indicado pelo controlador. Será pública a identidade e as informações de contato do encarregado, as quais deverão ser divulgadas, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador (art. 41, §1º, LGPD).

A ANPD elaborou um guia orientativo para a aplicação da LGPD por agentes de tratamento no contexto eleitoral. Nele há diversos conceitos como também orientações sobre o programa de governança de dados, das quais serão mencionadas algumas das recomendações que poderão ser úteis ao tema aqui abordado. Consta nesse guia que se deve privilegiar "[...] a comunicação transparente com a pessoa titular, com o objetivo de estabelecer relação de confiança com esta, assegurando, inclusive, mecanismos para sua participação nas atividades de tratamento"[765]. Além disso, deve existir uma estrutura geral de

[763] FRAZÃO; CUEVA, 2022, p. RB-19.5.
[764] ABILIO; FRAZÃO; OLIVA, 2020.
[765] ANPD, 2021, p. 35.

governança de agentes de tratamento e devem-se estabelecer e aplicar mecanismos de supervisão internos e externos[766]. Entre as atividades desempenhadas pelo programa de governança de dados estão o mapeamento de dados, bem como informar às pessoas titulares de dados sobre como os dados pessoais são tratados[767].

Outro aspecto importante, uma vez que o assunto tratado neste estudo é a decisão automatizada, é que os programas de *compliance* de dados devem contribuir para verificar se a tecnologia esteja de acordo com a legislação de proteção de dados e com os direitos fundamentais[768].

Ademais, conforme o art. 49 da LGPD, os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, assim como aos padrões de boas práticas e de governança, sem se descuidar, claro, dos princípios gerais previstos nessa lei e nas demais normas regulamentares.

Por seu turno, a auditoria não precisa se restringir ao momento posterior à tomada de decisão automatizada. Em razão disso, Jakob Mökander e coautores propõem uma auditoria baseada na *ethics-based auditing* (EBA)[769] como um mecanismo de governança que pode ser utilizado por desenvolvedores dos sistemas. Geralmente, são mencionados pelos estudiosos os seguintes princípios a serem observados: da não-maleficência, da autonomia, da justiça e

---

[766] *Ibidem*.

[767] "Uma atividade importante é o mapeamento dos dados pessoais tratados pelo(a) agente de tratamento, que pode ser consolidado em um inventário de dados pessoais. Esse inventário irá descrever todos os processos que tratam dados pessoais, informando, por exemplo: • as finalidades do tratamento; • as bases legais para o tratamento (art. 7º e 11 da LGPD); • as categorias de dados pessoais tratados; • a existência de decisões tomadas com base em tratamento automatizado e suas características; • a ocorrência de compartilhamento de dados incluindo, se for o caso, a transferência internacional de dados, quem são os destinatários, que dados são compartilhados e as hipóteses legais para o compartilhamento; • o tempo de retenção dos dados e os locais onde são armazenados; • as práticas de eliminação e descarte dos dados pessoais; • os meios pelos quais os direitos das pessoas titulares de dados podem ser exercidos; • as medidas de segurança técnicas e administrativas implementadas. 73. É importante que as políticas informem às pessoas titulares de dados como os dados pessoais são tratados, estabeleçam orientações internas para o tratamento de dados pessoais, definam as medidas de segurança técnicas e administrativas que devem ser adotadas e informem sobre a utilização de *cookies* ou outros rastreadores eletrônicos" (ANPD, 2021, p. 33-34).

[768] ABILIO; FRAZÃO; OLIVA, 2020.

[769] MÖKANDER *et al*., 2021.

da explicação[770]. Os autores chamam a atenção para o fato de que, embora esses princípios possam ser úteis, podem ser de difícil aplicação em virtude da interpretação deles, podem ser muito vagos na tradução de uma língua para outra, ou podem ser muitos vagos para terem uma aplicação prática.

Esse tipo de auditoria pode colaborar com os indivíduos para que possam compreender como uma decisão específica é tomada e como se opor a ela[771]. A auditoria tem potencial complementar de contribuir para o aprimoramento de outras ferramentas e métodos de supervisão humana, de certificação e de regulamentação[772]. Nesse sentido, cada organização pode criar e implementar os seus princípios éticos e utilizá-los para promover as suas auditorias[773]. Além disso, a auditoria pode ser feita por um auditor interno, estatal ou terceiro designado para essa função, desde que consiga ser independente[774].

Pode-se resumir que as estruturas revisadas propostas pela EBA se convergem em um procedimento baseado na avaliação de impactos[775]. São oito etapas: a descrição do propósito da decisão automatizada; definição dos padrões ou critérios verificáveis em que a decisão deve ser avaliada; divulgação do processo e de um relato completo dos dados usados e de como foram usados; avaliação dos impactos das decisões automatizadas sobre as pessoas, comunidades e o seu ambiente; avaliação de se os benefícios e os riscos justificam o uso da máquina; determinação de até que momento o sistema pode ser considerado confiável, seguro e transparente; documentação dos resultados e das considerações; reflexão e avaliação periódica[776].

---

[770] "Although varying in terminology, the different guidelines broadly converge around five principles: beneficence, non-maleficence, autonomy, justice, and explicability (Floridi & Cowls, 2019). While a useful starting point, these principles tend to generate interpretations that are either too semantically strict, which are likely to make ADMS overly mechanical, or too flexible to provide practical guidance (Arvan, 2018)" (MÖKANDER *et al*., 2021, p. 44).

[771] "[...] EBA can also serve the purpose of helping individuals understand how a specific decision was made as well as how to contest it" (MÖKANDER *et al*., 2021, p. 43).

[772] MÖKANDER *et al*., 2021.

[773] "But organizations that design and deploy ADMS may also formulate their own sets of ethics principles and use these as a baseline to audit" (MÖKANDER *et al*., 2021, p. 43).

[774] "Whether the auditor is a government body, a third-party contractor, an industry association, or a specially designated function within larger organizations, the main point is to ensure that the audit is run independently from the regular chain of command within organizations (Power, 1999)" (MÖKANDER *et al*., 2021, p. 43).

[775] MÖKANDER *et al*., 2021.

[776] "To synthesize, the reviewed EBA frameworks converge around a procedure based on impact assessments. IAF (2019) summarized this procedure in eight steps: (1) Describe the purpose of

Os procedimentos da EBA devem ser holísticos, rastreáveis, capazes de apontar a ligação entre comportamentos antiéticos e sanções proporcionais para o caso; estratégicos; dialéticos; contínuos. Além disso, devem ser capazes de reformularem o sistema, se necessário[777]. Ademais, os sistemas também devem ser testados em uma variedade de cenários típicos e atípicos. A EBA deve ser incentivada pelos legisladores, bem como para que seja feita de maneira voluntária[778].

Cathy O'Neil também defende a transparência[779], a auditoria dos algoritmos e que, nesse processo, deve-se partir do pressuposto da opacidade deles, tendo que ser estudados os seus resultados (*outputs*). Desse modo, será possível verificar as suposições por trás do modelo e verificar a justiça deles[780].

Portanto, a revisão da decisão automatizada, o direito à explicação e o devido processo informacional são alguns dos mecanismos que podem ser aplicados após a decisão, mas não são os únicos meios para tratar a complexidade que envolve uma decisão automatizada. Além disso, a aplicação das sanções previstas no art. 52 da, LGPD levará em consideração os seguintes parâmetros e critérios, em processo administrativo:

---

the ADMS; (2) Define the standards or verifiable criteria based on which the ADMS should be assessed; (3) Disclose the process, including a full account of the data use and parties involved; (4) Assess the impact the ADMS has on individuals, communities, and its environment; (5) Evaluate whether the benefits and mitigated risks justify the use of ADMS; (6) Determine the extent to which the system is reliable, safe, and transparent; (7) Document the results and considerations; and (8) Reflect and evaluate periodically, i.e. create a feedback" (MÖKANDER *et al*., 2021, p. 43).

[777] "For EBA to be effective, auditors must be able to test ADMS for a wide variety of typical and atypical scenarios" (MÖKANDER *et al*., 2021, p. 44).

[778] "Regulators can therefore support the emergence and implementation of voluntary EBA procedures by providing the necessary infrastructure to share information and create standardized reporting formats and evaluation criteria (Keyes et al., 2019)" (MÖKANDER *et al*., 2021, p. 44).

[779] "First, we need to demand transparency. Each of us should have the right to receive an alert when a credit score is being used to judge or vet us. And each of us should have access to the information being used to compute that score. If it is incorrect, we should have the right to challenge and correct it" (O´NEIL, 2016, p. 213).

[780] "To disarm WMDs, we also need to measure their impact and conduct algorithmic audits. The first step, before digging into the software code, is to carry out research. We'd begin by treating the WMD as a black box that takes in data and spits out conclusions. This person has a medium risk of committing another crime, this one has a 73 percent chance of voting Republican, this teacher ranks in the lowest decile. By studying these outputs, we could piece together the assumptions behind the model and score them for fairness" (O´NEIL, 2016, p. 207).

> Art. 52, §1º, I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Essas sanções são independentes da responsabilidade civil e não substituem a aplicação de sanções administrativas, civis ou penais definidas no CDC e em legislação específica. Essa disposição tem um aspecto pedagógico e de incentivo para que se adotem condutas e práticas para proteger os dados pessoais e os direitos fundamentais envolvidos no processamento de dados pessoais. Por outro lado, tem-se como objetivo não se obstaculizar a inovação e o desenvolvimento da tecnologia. Isso se deve à concepção trazida pela LGPD ao incentivar que sejam tomadas medidas preventivas, o que flexibiliza os modelos tradicionais da atuação estatal na via judicial para que os agentes de tratamento atuem de maneira a evitar danos aos sujeitos[781].

Nas relações de consumo haverá a atuação da ANPD, dos integrantes do Sistema Nacional de Defesa do Consumidor, além da "[...] atuação do outro órgão ou entidade da Administração com competência regulatória ou de supervisão específica sobre o setor econômico a que se vincule o fornecedor"[782].

Ademais, o tratamento de dados pessoais deverá observar a boa-fé (LGPD, art. 6º, *caput*), que tem entre as funções a observância de deveres anexos aos que decorrem da lei ou do conteúdo expresso da relação jurídica

[781] MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança da informação e governança como parâmetros para a efetiva proteção de dados pessoais. **Revista do Ministério Público do Estado do Rio de Janeiro**, Rio de Janeiro, n. 78, p. 157-164, out./dez. 2020.
[782] MIRAGEM, 2019, p. 06.

(LGPD, art. 9, §3º; 18)[783]. Pode-se mencionar como os deveres a cooperação, a lealdade e as legítimas expectativas das partes[784].

Nota-se que há uma mudança de paradigma no que diz respeito às justificavas das seguradoras[785] e daqueles que concedem empréstimo. Esses estavam em uma posição de assimetria da informação[786], e agora argumentam que há maior risco nos seus negócios por poderem ser mais afetados pelo inadimplemento e pela falta de informação do contratante.

Agora, não só o setor privado e o setor público têm acesso a uma imensa quantidade de informação, há também a possibilidade de compartilhamento dela de maneira muito mais rápida. Cada setor pode ter o seu banco de dados e sistema próprio para o tratamento de dados. Diante disso, há uma maior necessidade para a proteção dos titulares dos dados assim como de grupos de pessoas que são impactados pelas decisões automatizadas e pela criação de perfis. Deve-se encontrar um equilíbrio nessas relações e na proteção efetiva dos direitos fundamentais.

Até este passo, foram mencionadas diversas situações em que a decisão automatizada trouxe prejuízos a pessoas ou a grupos de pessoas. Apesar disso, deve-se ressaltar que a autora Cathy O´Neil[787] destaca diversos projetos em que se tem utilizado modelos matemáticos para contribuir para a sociedade de maneira positiva, tais como um sistema que ajuda a eliminar componentes de produtos que foram construídos com mão de obra escrava[788]. Há um outro modelo que foi desenvolvido para prever em quais residências seria provável que uma criança possa sofrer abusos[789]. Não cabe aqui tratar delas, mas

---

[783] *Ibidem*.
[784] *Ibidem*.
[785] JUNQUEIRA, 2020a, p. RB-3.5.
[786] CC/2002: “Art. 766. Se o segurado, por si ou por seu representante, fizer declarações inexatas ou omitir circunstâncias que possam influir na aceitação da proposta ou na taxa do prêmio, perderá o direito à garantia, além de ficar obrigado ao prêmio vencido. Parágrafo único. Se a inexatidão ou omissão nas declarações não resultar de má-fé do segurado, o segurador terá direito a resolver o contrato, ou a cobrar, mesmo após o sinistro, a diferença do prêmio”.
[787] O´NEIL, 2016.
[788] “Its goal is to use the model to help companies root out the slave-built components in their products” (O´NEIL, 2016, p. 216).
[789] “Another model for the common good has emerged in the field of social work. It’s a predictive model that pinpoints households where children are most likely to suffer abuse” (O´NEIL, 2016, p. 217).

mencionar que, a depender da maneira como forem desenvolvidas e aplicadas, as IA podem contribuir para a sociedade.

Como há diversas maneiras de proteger os titulares de dados e grupos de pessoas para não serem discriminadas ou prejudicadas, em momentos diferentes do processamento de dados, deve-se questionar qual sistema está a ser utilizado e também se verificar se aqueles que desenvolvem os códigos do sistema ainda têm controle sobre ele, ou mesmo se, em caso de desenvolvimento de autonomia da máquina, não se tem mais controle sobre ela[790]. Não obstante isso, se houver um dano, seja material ou moral, caberá ao judiciário analisar a situação[791]. Portanto, não há uma única resposta para toda essa temática, mas parece ser o mais adequado haver a revisão das decisões automatizadas por uma pessoa, assim como um procedimento em que as pessoas possam ter acesso às suas informações e que poderão se opor à decisão automatizada, haja vista a complexidade do sistema tecnológico.

Na fase anterior da decisão automatizada, pode ser utilizado o RIPDP, o qual pode ser solicitado a qualquer momento pela ANPD[792]. A auditoria poderá ser aplicada desde o desenvolvimento do sistema, podendo ser interna, externa, feita por um órgão ligado ao governo ou pela própria ANPD, assim como ser anterior ou posterior à tomada da decisão. O direito à explicação, ao devido processo tecnológico ou informacional também são ferramentas importantes para o efetivo exercício dos direitos para que haja transparência.

Observa-se que a LGPD dispõe de diversos dispositivos que podem ser aplicados à inteligência artificial. Além disso, os agentes de tratamento de dados devem atuar com "correção ética do procedimento"[793], ou seja, o desenvolvimento *privacy by design*, que pode ser mais eficiente para evitar

---

[790] "Loss of control can be broken down into two varieties. A loss of local control occurs when the AI system can no longer be controlled by the human or humans legally responsible for its operation and supervision. A loss of general control occurs when the AI system can no longer be controlled by any human". SCHERER, Matthew U. Regulating artificial intelligence systems: risks, challenges, competencies, and strategies. **Harvard Jounal of Law & Technlogy**, [*s. l.*], v. 29, n. 2, p. 353-400, 2016.
[791] *Ibidem*.
[792] LINDOSO, 2022.
[793] LORENZETTO; TEIXEIRA FILHO, 2020, p. 111.

danos futuros e discriminações diretas ou indiretas[794]. Como visto, diversas medidas para evitar danos e discriminações devem ser tomadas desde o desenvolvimento da máquina, com a participação de uma equipe plural e diversa que reflita a sociedade e as pessoas que a compõem.

[794] JUNQUEIRA, 2020a, p. RB-1.5.

CONSIDERAÇÕES FINAIS

A decisão automatizada envolve vários direitos fundamentais e tem uma potencialidade discriminatória por causa dos algoritmos. O sistema baseado em algoritmos apresentará respostas ou soluções conforme tiver sido desenvolvido. Em alguns casos, como no aprendizado sem supervisão da máquina, ela apresentará soluções a partir dos dados que estejam disponíveis.

Nesse sentido, o direito fundamental à proteção de dados pessoais foi necessário devido ao desenvolvimento e à ubiquidade da tecnologia. Desse modo, não só a privacidade deve ser resguardada no seu aspecto negativo, mas também deve ser propiciado o efetivo controle dos dados pessoais, haja vista que a partir deles se extrai todo o tipo de informações pessoais de alguém ou de um grupo (e nem sempre é possível saber se se trata de dados sensíveis). A natureza do dado deve ser vista no caso concreto, dentro de um contexto, ou seja, ele deve ser funcionalizado. Ademais, a proteção dos dados pessoais sensíveis visa à não discriminação.

É nesse contexto que a proteção contra a discriminação consta como princípio da LGPD. Não obstante isso, deve ser feita uma correlação desse tema com o princípio da igualdade, pois, uma vez que a Constituição da República proíbe tratamento desigual expressamente, deve-se existir a isonomia no aspecto formal e no material — embora, em algumas situações específicas, a lei permita discriminações a fim de promover a igualdade material.

A Constituição da República de 1988 elenca, em seu art. 3º, inciso IV, discriminações históricas, mas deve-se levar em conta a proteção delas, assim como as discriminações indiretas, que são causadas pelas informações obtidas pelo sistema. As discriminações indiretas podem decorrer do endereço, por exemplo. A discriminação pode ser contra um indivíduo ou contra grupos de pessoas, ou seja, na criação de perfis. Em ambos os casos, faz-se uma representação virtual do que seriam essas pessoas. As pessoas e os grupos são classificados previamente para que seja possa antever potenciais riscos nas contratações. Portanto, há no mínimo uma dupla vulnerabilidade causada pelo fato de serem consumidores e por serem considerados como pertencentes a

determinado grupo e terem dificuldade para discutir isso, embora haja direitos previstos.

Há uma generalização feita a partir das decisões automatizadas, que compõem uma identidade virtual que nem sempre corresponde à realidade. Por isso, deve-se verificar se são razoáveis e se são permitidas por lei. Existe uma outra proteção contra discriminação prevista no art. 5 da CRFB, inciso VIII, de que “[...] ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política, salvo se as invocar para eximir-se de obrigação legal a todos imposta e recusar-se a cumprir prestação alternativa, fixada em lei”.

Em razão disso, a proteção dos dados pessoais protege a privacidade, o livre desenvolvimento da personalidade e a autodeterminação informativa, para afastar discriminações e permitir a liberdade das pessoas para que não sejam reprimidas ou tenham os seus direitos restringidos. Para alguns autores como Ingo Sarlet e Dominika Iwan, o direito à proteção de dados pessoais deve ser salvaguardado como um direito humano, devido à transferência dos dados ser um problema que não se restringe ao território de um país.

A proteção dos dados também tem um aspecto coletivo, uma vez que os perfis e as classificações atingem diversas pessoas. Nessas situações, em que a proteção como um direito coletivo pode ser mais adequada e efetiva, há que se considerar o fardo que passa a ser a autodeterminação informativa em cada situação em que haja o tratamento de dados, principalmente nas relações de consumo. Além disso, determinadas informações sensíveis, como opiniões políticas e religiosas, quando manifestadas em público, não têm como característica serem sigilosas. Não obstante isso, para a sua utilização a LGPD, determina que sejam observados os seus princípios, principalmente, que sejam norteados pela finalidade, adequação e necessidade, assim como as hipóteses que autorizam o tratamento de dados pessoais (art. 7º, LGPD).

Este estudo teve como objetivo pesquisar os direitos dos consumidores, que também são direitos fundamentais, pois permitem que as pessoas tenham acesso a bens de consumos e serviços. Também foram vistos alguns casos de discriminações na contratação de seguros de carro. Não foram abordados,

porém, os planos de saúde por se tratar eminentemente de dados pessoais sensíveis e por demandarem legislações específicas.

Com a implementação das tecnologias, a vulnerabilidade dos consumidores não é só fática, jurídica, técnica, mas também informacional, pois muitas vezes esses não têm conhecimento sobre o funcionamento das máquinas, ou nem mesmo sabem que foram colhidos e tratados os seus dados pessoais. Há uma relação de assimetria em relação aos contratantes. Presume-se que aqueles que oferecem os serviços de crédito e de seguro têm mais poder nessas relações. Por isso, a legislação dos seguros determina que os segurados prestem informações verdadeiras. No entanto, com a inteligência artificial e os bancos de dados há uma mudança de paradigma.

Ademais, embora a legislação apresente uma distinção entre dados pessoais e os considerados sensíveis, em muitos casos essa divisão não é estática e dados considerados não sensíveis podem ser causa de discriminação, como a origem do sobrenome e o CEP, por remeterem à origem racial/étnica ou à situação econômica.

Diante disso, Celso Antônio Bandeira de Melo[795] ensina que critérios neutros, como o tempo, não podem justificar a discriminação, devendo-se levar em consideração as circunstâncias que envolvem os fatos. Ademais, há discriminações lícitas, ilícitas e abusivas. A discriminação ilícita está em desacordo com a legislação. A discriminação lícita pode ser abusiva quando utiliza um critério que a princípio não seria relevante e tem como fundamento o comportamento da pessoa.

Os algoritmos, por sua vez, também podem causar discriminações ao fazer uso de dados sensíveis. Esses dados nem sempre estão presentes no *input*, mas a máquina pode obtê-los de modo indireto. As discriminações podem decorrer de erros estatísticos. Em outras situações, as conclusões podem estar estatisticamente corretas, mas reforçarem discriminações não permitidas, como as que afetam determinados grupos de pessoas que sofrem preconceitos ao longo da história.

---

[795] MELLO, Celso Antônio Bandeira de. **O Conteúdo Jurídico do Princípio da Igualdade.** 3 ed. 18 tiragem. Malheiros editores: São Paulo, 2010, p. 32-33.

Nesse contexto, a discriminação causada pelo algoritmo pode limitar o exercício de direitos pelo seu titular. O algoritmo pode ainda fazer generalizações injustas. Desse modo, a tecnologia tem afetado também o princípio da igualdade de maneira direta, pois, ao ter acesso aos dados pessoais, classifica e faz generalizações sobre as pessoas, o que estabelece discriminações que nem sempre podem ser toleradas.

A inteligência artificial contribui para a tomada de decisões de maneira rápida e eficiente, mas há inúmeros exemplos em que essa tecnologia apresenta falhas e causa discriminações. Embora haja diversas técnicas e mesmo a possibilidade de combinações delas, ainda assim existe a opacidade, e a complexidade das IA nem sempre é compreendida pelas próprias pessoas que a desenvolvem.

Por conseguinte, a decisão automatizada tem sido aplicada em diversos setores de consumo, como nos seguros e na concessão de crédito. Em razão disso o Direito deve apresentar resposta às discriminações indevidas, haja vista que há uma limitação técnica e da própria lei (segredo comercial) para se fazer análise do código-fonte. Além do mais, a IA tem a capacidade de dar respostas rápidas e específicas, mas não apresenta soluções complexas para problemas que atingem a humanidade, como as desigualdades sociais, por exemplo. Outro aspecto que deve ser levado em consideração é a equipe que desenvolve a IA, que deve ser composta de maneira que permita a pluralidade e a diversidade de pessoas.

Existem diversos meios para se proteger os dados pessoais e para o exercício da autodeterminação informativa, como o *habeas data.* Contudo, o tratamento de dados deve ser protegido desde o desenvolvimento de um programa de inteligência artificial, que deve observar princípios éticos, bem como a equipe deve ser diversa a fim de que se evite discriminações.

De modo geral, criam-se perfis com a finalidade de classificar os consumidores. Essas classificações, por sua vez, são generalizações que enquadram as pessoas em determinados grupos. A LCP e o CDC estabelecem diversos direitos para a tutela do titular dos dados como: o direito à informação, de acesso, de retificação, notificação, cancelamento entre outros. Portanto,

contribuem para o processamento dos dados e o respeito dos direitos fundamentais. A LGPD também garante o direito à transparência para que os titulares tenham acesso a esses perfis e saibam de que maneira são manipulados.

Além disso, esses perfis são criados a partir dos dados pessoais e de métodos estatísticos que têm como objetivo extrair padrões, classificações, que nem sempre correspondem com a realidade de determinado grupo de pessoas ou com determinada pessoa. Essas classificações são feitas com dados e informações que correspondem ao passado, por isso as pessoas devem ter o direito de contestá-los e de ter livre acesso a eles, de maneira gratuita, como garante a LGPD, art. 6º, inciso IV. Além do mais, a referida lei considera os dados anonimizados como dados pessoais quando utilizados para a formação de perfil comportamental de determinada pessoa natural, se identificada (art. 12, § 2º).

A LGPD oportuniza a revisão da decisão automatizada quando tomada unicamente por meio automático. Mas, ainda que não determine expressamente que a revisão deva ser feita por uma pessoa humana, também não proíbe que seja assim realizada.

De fato, não há como ter uma única resposta para um tema tão complexo. Por isso, foram discutidas as principais soluções que têm sido apresentadas, em que se leva em consideração o que a legislação infraconstitucional brasileira e a Constituição da República apresentam.

Os mecanismos de controle não são excludentes entre si, mas complementares, a depender de que momento se está a analisar as decisões automatizadas — ou se mesmo antes delas, quando da coleta dos dados, do prazo para que possam ser utilizados e armazenados e do resultado apresentado pela máquina, ou seja, antes da decisão em si. Desse modo, devem existir também mecanismos de prevenção para a não violação de direitos fundamentais. A LCP (art. 5º, inciso II), por sua vez, garante ao consulente a possibilidade de solicitar a revisão de decisão realizada de maneira exclusivamente automatizada.

Nesse sentido, a doutrina tem apontado principalmente duas possibilidades para o enfrentamento dessa questão, que são: o devido processo

informacional e o direito à explicação. A doutrina baseada na RGPD desenvolveu estudos e discussões sobre o direito à explicação e as pesquisas nos Estados Unidos se voltam ao devido processo informacional e ao *compliance*, com a finalidade de autorregulação.

Ademais, a RGPD garante o direito à revisão da decisão por uma pessoa humana. Além disso, a decisão automatizada não é obrigatória. A RGPD também assegura ao titular dos dados que possa não se sujeitar a ela, porém estabelece exceções em que ela pode ser aplicada[796].

É por meio da intervenção humana será obtida a explicação. Esse entendimento é da doutrina, bem como do Parlamento, do Conselho Europeu e do grupo de trabalho do artigo 29 para a proteção de dados — embora o Considerando 71 da RGPD não tenha força normativa.

A aplicabilidade do devido processo legal às relações privadas decorre da eficácia horizontal dos direitos fundamentais, que além disso proporcionam a ampla defesa e o contraditório. O devido processo legal assegura o exercício da autodeterminação informativa e a proteção dos dados, o que garante ao titular o controle dos seus dados. Além dos mais, esses direitos podem ser exercidos antes e depois da tomada da decisão, ainda na via extrajudicial, haja vista que o direito à explicação decorre do princípio da transparência.

Há diversos direitos do titular previstos nos art. 18 e 19 da LGPD que devem ser observados, direitos esses que podem ser exercidos antes e depois da tomada da decisão. A LGPD estabelece o prazo de 15 (quinze) dias para que o agente de tratamento informe os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, previstos na LGPD art. 19, inciso II. Além disso, garante o direito à revisão, em seu art. 20.

Também deve ser informado ao titular se houve intervenção humana e se essa foi significativa. A decisão pode ser tomada com base em perfis já definidos anteriormente e nem sempre haverá um perfil prévio para decisão. Essas

---

[796] RGPD, art. 22. 2 “O n. 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados.”

informações devem estar documentadas por aqueles que as utilizam. E o titular dos dados tem o direito de saber quais dados seus foram utilizados e onde foram coletados. Também tem o direito de saber se houve discriminação e qual foi o resultado da decisão.

Já o controlador tem o dever de fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial, art. 20, § 1º da LGPD. Contudo, se não o fizer a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (art. 20, § 2º). Desse modo, a auditoria é um dos instrumentos a serem utilizados para o combate das discriminações algorítmicas.

Não obstante isso, a auditoria pode ser implementada já no desenvolvimento da máquina, para aplicar testes, bem como após as decisões automatizadas. Ou ainda como fiscalização da Autoridade Nacional de Proteção de Dados, por meio de auditoria, para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, caso o controlador não o faça, ou seja, não ofereça as informações, sempre que solicitadas.

Por parte daqueles que desenvolvem um sistema de decisão automatizada, cabe implementar a governança dos dados pessoais. Isso impacta não só naqueles que são atingidos pela decisão, como também mitiga riscos, ou seja, norteia a sua atuação com base no princípio da prevenção e da precaução, o que se refletirá também nas eventuais ações de responsabilidade civil que poderão ter que enfrentar.

Nas decisões automatizadas, deve ser analisado em cada situação se a diferenciação apresentada não é injusta, proibida, ilícita ou abusiva. Isso deve ser feito como intuito de que não se perpetuem discriminações que ocorrem ao longo da história e mais pessoas sejam marginalizadas e excluídas da sociedade.

Ainda se farão necessárias disposições específicas, sejam legislativas ou por parte da ANPD, para melhor regulamentação das decisões automatizadas e para as especificidades de cada setor que as utilizar, haja vista que muitas das disposições, como de autoria de governança, não são imposições, mas

recomendações — muito embora isso não exima os agentes de tratamento de dados de responsabilidade.

Ademais, há autores que recomendam que a auditoria seja aplicada antes mesmo da utilização do sistema, ou seja, que seja realizada durante a fase de testes para averiguar a eticidade do sistema e da equipe que a desenvolve.

Há outras técnicas que podem ser utilizadas para prevenir danos, como o *privacy by design* e *default by design*, assim como medidas preventivas a serem elaboradas e executadas em um plano de governança que inclua boas práticas, certificações, ouvidoria, relatório de impacto (RIPDP), por exemplo.

A *accountability* está prevista na LGPD como um princípio (art. 6º, inciso X), que consiste na "[...] responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". Esse princípio se coaduna com o devido processo informacional e com o direito à explicação, servindo também para aferir se foram tomadas as medidas necessárias para a utilização do sistema. Trata-se de uma espécie de prestação de contas que leva em consideração o risco da atividade desenvolvida.

Nessa esteira, a governança contribui para que seja observado o ordenamento jurídico por toda a equipe, ou seja, pelo ambiente corporativo, e que se permita a transparência, o direito à informação e à explicação. Trata-se de um mecanismo de autorregulação, que tem normas próprias e adequadas às suas operações internas que refletem a proteção dos direitos fundamentais.

Há outras disposições no CDC em que órgãos de proteção do consumidor poderão fiscalizar e aplicar sanções quando envolver direitos dos consumidores. A ANPD também tem a função de fiscalizar e aplicar sanções, que independem da responsabilidade civil. Na sanção a ser aplicada pela ANPD, levar-se-á em consideração a conduta do infrator, como "[...] a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;" e "a adoção de política de boas práticas e governança" (LGPD, art. 52, §1º).

Em suma, a LGPD ressalta a importância da cooperação dos agentes do tratamento de dados para prevenir discriminações e danos aos titulares de dados pessoais. Isso também contribui para que os titulares sejam protegidos, assim como seus direitos fundamentais, e para que haja um equilíbrio de poder entre as partes.

REFERÊNCIAS

ABILIO, Vivianne da Silveira; FRAZÃO, Ana; OLIVA, Milena Donato. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 669-706.

ANPD. **Planejamento estratégico 2021-2023**. Brasília/DF. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf. Acesso em: 11 fev. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo**: aplicação da lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral. Brasília, DF: Tribunal Superior Eleitoral, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf. Acesso em: 07 fev. 2023.

BARCELLOS, Ana Paula. **Curso de direito constitucional**. 4. ed. São Paulo: Grupo GEN, 2022.

BESSA, Leonardo Roscoe. **Nova lei do cadastro positivo**: comentários à lei 12.414, com as alterações da lei complementar n. 166/2019 e de acordo com a LGPD. São Paulo: Thomson Reuters Brasil, 2019.

BESSA, Leonardo Roscoe. Responsabilidade civil e limites normativos para o tratamento de dados do consumidor na pontuação de crédito. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022. p. 316-334.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019. p. RB-11.1-11.8.

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

BIONI, Bruno *et al*. (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo GEN, 2020.

BIONI, Bruno; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeamento convergência na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

BIONI, Bruno; MARTINS, Pedro. Devido processo informacional: um salto teórico-dogmático necessário? **Portal Bruno Bioni**, [*s. l.*], 08 ago. 2020. Disponível em: https://brunobioni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-Processo-Informacional1.pdf. Acesso em: 18 fev. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, [1988]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em: 29 ago. 2022.

BRASIL. **Lei n. 8.078 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, [1990]. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 29 ago. 2022.

BRASIL. Superior Tribunal de Justiça (4. Turma). **Recurso Especial n. 22337/RS**. Serviço de proteção ao crédito. Cancelamento do registro. Prazo (cinco anos). O registro de dados pessoais no SPC deve ser cancelado após cinco anos. Art. 43, § 1º, do Código de Defesa do Consumidor (lei 8.078/90). Recorrente: Clube de Diretores Lojistas de Passo Fundo-RS. Recorrido: José Orivaldo Moreira Branco. Relator: Ministro Ruy Rosado Aguiar, 13 fev. 1995. Disponível em: https://jurisprudencia.s3.amazonaws.com/STJ/IT/RESP_22337_RS_1313696547418.pdf?AWSAccessKeyId=AKIARMMD5JEAO67SMCVA&Expires=1682995976&Signature=5%2FKYSv5n5HYCiGNN1hjtAHa3c80%3D. Acesso em: 15 set. 2022.

BRASIL. **Lei n. 9.507, de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Brasília, DF: Presidência da República, [1997]. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9507.htm. Acesso em: 29 ago. 2022.

BRASIL. **Projeto de lei n. 3.360, de junho de 2000**. Dispõe sobre a privacidade de dados e a relação entre usuários, provedores e portais em redes eletrônicas. Brasília, DF: Câmara dos Deputados, [2000]. Disponível em: http://imagem.camara.gov.br/Imagem/d/pdf/DCD30JUN2000.pdf#page=159. Acesso em: 30 jan. 2023.

BRASIL. Superior Tribunal de Justiça (4. turma). **Recurso Especial n. 1348532/SP**. Consumidor. Cerceamento de defesa. Não ocorrência. Contrato de cartão de crédito. Cláusulas abusivas. Compartilhamento de dados pessoais. Necessidade de opção por sua negativa. Desrespeito aos princípios da transparência e confiança. Abrangência da sentença. *Astreintes*. Razoabilidade. Recorrente: HSBC Bank Brasil. Recorrido: Associação Nacional de Defesa da Cidadania e do Consumidor. Relator: Ministro Luis Felipe Salomão, 10 out. 2010. Disponível em:

https://www.jusbrasil.com.br/jurisprudencia/stj/526809457/inteiro-teor-526809464. Acesso em: 30 jan. 2023.

BRASIL. **Lei n. 12.414, de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, [2011]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 24 ago. 2022.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a lei nº 8.112, de 11 de dezembro de 1990; revoga a lei nº 11.111, de 5 de maio de 2005, e dispositivos da lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2011]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 30 jan. 2023.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 jan. 2023.

BRASIL. Superior Tribunal de Justiça (2. seção). **Recurso Especial n. 1.419.697/RS**. Recurso especial representativo de controvérsia (art. 543-C do CPC). Direito do consumidor. Arquivos de crédito. Sistema “credit scoring”. Compatibilidade com o direito brasileiro. Limites. Dano moral. Recorrente: Boa Vista Serviços. Recorrido: Anderson Guilherme Prado Soares. Relator: Ministro Paulo de Tarso Sanseverino, 12 nov. 2014. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/152068666. Acesso em: 30 jan. 2023.

BRASIL. Superior Tribunal de Justiça (4. turma). **Recurso Especial n. 1268478/RS**. Recurso especial. Ação cautelar de exibição de documentos. Crediscore. Interesse de agir. Demonstração de que a recusa de crédito se deu em razão da ferramenta de scoring, além de requerimento na instituição responsável por este e a sua negativa ou omissão. Relator: Ministro Luis Felipe Salomão, 18 dez. 2014. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/863738929. Acesso em: 17 jul. 2022.

BRASIL. Superior Tribunal de Justiça (4. turma). **Recurso Especial n. 1.365.279/SP**. Direito civil. Recurso especial. Condomínio. Ação de cobrança de multa convencional. Ato antissocial (art. 1.337, parágrafo único, do código civil). Falta de comunicação prévia ao condômino punido. Direito de defesa.

Necessidade. Eficácia horizontal dos direitos fundamentais. Penalidade anulada. Recorrente: Condomínio Edifício São Tomás. Recorrido: Jurandy Carador. Relator: Ministro Luis Felipe Salomão, 25 ago. 2015. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/864106706/inteiro-teor-864106715. Acesso em: 30 ago. 2022.

BRASIL. Supremo Tribunal Federal (plenário). **Recurso Extraordinário com Agravo 652.777/SP**. Constitucional. Publicação, em sítio eletrônico mantido pelo município de São Paulo, do nome de seus servidores e do valor dos correspondentes vencimentos. Legitimidade. 1. É legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias. 2. Recurso extraordinário conhecido e provido. Relator: Teori Zavascki, 23 abr. 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8831570. Acesso em: 30 jan. 2023.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 ago. 2022.

BRASIL. **Lei Complementar n. 166 de 8 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Brasília, DF: Presidência da República, [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp166.htm#art2. Acesso em: 24 ago. 2022.

BRASIL. **Mensagem n. 288, de 8 de julho de 2019**. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: 06 fev. 2023.

BRASIL. Supremo Tribunal Federal. **Referendo na medida cautelar na ação direta de inconstitucionalidade 6.387 Distrito Federal**. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (COVID-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o Instituto Brasileiro de Geografia e Estatística. *Fumus boni juris*. *Periculum in mora*. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Interessado: Presidente da República. Relatora: Ministra Rosa Weber, 11 nov. 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629 . Acesso em: 30 ago. 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. **Estratégia Brasileira de Inteligência Artificial – EBIA**. Brasília, DF: Ministério da Ciência, Tecnologia e Inovações, 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf. Acesso em: 15 set. 2022.

BROWN, Shea; DAVIDOVIC, Jovana; HASAN, Ali. The algorithm audit: scoring the algorithms that score us. **Big Data & Society**, [*s. l.*], v. 8, n. 1, jan. 2021. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/2053951720983865. Acesso em: 30 jan. 2023.

BURRELL, Jenna. How the machine ‘thinks’: understanding opacity in machine learning algorithms. **Big Data & Society**, [*s. l.*], v. 3, n. 1, jan. 2016. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512. Acesso em: 29 jan. 2023.

CAMURÇA, Lia Carolina Vasconcelos; MATIAS, João Luís Nogueira. Direito à privacidade e à proteção de dados pessoais: análise das práticas obscuras de direcionamento de publicidade consoante a lei nº 13.709 de 14 de agosto de 2018. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 6-23, 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1590. Acesso em: 12 ago. 2022.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020. p. 371-384.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020,

CARVALHO, Isadora. O preço do seu seguro será definido pela forma como você dirige. **Quatro Rodas**, [*s. l.*], 05 mar. 2021. Disponível em: https://quatrorodas.abril.com.br/noticias/o-preco-do-seu-seguro-sera-definido-pela-forma-como-voce-dirige/. Acesso em: 30 jan. 2023.

CAVALCANTE, Márcio André Lopes. Informativo esquematizado: informativo 551-STJ. **Dizer o Direito**, [*s. l.*], 2014. Disponível em: https://dizerodireitodotnet.files.wordpress.com/2015/01/info-551-stj.pdf. Acesso em: 05 dez. 2019.

CITRON, Danielle Keats; PASQUALE, Frank A. The scored society: due process for automated predictions. **Washington Law Review**, Washington, v.

89, p. 01-33, 2014. Disponível em: https://ssrn.com/abstract=2376209. Acesso em: 03 fev. 2023.

COMISSÃO EUROPEIA. Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis? **Comissão Europeia**, [*s. l.*], [20--]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt. Acesso em: 10 fev. 2023.

CONSELHO DA JUSTIÇA FEDERAL. I jornada de direito administrativo aprova 40 enunciados. **Conselho da Justiça Federal**, [*s. l.*], 10 ago. 2020. Disponível em: https://www.cjf.jus.br/cjf/noticias/2020/08-agosto/i-jornada-de-direito-administrativo-aprova-40-enunciados. Acesso em: 09 set. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução n. 332, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança na produção e no uso de inteligência artificial no Poder Judiciário e dá outras providências. Brasília, DF: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/files/original191707202008255f4563b35f8e8.pdf. Acesso em: 05 fev. 2023.

COSTA, Carlos Celso Orcesi D. **Cadastro positivo**: lei n. 12.414/2011: comentada artigo por artigo. São Paulo: Editora Saraiva, 2012.

CURSO de inteligência artificial para todos – aula 1. Apresentado por Diogo Cortiz. [*S. l.*: *s. n.*], 2020. 1 vídeo (38 min). Publicado pelo canal Diogo Cortiz. Disponível em: https://www.youtube.com/watch?v=Ze-Q6ZNWpco&ab_channel=DiogoCortiz. Acesso em: 30 jan. 2023.

DIDIER JR., Fredie. **Curso de direito processual civil**: introdução ao direito processual civil, parte geral e processo de conhecimento. 18. ed. Salvador: JusPodivm, 2016.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. O que é a governança de algoritmos? *In*: BRUNO, Fernanda *et al*. (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. 1. ed. São Paulo: Boitempo, 2018. p. 141-148.

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, 2020a.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo GEN, 2020b.

DRUMMONT, Victor. **Internet, privacidade e dados pessoais**. Rio de Janeiro: Lumen Juris, 2003.

EXPLICABILIDADE algorítmica e revisão das decisões automatizadas. [*S. l.*: *s. n.*], 2022. 1 vídeo (81 min). Publicado pelo canal Data Privacy Brasil. Disponível em: https://www.youtube.com/watch?v=Cntu132CjUc&ab_channel=DataPrivacyBrasil. Acesso em: 29 jul. 2022.

FALEIROS JÚNIOR, José Luiz de Moura. A evolução da inteligência artificial em breve retrospectiva. *In*: BARBOSA, Mafalda Miranda *et al.* (coord.). **Direito digital e inteligência artificial**: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021. p. 31-70.

FALLA, Naty. Brasil tem a 3ª maior taxa de juros do mundo; confira o *ranking*: levantamento mostra que país fica atrás apenas de Argentina e Turquia. **Forbes Money**, [*s. l.*], 16 ago. 2022. Disponível em: https://forbes.com.br/forbes-money/2022/08/brasil-tem-a-3a-maior-taxa-de-juros-do-mundo-confira-o-ranking/. Acesso em: 07 fev. 2023.

FERNANDEZ, Elizabeth. Will machine learning algorithms erase the progress of the fair housing act? **Forbes**, [*s. l.*], 17 nov. 2019. Disponível em: https://www.forbes.com/sites/fernandezelizabeth/2019/11/17/will-machine-learning-algorithms-erase-the-progress-of-the-fair-housing-act/#38fa291a1d7c. Acesso em: 05 dez. 2019.

FRAJHOF, Isabella Z. O papel dos mecanismos de *compliance* para a operacionalização do direito à explicação de decisões totalmente automatizadas. *In***:** FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). ***Compliance* e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022. p. RB-19.1-19.9.

FRAZÃO, Ana. O direito à explicação e à oposição diante de decisões totalmente automatizadas. **JOTA**, [*s. l.*], 05 dez. 2018a. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018. Acesso em: 25 ago. 2022.

FRAZÃO, Ana. Nova LGPD: ainda sobre a eficácia do direito à explicação e à oposição. **JOTA**, [*s. l.*], 26 dez. 2018b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-ainda-sobre-a-eficacia-do-direito-a-explicacao-e-a-oposicao-26122018. Acesso em: 30 jan. 2023.

FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana. O jogo da imitação jurídica: o direito à revisão de decisões algorítmicas como um mecanismo para a necessária conciliação entre

linguagem natural e infraestrutura matemática. *In*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O Direito Civil na era da inteligência artificial**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

FRAZÃO, Ana. Decisões algorítmicas e direito à explicação. **Jota**, [*s. l.*], 24 nov. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/decisoes-algoritmicas-e-direito-a-explicacao-24112021. Acesso em: 30 jan. 2023

FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022.

GANDY JR., Oscar H. **The panoptic sort**: a political economy of personal information. Colorado: Records, 1993.

GAVIÃO FILHO, Anizio Pires; FREITAS, Luiz Fernando Calil de. Direitos fundamentais estatuídos não diretamente ou implícitos? **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 25, n. 3, p. 232–257, 2020. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1630. Acesso em: 12 ago. 2022.

GILLIS, Talia B. The input fallacy. **Minnesota Law Review**, [*s. l.*], p. 1-86, 16 fev. 2021. Disponível em: https://ssrn.com/abstract=3571266. Acesso em: 30 jan. 2023.

GOETTENAUER, Carlos. Algoritmos de credit score, dados pessoais: um mapa regulatório para o compliance na análise de crédito. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022. p. RB-24.1-24.8.

GRINOVER, Ada P. *et al*. **Código Brasileiro de Defesa do Consumidor**. 13. ed. São Paulo: Grupo GEN, 2022.

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**. Bruxelas, Bélgica: Conselho Europeu, [2017]. Disponível em: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 16 fev. 2023.

GUTIERREZ, Andriei. É possível confiar em um sistema de inteligência artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de accountability. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019, p. RB-6.1-6.8.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**. São Paulo: Grupo GEN, 2020.

IDEC. Cadastro positivo acolhe sugestões do IDEC, mas mantém pontos críticos. **IDEC**, [*s. l.*], 26 jul. 2019. Disponível em: https://idec.org.br/noticia/cadastro-positivo-acolhe-sugestoes-do-idec-mas-mantem-pontos-criticos. Acesso em: 29 jul. 2019.

ITS. **Transparência e governança nos algoritmos**: um estudo de caso sobre o setor de birôs de crédito. Rio de Janeiro: ITS, 2017.Disponível em: https://itsrio.org/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf. Acesso em: 29 jan. 2023.

IWAN, Dominika. Applicability of human rights control mechanisms in algorithmic decision-making cases. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 269–291, 2021. DOI: 10.25192/issn.1982-0496.rdfd.v26i22286. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2286. Acesso em: 11 fev. 2023.

JIMENE, Camilla do Vale. Capítulo VII, da segurança e das boas práticas. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. RL-1.14-RL-1.15.

JUNQUEIRA, Thiago. Tomada de decisões automatizadas nos seguros privados: tratamento de dados pessoais e prevenção da discriminação racial à luz da LGPD. ***In***: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O direito civil na era da inteligência artificial**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020a. p. RB-14.1-RB-14.5.

JUNQUEIRA, Thiago. **Tratamento de dados pessoais e discriminação algorítmica nos seguros**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020b.

KAPLAN, Jerry. **Artificial intelligence**: what everyone needs to know. Oxford: Oxford University Press, 2016.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da lei 13.709/2018.*In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 441-458.

KOREN, James Rufus. Beyond mere numbers: some leaders and credit scores use unorhordox data – of ten – unrelated to money – to assess potential borrowers. **Los Angeles Times**, [*s. l.*], 20 dez. 2015. Disponível em: https://www.pressreader.com/usa/los-angeles-times/20151220/281990376480210. Acesso em: 24 set. 2022.

LIMA, Caio César Carvalho Lima. Capítulo II, do tratamento de dados pessoais. *In*: MALDONADO; Viviane Nóbregae; BLUM, Renato Opice. 2. ed. **LGPD**: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

LINDOSO, Maria Cristine. O uso do *compliance* e das políticas de proteção de dados como formas de coibir a discriminação algorítmica. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2022. p. RB-13.1-13.8.

LORENZETTO, Bruno Meneses; TEIXEIRA FILHO, Amilcar Cordeiro. A inteligência artificial e o direito à explicação. *In*: SCHIER, Adriana da Costa Ricardo; BITENCOURT, Caroline Müller (org.). **Direito administrativo, políticas públicas e estado sustentável**. Curitiba: Íthala, 2020. p. 97-118.

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

MALDONADO; Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MARQUES, Claudia Lima; BENJAMIN, Antonio Herman. A teoria do diálogo das fontes e seu impacto no Brasil: uma homenagem a Erik Jayme. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 115, p. 21-41, jan./fev. 2018.

MARQUES, Claudia Lima; MIRAGEM, Bruno; MAGALHÃES, Lucia Ancona Lopez de (org.). **Direito do consumidor** - 30 anos de CDC. São Paulo: Grupo GEN, 2020.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança da informação e governança como parâmetros para a efetiva proteção de dados pessoais. **Revista do Ministério Público do Estado do Rio de Janeiro**, Rio de Janeiro, n. 78, p. 157-164, out./dez. 2020.

MARTINS, Pedro Bastos Lobo. **Profiling na Lei Geral de Proteção de Dados**: desenvolvimento da personalidade em face da governamentabilidade algorítmica. Indaiatuba: Foco, 2022.

MEDON, F**ilipe**. Decisões automatizadas: o necessário diálogo entre **a inteligência artificial e a proteção de dados pessoais para a tutela de direitos fundam**entais. *In*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (**c**oord**.**). O Direito Civil na era da inteligência artificial**.** 1**.** ed. São Paulo: Thomson Reuters Brasil, 2020**.**

MELLO, Celso Antônio Bandeira de. **O conteúdo jurídico do princípio da igualdade**. 3. ed. São Paulo: Malheiros Editores, 2010.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. *Habeas data* e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, [*s. l.*], v. 12, n. 39, p. 185-216, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 4 maio 2022.

MENDES, Laura S.; MATTIUZZO, Marcela; FUJIMOTO, Mônica T. Discriminação algorítmica à Luz da Lei Geral de Proteção de Dados. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo GEN, 2020. p. 429-454.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, p. 13-14, nov. 2019. Disponível em: https://brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 30 jan. 2023.

MIRAGEM, Bruno. Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo. *In*: MARQUES, Claudia L.; MIRAGEM, Bruno; MAGALHÃES, Lucia Ancona Lopez de (org.). **Direito do consumidor –** 30 anos de CDC. São Paulo, Grupo GEN, 2020. p. 243-271.

MIRAGEM, Bruno. Sistemas de pontuação de crédito e acesso ao consumo: liberdade de contratar e proteção dos consumidores contra a discriminação injusta. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022. p. 297-315.

MÖKANDER, Jakob; FLORIDI, Luciano. Ethics-based auditing to develop trustworthy AI. **Minds and Machines**, [*s. l.*], v. 31, n. 2, p. 323-327, 19 fev. 2021.

MÖKANDER, Jakob. *et al.* Ethics-based auditing of automated decision-making systems: nature, scope, and limitations. **Science and Engineering Ethics**, [*s. l.*], v. 27, n. 44, p. 1-30, 6 jul. 2021.

MONCAU, Luiz Fernando. **Direito ao esquecimento**: entre a liberdade de expressão, a privacidade e a proteção de dados pessoais. São Paulo: Thomson Reuters Brasil, 2020.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Revista Instituto Igarapé**, Rio de Janeiro, Artigo Estratégico 39, p. 1-27, dez. 2018. 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 em: 08 fev. 2023.

MONTEIRO, Renato Leite; CRUZ, Sinuhe Nascimento e. Desafios da transparência e direito à informação no desenvolvimento de algoritmos de *credit scoring*: uma análise sob a ótica do devido processo informacional. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022. p. 163-192.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Frajhof. Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019. p. RB-13.1-13-6.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). **PUC-Rio**, [*s. l.*], jul. 2021. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 26 set. 2022.

MULHOLLAND, Caitlin; GOMES, Rodrigo D. P. Inteligência artificial e seus principais desafios para os programas de *compliance* e as políticas de proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). *Compliance* e políticas de proteção de dados**.** São Paulo: Thomson Reuters Brasil, 2022. p. RB-6.1-6.6.

OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. Tratamento de dados para a concessão de crédito. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 555-594.

OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022.

O´NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crowm Publishers, 2016.

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

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução: Maria Celina Bodin de Moraes. Rio de Janeiro: Editora Renovar, 2008.

RODRIGUES, Geisa. **Série carreiras federais** – ações constitucionais. São Paulo: Grupo GEN, 2014.

SÁ, Maria de Fátima Freire de; LIMA, Taisa Maria Macena de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 26, n. 04, p. 227-246, out./dez. 2021. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584. Acesso em: 5 ago. 2022.

SAMPAIO, Vinícius. **Proteção de dados pessoais**: da privacidade ao interesse coletivo. Rio de Janeiro: Lumen Juris, 2020.

SANTIAGO, Mariana Ribeiro; SANTOS, Paulo Jorge. Independência da autoridade fiscalizadora e efetividade da proteção de dados pessoais na sociedade em rede. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 27, n. 2, p. 39-62, 2022. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1711. Acesso em: 9 fev. 2023.

SARLET, Ingo W. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. rev. atual. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo W. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: BIONI, Bruno *et al.* (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo GEN, 2020. p. 40-78.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, Curitiba, v. 26, n. 2, p. 81-106, 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 9 fev. 2023.

SARLET, Ingo W. *et al.* **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital**. São Paulo: Saraiva, 2022.

SCHERER, Matthew U. Regulating artificial intelligence systems: risks, challenges, competencies, and strategies. **Harvard Jounal of Law & Technlogy**, [*s. l.*], v. 29, n. 2, p. 353-400, 2016.

SCHWARTZ, Fabio. **Manual do direito do consumidor**: tópicos e controvérsias. 2. ed. Rio de Janeiro: Editora Processo, 2020.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 23. ed. rev. atual. São Paulo: Malheiros Editores, 2004.

SILVA, Nilton Correia da. Compreensão da inteligência artificial e dos seus pressupostos de controle e regulação. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019. p. RB-3.1-3.8.

SILVA, Priscilla; MEDEIROS, Juliana. A polêmica da revisão (humana) sobre decisões automatizadas. **ITS Rio**, [*s. l.*] 10 dez. 2019. Disponível em: https://feed.itsrio.org/a-pol%C3%AAmica-da-revis%C3%A3o-humana-sobre-decis%C3%B5es-automatizadas-a81592886345. Acesso em: 06 fev. 2023.

SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O Direito Civil na era da inteligência artificial**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

SILVEIRA, Sérgio Amadeu da. **Democracia e os códigos invisíveis**: como os algoritmos estão modulando comportamentos e escolhas políticas. São Paulo: Edições Sesc, 2019. (Coleção Democracia Digital).

SIMÃO, Bárbara Prado. **Entre privacidade e eficiência econômica**: a trajetória da pontuação de crédito no Brasil. Dissertação (Mestrado em Direito) – Programa de Mestrado Acadêmico da Escola de Direito de São Paulo da Fundação Getúlio Vargas, Fundação Getúlio Vargas, São Paulo, 2022.

SOUZA, Carlos Affonso; PERRONE, Christian; MAGRANI, Eduardo. O direito à explicação entre a experiência europeia e a sua positivação na LGPD. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020. p. 254-281.

STEIBEL, Fabro; VICENTE, Victor Freitas; JESUS, Diego Santos Vieira de. Possibilidade e potenciais da utilização da inteligência artificial. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019. p. RB-4.1-4-6.

TAKAR, Téo. Seguro de carro é quase R$ 3.000 mais caro em bairro pobre do que em rico. **Portal UOL**, [*s. l.*], 17 out. 2018. Disponível em: https://economia.uol.com.br/financas-pessoais/noticias/redacao/2018/08/17/como-economizar-seguro-carro.htm?cmpid=copiaecola Acesso em: 24 set. 2022.

TAVARES, Clarice *et al*. **O auxílio emergencial no Brasil**: desafios na implementação de uma política de proteção social datificada. [*S. l.*]: Derechos Digitales América Latina, 2022. Disponível em : https://www.derechosdigitales.org/wp-content/uploads/01_Informe-Brasil_Inteligencia-Artificial-e-Inclusao_PT_22042022.pdf. Acesso em: 29 jul. 2022.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais**: comentada artigo por artigo. 2. ed. rev. atual. e ampl. Salvador: Editora JusPodvm, 2020.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

TEPEDINO, Gustavo (coord.). **O direito civil na era da inteligência artificial.** 1**.** ed. São Paulo: Thomson Reuters Brasil, 2020a.

TONIAZZO, Daniela Wendt; BARBOSA, Tales Schmidke; RUARO, Regina Linden. O direito à explicação nas decisões automatizadas: uma abordagem comparativa entre o ordenamento brasileiro e o europeu. **Revista Internacional Consinter de Direito**, Porto, Portugal, v. 7, n. 13, p. 55-69, 2021. Disponível em: https://revistaconsinter.com/index.php/ojs/article/view/63/106. Acesso em: 10 fev. 2023.

TRIGO, Alberto Lucas Albuquerque da Costa. Breves notas sobre o controle das decisões informadas por algoritmos. *In*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (coord.). **O Direito Civil na era da inteligência artificial.** 1**.** ed. São Paulo: Thomson Reuters Brasil, 2020.

TUNES, Suzel. Algoritmos parciais: como a inteligência artificial absorve padrões discriminatórios e o que a ciência pode fazer para evitar essas distorções. **Revista Pesquisa FAPESP**, ed. 287, [*s. l.*], jan. 2020. Disponível em: https://revistapesquisa.fapesp.br/algoritmos-parciais-2/. Acesso em: 05 fev. 2023.

UNA-SUS. Organização Mundial de Saúde declara pandemia do novo coronavírus. **UNA-SUS**, [*s. l.*], 11 mar. 2020. Disponível em: https://revistapesquisa.fapesp.br/algoritmos-parciais-2/. Acesso em: 17 fev. 2023.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas, Bélgica: Parlamento Europeu, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 25 ago. 2022.

UNIÃO EUROPEIA. **Orientações éticas para uma IA de confiança**. Bruxelas, Bélgica: Comissão Europeia, 2019. Disponível em: https://data.europa.eu/doi/10.2759/2686. Acesso em: 24 ago. 2022.

VAINZOF, Rony. Capítulo I, Disposições preliminares. *In*: MALDONADO; Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

VEGA, Italo S. Inteligência artificial e tomada de decisão – a necessidade de agentes externos. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

VERONESE, Alexandre. Os direitos de explicação e oposição diante das decisões automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 381-411.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.º e 11. *In*: BIONI, Bruno *et al*. (coord.). **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020. p. 131-162.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, [*s. l.*], 25 fev. 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469. Acesso em: 25 ago. 2022.

WIMMER, Miriam; DONEDA, Danilo. “Falhas de IA” e a intervenção humana em decisões automatizadas: parâmetros para a legitimação pela humanização. **Direito Público**, Brasília, v. 18, n. 100, p. 374-406, 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6119. Acesso em: 11 fev. 2023.

ZANATTA, Rafael A. F. Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção De Dados Pessoais. MARQUES, Claudia L.; MIRAGEM, Bruno; MAGALHÃES, Lucia Ancona Lopez de (org.). **Direito do consumidor** – 30 anos de CDC. São Paulo: Grupo GEN, 2020.

ZANATTA, Rafael A. F. O uso de informações excessivas nos sistemas de pontuação de crédito: a importância de critérios para aferir discriminação abusiva. *In*: OMS, Juliana (org.). **O consumidor na era da pontuação de crédito**. Belo Horizonte: Caso do Direito, 2022. p. 246-274.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. London: Profile Books, 2019.