# Decisões automatizadas: definição, benefícios e riscos

Nazareno César Moreira REIS[*]

Gabriel Rocha FURTADO[**]

RESUMO: O presente artigo tratou sobre a temática das decisões automatizadas produzidas por máquinas eletrônicas à luz do marco legal sobre o tema no Brasil: A Lei Geral de Proteção de Dados. A pesquisa buscou investigar o que são das decisões automatizadas, quais seus benefícios e riscos à luz das disposições da LGPD. A metodologia usada foi a pesquisa bibliográfica de doutrinas jurídicas e a pesquisa documental de legislação. Diante da complexidade e interdisciplinaridade do tema com outras áreas, mostra-se necessária a análise de textos fora do Direito, tais como de Ciência da Computação e de Filosofia da Tecnologia, em determinados momentos da pesquisa. Para concluir o trabalho, foi traçada uma definição para as decisões automatizada, com base na pesquisa feita, bem como foram pontuados os achados acerca de riscos e benefícios dessa forma decisória.

PALAVRAS-CHAVE: Decisões automatizadas; inteligência artificial; tratamento de dados; dados pessoais e Lei Geral de Proteção de Dados.



TITLE: *Automated Decisions: Definition, Benefits and Risks*

ABSTRACT: *This article studied the theme of automated decisions produced by electronic machines in the light of the legal framework on the subject in Brazil: The General Data Protection Law. The research sought to investigate what are the automated decisions, what are their benefits and risks in light of the provisions of the LGPD. The methodology used was the bibliographic research of legal doctrines and the documentary research of legislation. In view of the*

[*] Bacharel em Direito pela Universidade Federal do Piauí (1997) e Especialista em Direito Tributário e Finanças Públicas pelo Instituto Brasileiro de Direito Público (2004). Juiz Federal da Justiça Federal - Seção Judiciária do Estado do Piauí. Professor do Instituto de Ciências Jurídicas e Sociais Professor Camillo Filho.

[**] Professor Adjunto de Direito na Universidade Federal do Piauí (UFPI). Professor Adjunto de Direito no Instituto de Ensino Superior CEV (iCEV). Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Especialista em Ciências Penais pela Universidade do Sul de Santa Catarina (UNISUL). Bacharel em Direito pela Universidade Federal do Piauí (UFPI). Advogado. Pesquisador visitante no Max-Planck-Institut für ausländisches und internationales Privatrecht, Hamburg-Alemanha. Membro do Instituto Brasileiro de Direito Civil (IBDCivil). Membro Fundador do Instituto Brasileiro de Direito Contratual (IBDCont). Parecerista da Revista Eletrônica de Direito Civil Civilística.com (ISSN 2316-8374). Parecerista da Revista de Ciências Jurídicas Pensar, Unifor (ISSN 2317-2150). Parecerista da Revista de Direito Civil Contemporâneo, RDCC (ISSN 2358-1433). Parecerista da Revista Arquivo Jurídico, UFPI (ISSN 2317-918X). Foi Chefe do Departamento de Ciências Jurídicas (2016-2018). Foi Conselheiro Seccional da OAB/PI (2016-2018). Foi Diretor de Pesquisa e Pós-Graduação da Escola Superior de Advocacia do Piauí, ESA-PI (2016-2018). Foi Membro do Conselho Editorial da Revista da OAB-PI (ISSN 2318-1621). Tem experiência na área de Direito, com ênfase em Direito Privado, atuando principalmente nos seguintes temas: Teoria Geral do Direito Civil, Obrigações, Contratos, Responsabilidade Civil, Direitos Reais, Propriedade Intelectual e Direito do Agronegócio.

*complexity and interdisciplinarity of the theme with other areas, it is necessary to analyze texts outside the law, such as Computer Science and Philosophy of Technology, in certain moments of the research. To conclude the work, an automated decision definition was drawn up, based on the research carried out, as well as the findings about the risks and benefits of this decision-making form were scored.*

KEYWORDS: *Automated decisions; artificial intelligence; data processing; personal data and General Data Protection Law.*



## 1. Introdução

O tema desta pesquisa diz respeito à articulação entre o direito e as decisões automatizadas produzidas por máquinas eletrônicas. Havendo já um marco legal no país sobre o assunto (Lei 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados – LGPD), a investigação volta-se para tentar esclarecer em que consiste as decisões automatizadas, quais os seus benefícios e riscos.

A relevância do tema é grande. O modo de vida atual torna-se cada vez mais dependente das tecnologias da comunicação, em especial dos dispositivos computacionais (fixos ou móveis) e da internet. O trabalho, as compras, o lazer e, enfim, as relações humanas em geral passam por um processo de incorporação à atmosfera digital.

A representação de crescente coleção de fatos da vida em termos de códigos e objetos digitais, por seu turno, tem reduzido a distância entre o plano *off-line* o plano *on-line*, gerando influências recíprocas entre eles e abalando modelos mentais outrora consolidados, em especial aqueles ligados à intimidade e à privacidade.

Como todas as operações com códigos digitais são potencialmente gravadas e tendem a convergir para a internet, no ambiente das redes não há nada informal, nada local e nada completamente oculto à esfera pública. Todas as categorias jurídicas que se

utilizam, portanto, das ideias de informalidade, territorialidade ou de sigilo precisam ser reconsideradas à luz dessa nova realidade material e social.[1]

A massa sempre crescente de dados, produzidos simultaneamente em vários contextos da vida coletiva, desde o âmbito doméstico até à política e à cultura, passando pela agricultura, indústria, comércio, ensino, pesquisa, etc., não fica sob o controle absoluto de nenhum indivíduo ou governo. Esses dados aglutinam-se em grupos geralmente volumosos (*big data*), fundem-se, refundem-se, apartam-se e se propagam inexoravelmente nos meios digitais; e, mesmo quando protegidos por mecanismos de criptografia que imitam no mundo *on-line* os muros, as paredes e os cofres do mundo *off-line*, apresentam suscetibilidades próprias de sua conformação, que precisam ser consideradas pelo direito.[2]

Embora os dados sejam gravados, no modo digital, sob a mesma lógica e segundo um padrão físico homogêneo (como um sinal eletromagnético), os fatos aos quais eles se referem concedem-lhes pesos jurídicos muito variados. Enquanto o meio físico os iguala, os valores humanos subjacentes os hierarquizam, donde surge uma tensão entre a técnica e a política, que acaba se expressando em termos jurídicos.

Assim é que, quando os dados estão ligados a uma pessoa natural identificada ou identificável, isto é, quando dizem respeito a fatos ou atos da vida de um ser humano, indicando aspectos específicos dos seus comportamentos, dos seus gostos, das suas preferências, eles são chamados de "dados pessoais" (LGPD, art. 5º, I), e têm uma proteção legal especial. Se, ademais, forem considerados especificamente os dados da pessoa natural que estão ligados à sua origem racial ou étnica, à sua convicção religiosa, à sua opinião política, à sua filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como os referentes à sua saúde ou à sua vida sexual, dados genéticos ou biométricos — então se fala em "dados sensíveis" (LGPD, art. 5º, II), cuja proteção legal é ainda mais forte.

Esses dados (os pessoais e, mais ainda, os sensíveis) apresentam valor maior para o direito porque são expressões da personalidade humana, estando por isso no centro do

[1] LÉVY, Pierre. *As tecnologias da inteligência*: o futuro do pensamento na era da informática. São Paulo: Editora 34, 1993. Tradução de Carlos Irineu da Costa, p. 115-134.
[2] HILDEBRANDT, Mireille. Privacy as Protection of the Incomputable Self: from agnostic to agonistic machine learning. *Theoretical Inquiries In Law*, Tel Aviv, v. 20, n. 1, p. 83-121, jan. 2019. Disponível em: https://www7.tau.ac.il/ojs/index.php/til/article/view/1622/1723. Acesso em: 17 jul. 2020; CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: toward a framework to redress predictive privacy harms. *Boston College Law Review,* Boston, v. 55, n. 1, p. 93-128, 29 jan. 2014. Disponível em: https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4. Acesso em: 17 jul. 2020.

ordenamento jurídico (CF, art. 1º, III). O esquema doutrinário tradicional, que explica a relação do homem com as coisas por meio dos direitos reais, em especial o direito de propriedade, não atende às necessidades ligadas à proteção dos dados pessoais. É que, por meio desses rastros digitais, com o devido "tratamento", pode-se reconstituir fatos, atos e até pensamentos relacionados a alguém, acossando o ser humano na intimidade de sua vida intelectual, afetiva, moral, política, econômica e social. Os dados pessoais não são, portanto, em relação à pessoa a quem se referem, coisas sobre as quais ela exerce algum direito real, mas sim emanações da sua personalidade, daí porque se fala de um "direito à proteção de dados", e não de um direito de propriedade sobre dados.[3]

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

Os usos desse poder novo e espantoso têm sido muito diversificados. As máquinas têm sido usadas para avaliar a capacidade de pagamento de pessoas que pedem empréstimos,[4] para estimar preços de mercadorias conforme o consumidor que as queira comprar,[5] para prever locais que devem receber maior atenção das rondas policiais,[6] para dirigir carros autônomos,[7] para fazer diagnósticos de doenças,[8] em reconhecimento facial ou detecção de objetos por imagens para diversos fins, em *sites* de busca, veículos autônomos, classificação de crédito, publicidade comercial, seleção de pessoal para vagas de emprego, avaliação de produtos, etc.[9]

---

[3] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p.120-124.

[4] LEE, Tian-Shyug; CHEN, I-Fei. A two-stage hybrid credit scoring model using artificial neural networks and multivariate adaptive regression splines. *Expert Systems with Applications*, [*s. l.*], v. 28, n. 4, p. 743-752, mai. 2005.

[5] HANNÁK, Anikó et al. Bias in Online Freelance Marketplaces: Evidence from TaskRabbit and Fiverr. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, New York, p. 1914–1933, fev. 2017.

[6] PERRY, Walter L. *et al. Predictive Policing:* The Role of Crime Forecasting in Law Enforcement Operations. [*S. l.*]: RAND Corporation, 2013. E-book.

[7] MASSACHUSETTS INSTITUTE OF TECHNOLOGY (ed.). *MIT Technology Review*. Self-driving cars. Topics. Disponível em: https://www.technologyreview.com/topic/smart-cities/self-driving-cars/. Acesso em: 02 jun. 2020.

[8] MIT TECHNOLOGY REVIEW INSIGHTS. How AI is humanizing health care: Artificial intelligence is helping health-care professionals do their jobs better, giving them the tools to build a smarter, more efficient ecosystem. *In*: MASSACHUSETTS INSTITUTE OF TECHNOLOGY (ed.). *MIT Technology Review*. [*S. l.*], 22 jan. 2020. Disponível em: https://www.technologyreview.com/2020/01/22/276128/how-ai-is-humanizing-health-care/. Acesso em: 2 jun. 2020.

[9] RAHWAN, -Iyad et al. Machine behaviour. *Nature,* [s. l.], v. 568, p. 477–486, 24 abr. 2019. Disponível em: https://www.nature.com/articles/s41586-019-1138-y. Acesso em: 2 jun. 2020.

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

Em semelhante contexto, o direito precisa se ocupar da disciplina dessas máquinas cognoscentes, visto que elas estão gerando fatos com importantes consequências jurídicas na vida das pessoas. Levanta-se, entre outras, uma questão que promete ocupar crescente atenção dos juristas em toda parte, mas nesta pesquisa com enfoque no Brasil: em que consistem as decisões automatizadas com base no tratamento de seus dados pessoais? Esse é o problema de pesquisa que será desenvolvido, especialmente, à luz da legislação interna, especialmente da Lei Geral de Proteção de Dados – LGPD (Lei 13.709, de 14 de agosto de 2018, com as alterações promovidas pela Lei n. 13.853, de 8 de julho de 2019).

O objetivo geral da pesquisa, desse modo, é avaliar o que são as decisões automatizadas, quais os riscos e benefícios que elas trazem, bem como quais as soluções jurídicas oferecidas pela LGPD para acomodar essa importante inovação tecnológica dentro do sistema jurídico.

De maneira específica, a pesquisa volta-se para a anatomia da decisão automatizada, intentando analisar os elementos fundamentais que a compõem, de modo a verificar por quais razões elas estão sendo tão utilizadas agota, quais suas vantagens, e quais os riscos inerentes ao iter decisório automático.

A metodologia consiste basicamente em pesquisa bibliográfica de doutrinas jurídicas e a pesquisa documental de legislação e jurisprudência. Como o tema apresenta aspecto interdisciplinar, mostra-se necessária eventualmente também a análise de textos ligados a outras áreas, tais como de Ciência da Computação e de Filosofia da Tecnologia.

Em conclusão, a pesquisa responde o problema de pesquisa, que consiste justamente em explicar em que consistem as decisões automatizadas com base no tratamento de seus dados pessoais

## 2. Conceito de decisões automatizadas

A concepção de uma decisão automatizada envolve vários elementos, e somente se tornou possível com o uso de computadores eletrônicos. Na verdade, apenas em sentido metafórico se pode falar em "decisão" aqui, porque a máquina não age de modo consciente com algum propósito, mas apenas efetua cálculos aritméticos, segundo um programa (algoritmo) e conforme os dados que a alimentam. Logo, as máquinas apenas podem emular a parcela calculável da inteligência humana, não o livre-arbítrio, nem sentimentos, nem emoções.[10]

Como explicam Ajay Agrawal, Joshua Gans e Avi Goldfarb[11], quando a máquina toma uma decisão, ela usa dados de entrada (imagens, textos, sons, etc., que têm de ser reduzidos a um formato digital legível pela máquina), para fazer uma predição. A predição está baseada no "conhecimento" que o algoritmo ou modelo adquiriu na fase de treinamento, com os chamados dados de treinamento. Combinando a predição com o julgamento (escolha da solução, segundo o interesse do programador/desenvolvedor, expresso no algoritmo ou modelo), a máquina de decisão automática indica uma ação a ser efetivada (por humano ou outra máquina) e essa ação leva a um resultado (eventualmente com uma recompensa associada pelo programador). O resultado fornece ao modelo um *feedback* (positivo ou negativo), que assim realimenta todo o processo para decisões futuras.

A diferença entre algoritmo e modelo é fundamental para entender posteriores desdobramentos jurídicos relacionados às decisões automatizadas. Michael Kearns e Aaron Roth[12] explicam que a distinção entre algoritmo e modelo está em que o segundo é o resultado da aplicação do primeiro sobre uma vasta coleção de dados. Enquanto o algoritmo é o conjunto de regras que, aplicadas a um conjunto finito de dados, pode solucionar problemas semelhantes em tempo finito, o modelo é, por assim dizer, um algoritmo com experiência prática anterior em avaliar dados. O modelo tem, portanto, um *background* que condiciona o seu modo de tratar dados novos, encaixando-os na sua "pré-compreensão". Dizem os referidos autores:

---

[10] É certo que existem debates filosóficos, filmes e livros sobre a possível ascensão das máquinas inteligentes ao nível da autoconsciência, quando então ocorreria a singularidade, isto é, um crescimento teoricamente infinito da inteligência das máquinas sem a intervenção humana. Porém, tais discussões estão fora do propósito desta pesquisa. Para um bom panorama do tema, Cf.: CHACE, Calum. *Surviving AI:* the promise and peril of artificial intelligence. Oxford: Three Cs, 2015. Kindle Edition.

[11] AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. *Máquinas Preditivas:* a simples economia da inteligência artificial. Rio de Janeiro: Editora Alta Books, 2018. Tradução de Wendy Campos, p. 74.

[12] KEARNS, Michael; ROTH, Aaron. *The Ethical Algorithm*: the science of socially aware algorithm design. New York: Oxford University Press, 2019. Edição Kindle, p.9.

> As we've suggested, many of the algorithms we discuss in this book would more accurately be called models. These models, which make the actual decisions of interest, are the result of powerful machine learning (meta-) algorithms being applied to large, complex datasets. A crude but useful sketch of the pipeline is that the data is fed to an algorithm, which then searches a very large space of models for one that provides a good fit to the data. Think of being given a cloud of 100 points on a piece of paper, each labeled either "positive" or "negative," and being asked to draw a curve that does a good but perhaps imperfect job of separating positives from negatives. The positive and negative points are the data, and you are the algorithm—trying out different curves until you settle on what you think is the best separator. The curve you pick is the model, and it will be used to predict whether future points are positive or negative. But now imagine that instead of 100 points, there are 10 million; and instead of the points being on a 2-dimensional sheet of paper, they lie in a 10,000-dimensional space.[13]

A "experiência" do algoritmo com os dados de treinamento é aprimorada por meta-algoritmos que otimizam o trabalho de construção do modelo, mediante a revisão sistemática dos dados de saída, segundo o resultado desejado pelo programador, para melhor agrupá-los e interrelacioná-los. O meta-algoritmo mais conhecido e usado é de *backpropagation*, que resumidamente pode ser descrito como um conjunto de instruções para reanalisar várias vezes os dados de saída e corrigir erros de avaliação porventura verificados, mediante um processamento inverso, melhorando o desempenho do modelo e reequilibrando os pesos dos fatores em jogo para a tomada de decisão.[14]

Assim, por exemplo, uma máquina de reconhecimento facial para fins de localização de possíveis foragidos da justiça que estejam circulando em áreas públicas funciona da

---

[13] Como sugerimos, muitos dos algoritmos que discutimos neste livro seriam chamados de modelos com mais precisão. Esses modelos, que tomam as decisões reais de interesse, são o resultado de poderosos algoritmos de aprendizado de máquina (meta-) aplicados a conjuntos de dados grandes e complexos. Um esboço rudimentar, mas útil, do pipeline é que os dados são alimentados para um algoritmo, que então procura um espaço muito grande de modelos por um que forneça um bom ajuste aos dados. Pense em receber uma nuvem de 100 pontos em um pedaço de papel, cada um rotulado como "positivo" ou "negativo", e ser solicitado a desenhar uma curva que faz um bom, mas talvez imperfeito trabalho de separar os positivos dos negativos. Os pontos positivos e negativos são os dados, e você é o algoritmo - experimentando curvas diferentes até chegar ao que você acha que é o melhor separador. A curva que você escolhe é o modelo e será usado para prever se os pontos futuros são positivos ou negativos. Mas agora imagine que em vez de 100 pontos, há 10 milhões; e em vez de os pontos estarem em uma folha de papel bidimensional, eles ficam em um espaço de 10.000 dimensões (tradução nossa)

[14] Para descrição dos aspectos matemáticos da questão, Cf AGGARWAL, Charu C.. *Neural Networks and Deep Learning*: a textbook. New York: Springe, 2018, p. 21 e ss. Esse tipo de meta-algoritmo é usado para otimizar mecanismos de *deep learning* que, como se explicará adiante, são os mais utilizados atualmente em aplicações práticas da chamada Inteligência Artificial.

seguinte maneira: 1º) ela coleta os dados automaticamente (imagens), por meio de câmeras apontadas para os transeuntes em vias públicas (dados de entrada); 2º) o modelo utilizado para analisar esses dados, comparando-os com as imagens dos foragidos armazenadas em seus arquivos, foi previamente treinado com dados de muitos prisioneiros (dados de treinamento), de modo a fazer a associação tida como "correta" pelo programador; 3º) feito o cruzamento, se for encontrado uma correspondência (*match*), a máquina faz a *predição* de que ali está um foragido, com base no alto nível de probabilidade de a imagem coincidir com a do foragido X, por exemplo; 4º) em seguida, a máquina "julga" e aponta aquele suspeito para o operador; 5º) com base nesse julgamento, adota-se uma ação, que são os atos posteriores (que podem ser humanos ou automatizados também — no caso, a detenção do sujeito) que levarão ao resultado (no caso, prisão correta ou incorreta). Conforme esse resultado tenha sido correto ou incorreto, a depender de uma análise humana posterior, a máquina é informada, por *feedback*, para reforçar ou não aquele julgamento.

As regras de julgamento terão sido dadas pelo programador[15] com base em níveis estatísticos de confiabilidade em ambiente de incerteza, daí a semelhança desse processo automatizado com o funcionamento da mente humana. A grande capacidade de adaptação ao ambiente é o ponto forte da inteligência humana; o cérebro humano é capaz de reconhecer padrões, generalizá-los e de ajustar a decisão tendo em conta pequenas mudanças nesses padrões. Os modelos que trabalham com *machine learning*, em particular os de *deep learning*, buscam reproduzir artificialmente essa capacidade adaptativa do funcionamento orgânico do cérebro e, por isso, estão no centro das mais importantes e avançadas aplicações práticas do que se convencionou chamar da Inteligência Artificial.[16]

Observa-se que a decisão automatizada, para além do algoritmo, é fortemente influenciada pelos dados, mais especificamente por três tipos de dados: a) os *dados de treinamento*; b) os *dados de entrada*; e c) os *dados de feedback*. Os dados de treinamento criam o *background* do modelo, numa fase anterior à colocação dele em funcionamento; os dados de entrada, já na fase de aplicação, sinalizam para o modelo o que está no ambiente externo, e os dados de saída são o resultado do processo decisório artificial. Os dados de saída poderão voltar à máquina, como *feedback* positivo ou negativo, para que ela possa se autoajustar ou ser ajustada pelo desenvolvedor.

---

[15] Como se verá adiante, existem métodos de aprendizado de máquina em que, embora as regras iniciais sejam dadas pelo programador, o modelo pode autonomamente ponderar os pesos dos dados, a partir de exemplos que lhe são apresentados, alterando a programação inicial.

[16] ERTEL, Wolfgang. *Introduction to Artificial Intelligence*. Cham (Switzerland): Springer, 2017. Tradução de Nathanael T. Black, p.3

Somente quando os dados de entrada são *dados pessoais* ou quando o julgamento diz respeito a alguma pessoa natural (caso em que os dados de saída são dados pessoais), é que se pode falar em "decisão automatizada", no direito brasileiro, conforme se extrai do art. 20 da LGPD:

> 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 (...)

Ora, se em toda decisão automatizada o titular dos dados (de entrada ou de saída) tem direito de solicitar a revisão, então sempre haverá um titular em tais casos; logo, sempre estão em jogo dados pessoais nas decisões automatizadas, pois o titular é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (LGPD, art. 5º, V).

De fato, há muitos processos automatizados na indústria ou na pesquisa científica que, no entanto, não produzem "decisões", no sentido empregado pela legislação brasileira. Em uma pesquisa científica sobre uma bactéria, por exemplo, pode-se usar processos automatizados para avaliar e prever aspectos ou comportamentos dessa forma de vida, sem que se possa falar, no entanto, em "decisão automatizada", na acepção jurídica da expressão. O mesmo pode ocorrer numa fábrica de parafusos que automatize os processos de avaliação da qualidade de seus produtos: isso não gera decisões automatizadas, no sentido empregado pela LGPD.

A LGPD não chega a definir o que seja decisão automatizada, mas a ela se refere para assegurar ao titular de dados pessoais o *direito à revisão* dessa decisão, bem como o *direito à explicação* sobre os processos e os dados utilizados na formulação da decisão, nos seguintes termos:

> 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)
> § 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.

Adiante analisa-se cada um dos elementos normativos utilizados para a composição de uma definição de decisão automatizada.

### 2.1. Uso de dados pessoais

O dispositivo legal referido estipula alguns elementos que permitem inferir o conceito de decisão automatizada, para os fins da LGPD. Em primeiro lugar, é preciso que a decisão tenha sido tomada mediante o uso de dados pessoais, visto que a lei fala de direitos do "titular" a respeito dessa decisão. E "titular" tem uma definição precisa na LGPD, a saber: é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (LGPD, art. 5º, V). Dados pessoais, por sua vez, são aqueles que produzam informações relacionadas a pessoa natural identificada ou identificável (LGPD, art. 5º, I).

Logo, como referido acima, processos de automatização adotados em atividades que não envolvam dados pessoais, não estão abrangidos pela disciplina da LGPD. Um caso particularmente interessante é o da pessoa jurídica. Os dados relativos a pessoas jurídicas não são dados pessoais, de modo que o tratamento automatizado de dados relacionados às pessoas jurídicas não estão no raio de incidência da norma da LGPD que assegura os direitos de revisão e de explicação — embora não fique excluída a hipótese de se buscar tais direitos, sobretudo em casos de assimetria negocial, por aplicação analógica do Código de Defesa do Consumidor, ou de alguma normativa protetiva específica, ou até mesmo por aplicação direta da Constituição, com base na ideia mais geral de proteção de dados como direito fundamental extensível também às pessoas jurídicas.

Outra questão que pode ser levantada aqui é dos dados anonimizados. Eles não são considerados dados pessoais pela LGPD (art. 12), salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Todavia, a agregação de dados pessoais com posterior anonimização para a criação de modelos preditivos de

comportamento humano individual parece estar dentro da disciplina das decisões automatizadas, sobretudo quando venham a afetar algum interesse individual ou coletivo, pois nesses casos os dados de saída serão pessoais.

Assim é que, por exemplo, o autopreenchimento dos *sites* de busca é modelado a partir de um grande número de pesquisas individuais. Mesmo que a anonimização dos dados que deram base para a formulação do modelo retire o caráter pessoal desses dados, é certo que a decisão automatizada de preenchimento pode vir a trazer danos individuais ou coletivos e, por isso, está sujeito à disciplina do art. 20 da LGPD. É o que ocorre, por exemplo, quando o autopreenchimento se refere a alguma pessoa natural específica. Neste caso, o nome da pessoa é um dado pessoal e a decisão automatizada, ao ligar esse nome a um fato, a uma característica, a uma imagem, enfim a uma informação, produz conhecimento com dados pessoais do interessado.

Há inúmeros exemplos de precedentes, em vários países, sobre a questão do autopreenchimento pelos motores de busca na internet, notadamente o *Google*. Um tribunal em Milão obrigou o *Google* a rever o autopreenchimento de pesquisa que associava automaticamente o nome de uma pessoa, quando pesquisada, à palavra "vigarista".[17] No Japão, a mesma empresa foi obrigada a excluir um autopreenchimento que associava o nome de um indivíduo a crimes cometidos por um homônimo.[18] Em 2013, na Alemanha, um tribunal federal foi mais longe e obrigou o *Google* a eliminar todos os autopreenchimentos difamatórios, quando provocado pelo respectivo interessado.[19]

### 2.2. Tratamento automatizado

O tratamento de dados por mecanismos eletrônicos (digitais) está no cerne da concepção de decisões automatizadas. É por meio do Aprendizado de Máquina (*Machine Learning*), o tipo de programação mais usado em aplicações práticas, que dados pessoais podem ser transformados em informações e em conhecimento, por dispositivos que funcionam de forma autônoma, mediante associações, agregações e desagregações, arranjos e rearranjos de dados; análises de padrões em vastos conjuntos de dados; inferências estatísticas e estimativas probabilísticas — enfim, técnicas

[17] A íntegra de decisão pode ser lida em: MONTI, Andrea. Tribunale di Milano: Ord. 24 marzo 2011. *In*: MONTI, Andrea. *ICT LEX*: Diritto, politica, cultura della Rete. [S. l.], 24 mar. 2011. Disponível em: <https://www.ictlex.net/?p=1285. Acesso em: 7 jan. 2021.
[18] Cf.: https://www.bbc.com/news/technology-17510651, Acesso em: 7 jan. 2021.
[19] AMBROSE, Meg Leta; AMBROSE, Ben M.. When robots lie a comparison of auto-defamation law. *2014 Ieee International Workshop On Advanced Robotics And Its Social Impacts*, [S.L.], p. 56-61, set. 2014. IEEE. http://dx.doi.org/10.1109/arso.2014.7020980.

matemáticas convenientes para extrair conhecimentos de dados, mimetizando o funcionamento da inteligência humana, ou, pelo menos, a parte computável da inteligência humana.

Com efeito, a LGPD, para esboçar a ideia de decisão automatizada, estabelece que tal é aquela que tenha sido tomada "unicamente com base em tratamento automatizado" (art. 20, LGPD). Assim, a lei parece buscar excluir de seu raio de eficácia tanto as decisões decorrentes diretamente da inteligência humana, como as decisões humanas assistidas por processos automatizados, que não devem ser consideradas decisões automatizadas, segundo a lei brasileira.

Nesta altura, vale lembrar a interessante discussão travada nos Estados Unidos caso Loomis *x* Winsconsin. Em fevereiro de 2013, Eric Loomis foi preso por dirigir um carro roubado e por fugir de uma barreira policial em La Crosse (Wisconsin). Após o regular processamento da acusação, ele foi condenado pelo juiz local a uma pena de 6 anos de prisão. A sentença, ademais, negou a liberação condicional do condenado, sob o argumento, entre outras coisas, de que o COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), um modelo utilizado pelo Judiciário de Wisconsin para calcular o risco de reincidência dos acusados, apontava alto grau de periculosidade em Eric Loomis.

A defesa de Loomis apresentou recurso contra essa condenação, alegando que não se sabia exatamente de que maneira o COMPAS funcionava, e que os seus fabricantes naturalmente não iriam revelar, porque nesse sigilo residiria justamente o valor econômico do produto. Assim, o uso desse tipo de ferramenta, segundo a defesa, violaria o devido processo legal, especialmente o direito de ser sentenciado de forma fundamentada e sem o uso de fatores inverificáveis.

A Suprema Corte de Wisconsin rejeitou a apelação,[20] sob o argumento de que o juiz não decidira unicamente com base no tratamento automatizado de dados, mas sim também com base em todo o contexto probatório. A Suprema Corte Americana, para a qual posteriormente foi dirigido um pedido de *writ of certiorari*, rejeitou o julgamento do mérito da questão.[21]

[20] Cf.: https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690. Acesso em: 8 jan. 2021.
[21] Loomis v. Wisconsin, 881 N.W.2d 749 (Wis. 2016), cert. negado, 137 S.Ct. 2290 (2017).

Observa-se que a posição do Judiciário americano, nesse caso, tolerando o uso do tratamento automatizado de dados em um tema tão sensível como é a decisão sobre a liberdade de locomoção, apoiou-se no fato de que a deliberação, em última análise, não foi da máquina, mas sim do humano (o juiz) que apreciou o pedido de liberdade condicional, embora ele possa ter levado em conta a predição do modelo, que indicava alto risco de reincidência.

O problema do grau de contribuição humana para a decisão tende a ser geralmente o de mais difícil abordagem, quando se trata de delimitar o alcance da LGPD na questão das decisões automatizadas. O uso do advérbio "unicamente" parece sugerir que qualquer mínima intervenção humana no processo decisório descaracteriza a decisão como sendo automatizada. Isso porque se a decisão tem intervenção humana, qualquer que seja ela, não é possível calcular quanto dessa decisão decorreu de contribuição da máquina, de modo que, pela lei brasileira, tal decisão não é automatizada.

É certo que a decisão automatizada apenas se torna possível mediante ações humanas anteriores, de programadores, investidores, cientistas de dados, engenheiros, matemáticos, etc.. No entanto, chega um ponto em que o modelo pode funcionar autonomamente, produzindo deliberações de acordo com o seu modo de funcionamento ordinário, mediante a combinação de dados de entrada segundo um procedimento criado total ou parcialmente por programadores. É neste ponto que a intervenção humana pode descaracterizar a decisão como automatizada.

Se a máquina apenas assiste o humano, fornecendo-lhe elementos para avaliar as melhores alternativas, cabendo a escolha do resultado ao humano, isso não pode ser definido como decisão automatizada, segundo a LGPD. Por outro lado, se o humano apenas ratifica a decisão da máquina, sem possibilidade de criticá-la ou descartá-la, então a decisão é automatizada, apesar de eventualmente ser assinada por um ser humano. Neste último caso, ocorre aquilo que se se chama de *rubber-stamping*,[22] ou seja, um mero carimbo do ser humano.

A Autoridade Independente de Dados do Reino Unido[23] e o Conselho Europeu de Proteção de Dados[24] publicaram algumas orientações elucidativas sobre a questão da

[22] BINNS, Reuben; GALLO, Valeria. *Automated Decision Making*: the role of meaningful human reviews. In: ICO. Information Commissioner's Office. 12 abr. 2019. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/ai-blog-automated-decision-making-the-role-of-meaningful-human-reviews/. Acesso em: 11 jan. 2021.

[23] ICO. What does the UK GDPR say about automated decision-making and profiling?. *In*: ICO. *Information Commissioner's Office*. Disponível em: https://ico.org.uk/for-organisations/guide-to-

intervenção humana como causa da descaracterização da decisão como automatizada. Tais orientações podem ser resumidas no seguinte: a) os revisores humanos devem estar envolvidos na verificação da recomendação do sistema e não devem apenas "rotineiramente" aplicar a decisão automatizada (o envolvimento dos revisores deve ser ativo e não apenas simbólico); b) os revisores humanos devem ter uma influência "significativa" (*meaningful*) na decisão automatizada, inclusive com autoridade e competência para ir contra ela; c) os revisores humanos devem "pesar" e "interpretar" a predição da máquina, considerando todos os dados de entrada disponíveis e outros fatores adicionais.

Dois exemplos, citados nas orientações da Autoridade de Proteção de Dados do Reino Unido,[25] podem esclarecer a diferença entre decisão automatizada e decisão humana assistida por processos automatizados: 1º) Pense-se numa fábrica que calcula e paga o valor de uma gratificação dos empregados conforme a sua produtividade, apurada por mecanismos automatizados e sem qualquer intervenção humana ou com intervenção humana meramente homologatória — isso é uma decisão automatizada; 2º) agora pense-se numa fábrica que use mecanismos automatizados para avaliar a pontualidade dos empregados, disparando um aviso a um gerente de recursos humanos sempre que algum empregado, segundo apuração automatizada de dados, chega atrasado mais de tantas vezes — isso não é decisão automatizada, pois a máquina apenas prediz a situação (a falta de pontualidade) e comunica ao ser humano responsável, para que decida e adote a ação adequada.

### 2.2.1. Tratamentos automatizados excluídos do alcance da LGPD (tratamentos domésticos, jornalísticos, artísticos e acadêmicos)

Conforme o art. 4º, I, II e III da LGPD, para além dos casos de extraterritorialidade, não estão sob a proteção da lei especial brasileira os tratamentos de dados que sejam realizados: a) por pessoa natural para fins exclusivamente particulares e não econômicos; b) para fins exclusivamente jornalísticos ou artísticos; c) para fins acadêmicos, observado o disposto nos arts. 7º a 11 da LGPD.

---

data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/. Acesso em: 11 jan. 2021.

[24] JUSTICE AND CONSUMERS (Europea Union). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. *In*: JUSTICE AND CONSUMERS (Europea Union). *European Commission*. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 11 jan. 2021

[25] ICO, *op. cit.*

Significa isso dizer que eventual decisão automatizada tomada com os objetivos acima expostos não está sujeita às restrições da LGPD, notadamente as previstas no art. 20. Tal conclusão decorre logicamente do fato de não ser o tratamento de dados, nesses casos, protegido pela LGPD. Está claro, todavia, que eventual violação a direito individual em tais circunstâncias, especialmente à privacidade ou à imagem do titular de dados pessoais, não deve ficar sem meios de reparação, podendo ser corrigida por instrumentos atípicos mediante a aplicação direta da Constituição, sobretudo por força da cláusula do devido processo legal (CF, art. 5º, LIV).

Afinal, o pressuposto da lei para excluir essas decisões da sua disciplina é de que elas são presumivelmente inofensivas a direitos de terceiros, ou estão albergadas pela liberdade de expressão, ou pela liberdade de investigação científica, de modo que, se for alegado e comprovado dano, ameaça de dano por abuso dessas liberdades, há de existir proteção legal contra a violação, ainda que apenas judicial (CF, art. 5º, XXXV).

### 2.2.2. Tratamento automatizado regulado subsidiariamente pela LGPD (segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais)

Os tratamentos de dados para fins de exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais (LGPD, art. 4º, III), embora sujeitos a futura legislação específica (LGPD, art. 4º, §1º), deverão até lá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal (CF, art. 5º, LIV), os princípios gerais de proteção (LGPD, arts. 2º e 6º) e os direitos do titular previstos na própria LGPD (arts. 17 a 22).

Cabe à Agência Nacional de Proteção de Dados – ANPD um papel preponderante de regulamentação e fiscalização, na falta de lei específica, dos tratamentos de dados não inteiramente sujeitos à LGPD, como é a hipótese daqueles relacionados à segurança pública e à defesa nacional. Nesses casos, deverá a ANPD emitir opiniões técnicas ou recomendações, e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais (LGPD, art. 4º, §3º).

Um ponto de grande interesse na disciplina do tratamento de dados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais (LGPD, art. 4º, III), é que pessoas de

direito privado não podem realizar esses tratamentos (LGPD, art. 4º, §2º) — exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional —, o que está em conformidade com o disposto nos arts. 142 e 144 da Constituição Federal, que atribuem com exclusividade às Forças Armadas e às Polícias Federal, Rodoviária Federal, Ferroviária Federal, Civis, Militares e Penais, a competência para as atividades de segurança externa e interna do país.

Enquanto não advém a legislação específica disciplinando o tratamento de dados para fins de segurança pública e atividades de investigação, o que se observa, pela remissão ampla feita pelo art. 4º, §1º da LGPD, é que eventuais decisões automatizadas tomadas nesse campo estarão sujeitas juridicamente ao disposto no art. 20 da LGPD, além de também deverem atender aos princípios gerais de proteção e ao devido processo legal.

A questão peculiar no tratamento de dados pessoais para fins de segurança e apuração criminal é que, como se sabe, há uma larga tradição jurídica, tanto legislativa quanto jurisprudencial, construída na era analógica, que abria exceções importantes à privacidade quando se cuidava de medidas investigativas requeridas judicialmente por autoridades policiais ou de segurança em geral, independentemente do consentimento do titular e, em alguns casos, até mesmo de sua ciência.

Assim, a proteção à privacidade se dava pela oposição de obstáculos ao acesso às informações íntimas do cidadão (por exemplo: sigilo bancário, sigilo fiscal, sigilo profissional, inviolabilidade de domicílio[26]); obstáculos esses que, excepcionalmente, poderiam ser afastados, com certas reservas procedimentais, a pedido de autoridades policiais. Entretanto, na era digital, esse tipo de garantia torna-se em certos aspectos anacrônica, porque o indivíduo já não governa seus dados, que estão dispersos e profusos em muitos bancos de dados espalhados pela internet; e esses dados podem ser entrecruzados, por mecanismos de inferência apropriados, permitindo a prospecção indireta de informações sobre o indivíduo sem a necessidade de quebra de sigilos.

Nesse contexto, sem prejuízo dos sigilos tradicionais, é fundamental regulamentar a forma como a autoridade policial pode coletar dados pessoais ou reorientar dados já coletados para outros propósitos; como pode tratar esses dados; como pode

[26] Lei Complementar 105/2001; Lei Complementar 104/2001; Lei 5.172/1966 (Código Tributário Nacional); Decreto-lei 2.848/1940 (Código Penal); Constituição Federal, art. 5º, XI.

correlacioná-los com outros, partindo já do pressuposto de que o acesso aos dados não sigilosos pode, indiretamente, levar ao conhecimento de informações sigilosas.

Jacqueline de Sousa Abreu, a esse propósito, faz as seguintes considerações:

> Se o direito à privacidade servia à proteção de escolhas e espaços individuais para realização de intimidade, o direito à proteção de dados pessoais emerge como uma ampla estrutura de proteção regulatória, em atenção a novas formas de danos e riscos a que cidadãos estão expostos. Está assentado na constatação de que a sociedade da informação expõe o indivíduo a diversos riscos de dano físico, material ou moral que comprometem o exercício de sua autonomia, a níveis individual e coletivo. Tais riscos são decorrentes de práticas e/ou estruturas institucionais que se desviam de noções básicas de justiça: ter uma expectativa legítima de respeito e consideração frustrada em suas relações sociais com empresas e com o Estado (pelo uso inesperado de suas informações, pela falta de segurança razoável dispensada a suas informações, pelo uso discriminatório, para dar alguns exemplos), e não possuir instrumentos de remediação, por exemplo.[27]

Constata-se aqui uma premissa que é constante na proteção de dados no ecossistema digital: as possibilidades de produção de informação a partir de dados são tantas e tão diversificadas que é mais conveniente regulamentar a forma como elas podem ser legitimamente implementadas do que tentar usar critérios materiais proibitivos, que sempre foi a técnica mais usada no mundo analógico.

Pequenos fragmentos de informação sobre o investigado, indícios quase desprezíveis, quando devidamente tratados e colocados em contato com grandes volumes de dados pessoais até mesmo de outras pessoas, colhidos muitas vezes para fins inocentes, podem ter um poder revelador insuspeitado. A importância desses fragmentos e indícios acaba se revelando *a posteriori*, em razão das ferramentas de mineração de dados (*data mining*), e não exatamente da matéria de que tratam. Por isso a técnica de isolar e tutelar mais fortemente certos tipos de dados pode não ser suficiente para a adequada proteção de dados pessoais no campo das investigações criminais e da segurança pública em geral.

---

[27] ABREU, Jacqueline de Souza. Tratado de Proteção deTratamento de Dados Pessoais para Segurança Pública: contornos do regime jurídico pós-LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. Edição do Kindle, p. 592-593.

### 2.3. Ameaça ou lesão a interesse juridicamente tutelado

Outro elemento integrante do conceito legal brasileiro de decisão automatizada, constante do art. 20 da LGPD, com forte inspiração na Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, está na necessidade de que a deliberação de máquina ameace ou atinja um interesse juridicamente protegido.

Assim, qualquer demanda, judicial ou extrajudicial, contra o controlador que produza decisões automatizadas está na dependência de que o titular dos dados pessoais alegue e prove a ameaça ou violação, pela decisão automatizada, de algum interesse próprio que tenha a tutela do direito. Depreende-se a contrario sensu que decisões automatizadas inofensivas a direitos individuais ou coletivos não estão sob a tutela da lei — como, de resto, ocorre em qualquer área do direito em relação a atos abnóxios, que recaem no campo da licitude.

Os interesses violáveis por decisões automatizadas são os mais diversos, tais como, por exemplo: liberdade de expressão, numa rede social que use algoritmos para moderar publicações ou filtros de *upload*;[28] imagem, num site de busca que associe automaticamente o nome de uma pessoa natural a uma notícia falsa; direitos autorais, numa rede que publique livremente os conteúdos carregados pelos usuários;[29] patrimônio e imagem, num site de compras que manipule automaticamente preços e ofertas, discriminando pessoas pela localização de sua residência, etc.

Todos esses interesses, quando violados dentro do contexto de processos automáticos de tratamento de dados, podem ser reconduzidos à esfera tutelada pelo direito à proteção de dados e suas manifestações especiais e instrumentais previstas na LGPD.

Embora já existam questões relativamente conhecidas nesse campo das decisões automatizadas, tais como aquelas associadas à discriminação algorítmica, não é possível antecipar todas as possíveis ofensas a interesses protegidos que são suscetíveis de ocorrer por força do tratamento automático de dados pessoais. A maior parte da responsabilidade nesse campo é atípica e centrada mais nos danos que nas condutas, como acentuado no capítulo anterior.

---

[28] SCHILLER, Arnold; WEISKOPF, Tobias. Automated Censorship in the Digital Space. *In*: YOUNG EUROPEAN FEDERALISTS (Europe). *The New Federalist*, 1 maio 2019. Tradução de Nora Teuma. Disponível em: https://www.thenewfederalist.eu/automated-censorship-in-the-digital-space?lang=fr. Acesso em: 9 dez. 2020.

[29] BREEN, Jason. YouTube or YouLose? Can YouTube Survive a Copyright Infringement Lawsuit. *Bepress Legal Series.Working Paper 1950*, Los Angeles, p. 1-37, 18 jan. 2007. Disponível em: https://law.bepress.com/cgi/viewcontent.cgi?article=9209&context=expresso. Acesso em: 10 dez. 2020.

O art. 44, parágrafo único, da LGPD, bem enfatiza que a responsabilidade por tratamento irregular de dados nasce do dano, quando o agente de tratamento não observa as normas de segurança previstas no art. 46 da LGPD.

Sem dano ou ameaça de dano, não há responsabilidade, porquanto não há o que reparar ou assegurar. Assim, o critério inicial para avaliar a presença de uma situação em que a decisão automatizada pode ser questionada ou mesmo anulada, com base em algum direito do titular, é o dano ou o potencial de dano que ela pode causar a interesse juridicamente protegido. Este é um critério de ordem pragmática que está na essência da própria ideia de direito subjetivo. Como explica Manuel A. Domingues de Andrade,

> De toda maneira, onde há um direito subjectivo, ele foi concedido para que através dele fosse obtido o predomínio de certo interesse; tal como a correspondente obrigação ou sujeição foi imposta para que um outro interesse oposto resultasse subordinado àquele.
> Mas uma coisa é o direito subjectivo em si mesmo e outra coisa é a razão por que, ou o fim em vista do qual, a lei atribui esse direito, ou seja o interesse para cuja prevalência tal direito foi concedido.
> O interesse constitui o substrato do direito subjectivo. É-lhe subjacente; está antes dele. Ou então — se assim se prefere — está para além dele. Em todo caso, está fora dele. Não diz respeito à sua estrutura, mas só à sua função. Não tem que entrar, portanto, na definição do respectivo conceito.[30]

O interesse está, consequentemente, no cerne da função de proteção jurídica. É por meio do interesse que, antes de tudo, se pode avaliar a necessidade e a utilidade de mecanismos jurídicos de tutela contra as decisões automatizadas. Se algum interesse juridicamente protegido for violado ou ameaçado pela decisão automatizada, há, quando menos, o direito de questionar em juízo o ato da máquina, por força da garantia do direito de ação (CF, art. 5º, XXXV). Adicionalmente, pode-se invocar os direitos consagrados na LGPD, e, conforme o caso, no CDC, no CC, na Lei do Cadastro Positivo (Lei 12.414/2011), na Lei de Acesso à Informação (Lei 12.527/2011) e em qualquer outra legislação, inclusive tratados, que, mesmo pensados para relações do mundo analógico, possam ser aplicados por semelhança ao contexto digital, conforme determina o art. 64 da LGPD.

---

[30] ANDRADE, Manuel A. Domingues. *Teoria geral da relação jurídica*. Coimbra: Almedina, 1992. v. 1, p. 8.

### 2.4. Definição

Baseado nas premissas acima apresentadas, pode-se construir uma definição que expresse objetivamente em que consiste uma decisão automatizada no contexto da Lei Geral de Proteção de Dados – LGPD.

Decisão automatizada é todo julgamento feito exclusivamente por máquina, com base em predição decorrente de tratamento automatizado de dados pessoais de entrada, segundo um modelo ou algoritmo condicionado por dados de treinamento, que afete imediatamente interesse juridicamente tutelado de pessoa natural, excetuados aqueles que tenham fins particulares e não econômicos, jornalísticos ou científicos.

Em adição, há dois tipos de julgamento que podem ser classificados como decisões automatizadas por equiparação: 1º) aqueles que, satisfazendo as condições referidas acima, recebam intervenção humana meramente homologatória (*rubber-stamping*); e 2º) as perfilizações automáticas, conforme se verá adiante.

No núcleo do processo de decisão automatizada estão técnicas estatísticas que permitem a extrapolação de informações, a partir de amostras de dados de uma população. Evidentemente, essas técnicas estão sujeitas a erros e desvios típicos do campo estatístico, embora no geral sejam confiáveis como processo de inferência e predição.[31] Como dados pessoais são indispensáveis para qualquer tipo de decisão automatizada, dentro do contexto da legislação brasileira, a construção de perfis individuais aparece sempre associada a qualquer julgamento feito por máquina e foi equiparada, por lei, à decisão automatizada.

## 3. Decisões automatizadas e perfilização

A perfilização está tão intimamente ligada às decisões automatizadas que a LGPD (art. 20) a inclui no próprio conceito destas:

> 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.*

[31] KUBAT, Miroslav. *An Introduction to Machine Learning*. 2. ed. Coral Gables: Springer, 2017, p. 231.

Na verdade, porém, a perfilização está mais associada à predição e somente pode ser considerada a decisão automatizada se ela mesma for o objetivo do modelo ou algoritmo. Caso se queira, por exemplo, avaliar a capacidade de pagamento de alguém para efeito de concessão de um empréstimo, a perfilização será parte do tratamento de dados e da predição, mas a decisão não estará nisso, e sim na concessão ou não do empréstimo. A decisão é sempre uma tomada de posição diante dos dados, e não apenas uma inferência estatística. A predição, que decorre das inferências estatísticas, apontará o provável resultado da operação de empréstimo (digamos, há 80% de chance de o indivíduo pagar o empréstimo dentro do prazo); já a decisão estará em definir o titular dos dados como apto ou não para o empréstimo. Por exemplo, certa instituição financeira pode decidir pelo sim, com 80% de chance de pagamento, mas outra pode exigir um limiar de predição maior (digamos, 90%) para contratar o empréstimo. Portanto, a predição não é ainda a decisão; ela é o prenúncio do que provavelmente ocorrerá, caso a decisão seja tomada em um ou outro sentido, à luz dos dados tratados pelo modelo. A preferência por acolher essa probabilidade como um "sim" ou um "não" é que a decisão.

É difícil pensar a decisão automatizada sem algum grau de perfilização. Visto como os dados pessoais, por definição, sempre estão associados a alguma pessoa natural e devem fazer parte do processo de formação da decisão automatizada, como exposto acima; considerando também que o objetivo prático dessas decisões sempre está de algum modo associado à compreensão de características ou do comportamento pretérito de pessoas naturais, para avaliar as suas características ou seus comportamentos futuros, então algum grau de perfilização quase sempre está na base das decisões automatizadas.

Em certos casos, todavia, pode ocorrer decisão automatizada sem perfilização. A Autoridade Independente do Reino Unido menciona, a esse respeito, o caso de uma correção de prova automatizada[32]. Uma banca examinadora pode usar um sistema automatizado para marcar as folhas de respostas de um exame de múltipla escolha. O sistema é pré-programado com o número de respostas corretas necessárias para alcançar marcas de aprovação e distinção. As pontuações são automaticamente atribuídas aos candidatos com base no número de respostas corretas de cada um e os

[32] ICO. What is automated individual decision-making and profiling?. *In*: ICO. *Information Commissioner's Office*. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#:~:text=Automated%20decision%2Dmaking%20is%20the,to%20award%20a%20loan%3B%20and. Acesso em: 27 jan. 2021

resultados estão disponíveis *online*. Trata-se de um processo automatizado de tomada de decisão que não envolve criação de perfil. Mas isso apenas ocorre em situações pontuais, que não busquem utilizar o modelo reiteradamente para o futuro, como essa cogitada, e não representa o coração das aplicações de processos automatizados nos processos produtivos.

O Regulamento Europeu para a Proteção de Dados (GDPR) define a perfilização (ou "definição de perfil", na tradução portuguesa) como algo diferente da decisão automatizada, embora não seja totalmente fiel a essa distinção em outros pontos. Com efeito, o art. 4º, n. 4 do GDPR associa a perfilização com a análise e a predição, que são anteriores à decisão, *verbis*:

> «Definição de perfis», 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 económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

Já em relação à decisão automatizada, o art. 22, n. 1 do GDPR (que, no ponto, foi praticamente copiado pela LGPD) estipula, *verbis*:

> 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.

A associação da perfilização com as decisões automatizadas decorre da circunstância de que, como visto, somente são consideradas automatizadas decisões que utilizem dados pessoais em seu processo de concepção. Como os dados pessoais, por definição, somente são aqueles referentes a uma pessoa natural, então o modelo capaz de produzir decisão automatizada sempre terá dados referentes a alguma pessoa natural como dados de entrada, daí porque a predição que ele fará resultará no prognóstico sobre alguma característica ou comportamento humano, baseado em características ou comportamentos anteriores da mesma ou de outras pessoas naturais que apresentem certo padrão reconhecido pela máquina. A decisão automatizada será baseada nessa predição, por isso ela de alguma maneira está conectada ao perfil decorrente dos dados de entrada.

Assim, um modelo que crie decisões automatizadas para admitir ou negar a entrada de pessoas numa universidade será previamente alimentado com um vasto conjunto de dados anteriores, sobre a admissão e a rejeição de candidatos (dados pessoais, portanto). Matematicamente, o modelo inferirá padrões desse conjunto de dados pessoais: tanto padrões para os que devem ser admitidos, como para os que devem ser rejeitados. Tão logo sejam inseridos os dados de interesse de um novo candidato (local de residência, notas, renda mensal, idade, enfim o conjunto de dados pessoais do postulante à vaga), o modelo predirá se o caso, à luz dos anteriores, é de admissão ou de rejeição; e a decisão de admitir ou rejeitar será tomada com base no grau da predição. É evidente que, em tal contexto, o novo candidato estará sendo perfilizado pelo modelo, embora não seja a perfilização propriamente o objetivo do tratamento de dados; ela é, na verdade, uma etapa para a construção da decisão — seguramente uma etapa muito relevante.

O mesmo ocorrerá em um modelo de previsão de fraudes bancárias, ou de cotação de preços de mercadorias com base nos dados do pretenso comprador, ou em um mecanismo policial ou alfandegário que decida automaticamente quem deve ser fiscalizado preferencialmente. Sempre haverá a concepção de tipos genéricos que serão comparados aos dados pessoais dos sujeitos de interesse, para a solução do problema de negócio. Logo, a perfilização é um passo necessário para a tomada de decisões automatizadas, mas não é a própria decisão automatizada.

As decisões automatizadas podem ser realizadas com ou sem definição de perfis; a definição de perfis pode ocorrer sem que dela decorra uma decisão automatizada. Todavia, a definição de perfis e as decisões automatizadas não constituem necessariamente atividades separadas. Um procedimento iniciado como um processo de decisão automatizada pode tornar-se um procedimento de definição de perfis, dependendo da forma como os dados sejam utilizados.[33]

Em outras circunstâncias, a decisão automatizada pode ou não depender de perfilização, segundo o interesse do desenvolvedor na concepção do modelo. Assim, um sistema automatizado de imposição de multas de trânsito, a partir de imagens de câmeras de monitoramento espalhadas nas vias públicas, pode não levar em conta nenhum fator particular do infrator — nesse caso, portanto, desprezando a perfilização.

[33] Cf.: JUSTICE AND CONSUMERS (Europea Union). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. In: *JUSTICE AND CONSUMERS* (Europea Union). European Commission. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 11 jan. 2021

Mas o mesmo modelo pode ser incrementado, para incluir características específicas do infrator (tempo de habilitação, multas anteriores, profissão, etc.), de modo a calibrar o valor da multa. Nesse caso, a perfilização estaria presente na composição da decisão automatizada.[34]

Pela redação da LGPD, no entanto, deve-se admitir que a perfilização, mesmo quando não seja seguida de uma decisão automatizada, mas sim de uma decisão humana assistida por máquina, deve ser considerada em si mesma uma decisão automatizada por equiparação, já que a lei afirma expressamente que estão incluídas entre as decisões automatizadas aquelas "decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade" (artigo 20, LGPD).

Historicamente, a perfilização antecede o uso massivo de processos automatizados de coleta e tratamento de dados. Já nos anos 1980, falava-se do processo de crescente perfilização em várias áreas, especialmente no campo criminal e no âmbito do marketing direcionado.[35] O método de construção de perfis é notoriamente suscetível às técnicas que estão na base dos processos de aprendizado de máquina, daí porque a coleta massiva e o tratamento automatizado de dados pessoais naturalmente implicaram um processo exponencial de perfilização.

De fato, a perfilização, conforme Roger Clarke,[36] é uma técnica por meio da qual um conjunto de características de um grupo particular de pessoas é inferido a partir de experiências passadas (das mesmas pessoas ou de pessoas com comportamento assemelhado), de modo tal a formar acervos que podem ser comparados com indivíduos no futuro, para avaliar o quanto estes se ajustam às características típicas do grupo. Bem analisada, a ideia de perfilização, em termos de método para conhecer objetivamente a mecânica dos comportamentos humanos, pode mesmo remontar ao conceito de "tipo ideal", de Max Weber,[37] pois na sociologia o estudo de padrões de

---

[34] O exemplo é dado, com pequenas alterações, na página 7 do Guia de Orientações já citado: Cf.: JUSTICE AND CONSUMERS (Europea Union). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. In: *JUSTICE AND CONSUMERS* (Europea Union). European Commission. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 11 jan. 2021

[35] CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. *Journal Of Law, Information And Science*, v. 2, n. 4, jan. 1993. Disponível em: http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/JlLawInfoSci/1993/26.html?query=. Acesso em: 10 dez. 2020.

[36] *Op. cit.*

[37] WEBER, Max. A objetividade do conhecimento nas ciências sociais. In: FERNANDES, Florestan (org.). *Weber*: sociologia. São Paulo: Ática, 1999. Coleção Grandes Cientistas Sociais, p. 79-123.

comportamentos sociais a partir da junção e organização de fragmentos esparsos de condutas individuais e de grupo é uma ferramenta há muito utilizada.

A metodologia matemática, na qual está a essência das técnicas de aprendizado de máquina, usa frequentemente o processo de reunião de objetos por características comuns (conjuntos), para inferir as relações de pertinências ou não de outros objetos. A perfilização por mecanismos automatizados é fundamentalmente um procedimento matemático de coleta, seleção, agrupamento e comparação de dados pessoais.

## 4. Os benefícios das decisões automatizadas

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

Decisões tomadas em massa, com certo padrão, traduzíveis em termos matemáticos, tais como preços de mercadorias, contratos de empréstimos e análises de risco, são particularmente suscetíveis ao processo de automatização, desde que se tenha um conjunto relevante de dados que permita construir um modelo replicador das decisões anteriores.

O aprendizado de máquina busca imitar a racionalidade humana, a qual, por sua vez, está baseada na observação e organização intelectual do mundo, segundo padrões prévios, para predizer o futuro.

A automatização é um processo fundamentalmente estatístico-matemático: desvendam-se padrões nos dados e, a partir disso, a máquina "aprende" a reconhecê-los e a associá-los às "decisões corretas" respectivas. Cria-se, em suma, uma conexão lógica entre os dados de entrada e a decisão desejável para um futuro presumível. A máquina "aprende" a fazer essa imputação e, a partir de então, pode trabalhar de forma autônoma à vista da entrada de novos dados.

Durante o funcionamento do processo de decisão automatizada, as saídas podem ser otimizadas pelos programadores, mediante um processo ajuste fino do modelo por

meio dos dados de *feedback*, ou mesmo por meta-algoritmos, como os de *backpropagation*; assim, o modelo pode criar decisões automatizadas ainda melhores, num processo teoricamente infinito de autoaprendizagem e autocorreção coadjuvado ou não por seres humanos, chamado de programação dinâmica (*dynamic programming*).[38]

No processo de autoaprendizagem são muito relevantes também as exceções, ou seja, aquelas situações que parecem se encaixar em certo padrão, mas na verdade são diferentes. É justamente nesse ponto que o modelo pode produzir decisões enviesadas ou iníquas, por generalizar demais ou de menos o padrão que lhe foi ensinado. Em tese, quanto mais dados são apresentados ao modelo, mais chance de ele encontrar exceções que precisam de um tratamento diferente. Em contraste, o modelo pode ser pobre em dados de treinamento, não atinando para padrões que seriam perceptíveis num conjunto maior de dados. Os dados de treinamento são determinantes para a acurácia de qualquer modelo de aprendizado de máquina atual.

Os modelos podem assumir grande número de processos decisórios em empresas, governos e organizações em geral, liberando recursos humanos e materiais para a assunção das exceções, normalmente ligadas a processos não quantificáveis. Assim, os benefícios da automatização para as empresas e organizações em geral são, antes de tudo, econômicos. No caso dos governos, a automatização pode trazer maior eficiência em serviços e políticas públicas, além de ser também fator de aperfeiçoamento econômico e administrativo.

Para os consumidores e usuários de serviços públicos, as vantagens dos processos automatizados residem na criação de comodidades cada vez mais personalizadas e, consequentemente, mais adequadas às necessidades específicas de cada indivíduo ou família. Desde a indicação de filmes, livros e produtos em geral, conforme os hábitos de consumo demonstrados em operações anteriores, até o relacionamento com o Fisco ou o deferimento de benefícios sociais ou outras prestações do Poder Público, conforme o perfil do contribuinte ou do grupo familiar, os mecanismos automatizados criam uma sinergia profunda que proporciona altos graus de eficiência em grande escala nos mais diferentes processos produtivos.

Numa visão mais radical e mais otimista, o processo de automatização levará a humanidade a uma Sociedade 5.0, de grande abundância e conforto proporcionado

[38] KUBAT, Miroslav, *op. cit.*, p. 338.

pelas máquinas, mediante a integração total de vários sistemas inteligentes, com a fusão quase completa do mundo *off-line* com o mundo *on-line*.

Embora alguns processos de automatização já tragam benefícios palpáveis para consumidores e usuários de serviços públicos, a ideia de uma sociedade 5.0 é muito mais ampla e profunda, porque imagina toda a vida social imersa no crisol da Inteligência Artificial, sem que haja a necessidade de "acessar" nada, uma vez que a realidade física estará ela mesma envolta e hibridizada com os mecanismos inteligentes, a tal ponto que não será possível perceber qualquer diferença entre estar *on-line* ou *off-line*. Nesse sentido, observou-se:

> In summary, Society 5.0 will feature an iterative cycle in which data are gathered, analyzed, and then converted into meaningful information, which is then applied in the real world; moreover, this cycle operates at a society-wide level.[39]

Seria, assim, um passo à frente da Indústria 4.0, que diz respeito apenas aos processos produtivos da indústria e do comércio, mas não de outros aspectos da vida individual e coletiva. Na Sociedade 5.0 as pessoas individual e coletivamente seriam o centro do processo tecnológico de disseminação da inteligência sobre objetos e sobre todo o ambiente circundante, ou seja, a culminância da perfilização.

### 4.1. Ciclo Virtuoso da Inteligência Artificial

Pelo visto, as vantagens do processo de automatização resultam da disseminação de "inteligência" sobre objetos inanimados, de tal maneira a "cognificar"[40] o mundo, fazendo com que objetos, tais como eletrodomésticos, automóveis, móveis, e até a infraestrutura das cidades, colaborem ativamente para ganhos de produção das empresas, melhoria de serviços públicos e aumento da qualidade de vida das pessoas.

Andrew Ng, uma das maiores autoridades no tema do aprendizado de máquina, diz, por essa razão, que a Inteligência Artificial é a nova eletricidade[41]. O caráter transversal

---

[39] HITACHI-UTOKYO LABORATORY (H-UTOKYO LAB). *Society 5.0*: a people-centric super-smart society. Tokyo: Springer, 2018. Edição do Kindle, p.24.
Em resumo, o Sociedade 5.0 apresentará um ciclo iterativo no qual os dados são coletados, analisados e, em seguida, convertidos em informações significativas, que são então aplicadas no mundo real; além disso, este ciclo opera em um nível de toda a sociedade (tradução nossa).

[40] A expressão é de Kevin Kelly. Cf.:KELLY, Kevin. *Inevitável:* as 12 forças tecnológicas que mudarão nosso mundo. Rio de Janeio:Alta Books, 2019, Tradução de Cristina Yamagami, p. 31-65.

[41] ANDREW Ng: *Artificial Intelligence is the New Electricity*. Stanford: Stanford Graduate School of Business, 2 fev. 2017. 1 vídeo (1h 27 min). Publicado por Stanford Graduate School of Business. Disponível em: https://www.youtube.com/watch?v=21EiKfQYZXc. Acesso em 30 dez. 2020.

dessa tecnologia tende a repetir o que ocorreu com a eletricidade, na virada do século XIX para o XX, isto é, tende a exercer influência sobre todas as áreas da vida humana, assim como se deu com a eletricidade. Desde tarefas domésticas, passando pela agricultura, pela indústria, pelo comércio, pelo entretenimento, enfim, tudo será de algum modo afetado pelo processo de espalhamento da inteligência artificial.

Logicamente, a aposta de que a IA será amplamente incorporada em objetos decorre do fato de que há atrativos muito claros na adoção dos mecanismos inteligentes, de modo que se pode presumir razoavelmente que a implementação dessas tecnologias ocorrerá sem a necessidade de qualquer incentivo adicional.

Adriano Mussa fala de um "Ciclo Virtuoso da Inteligência Artificial" para aqueles que implantarem a IA em seus negócios:

> Em linhas gerais, o ciclo funciona da seguinte forma: se a organização desenvolver um produto ou serviço de qualidade satisfatória, ela conseguirá alguns usuários iniciais. Os usuários iniciais, ao utilizarem o produto ou serviço, gerarão dados que serão coletados e armazenados pela organização. Esses dados, se bem tratados por técnicas de Inteligência Artificial, principalmente *Machine Learning*, possibilitarão a melhoria do produto ou serviço. O produto ou serviço aperfeiçoado levará à aquisição de mais usuários. Mais usuários gerarão mais dados; mais dados levarão à melhoria do produto ou serviço e esse ciclo seguirá continuamente.[42]

Ao contrário do que se pode pensar a partir do imaginário criado especialmente pela indústria cinematográfica, a IA não é uma poderosa e maligna ferramenta capaz até de se rebelar contra os seus criadores. A maioria das aplicações de IA hoje são estreitas (*narrow*), isto é, são direcionadas a finalidades bem específicas e limitadas. Não existe ainda, e provavelmente nunca existirá, uma Inteligência Artificial Geral (AGI, na sigla em inglês para *Artificial General Intelligence*), unificada e com aptidão para quaisquer propósitos.

As aplicações de IA atualmente estabelecem uma relação simples do tipo: A → B, em que "A" representa os dados de entrada (*Input*), "→" indica uma relação de implicação condicional, e "B", os dados de saída (*Output*). Os dados de saída resultam, portanto, do tratamento dos dados de entrada pelo modelo. O modelo cria uma conexão

[42] MUSSA, Adriano. *Inteligência Artificial - Mitos e Verdades:* as reais oportunidades de criação de valor nos negócios e os impactos no futuro do trabalho. São Paulo: Saint Paul, 2020. Edição Kindle, p.105.

estatístico-matemática entre o *Input* e o *Output*, que emula a conexão semântica estabelecida pela inteligência humana, só que numa escala, precisão e velocidade muito maiores e, em compensação, infinitamente mais estreita e descontextualizada também.

Para que o modelo funcione adequadamente, os programadores "ensinam", com dados de treinamento, qual a conexão "correta" a ser estabelecida. Em seguida, o próprio modelo "aprende" o padrão da conexão e passa replicá-la. Quando já na fase de aplicação, os usuários também acabam ajudando o modelo a melhorar, por meio de suas interações, que nada mais são do que rotulações para o modelo. Por exemplo, quando o usuário dá um *like* num produto, ele rotula aquele produto — e todos os que a ele estão ligados — como um *output* desejável para si, caso posteriormente ele faça uma pesquisa de compra. O mesmo ocorre também quando o usuário, por exemplo, marca um *e-mail* como *spam*: o modelo incorpora esse rótulo como negativo, posteriormente qualificando *e-mails* com o mesmo padrão como *spams*.

Observa-se, assim, que à medida que o modelo entra em contato com os usuários e suas rotulações, salvo interferências propositais do programador, ele vai se amoldando às preferências e repulsões que estes manifestam, potencializando os comportamentos tidos como normais. Isso vale para o indivíduo e para o grupo. Há um processo de *perfilização* constante, individual e grupal.

Vê-se também que o modelo carece de muitos dados para ter acurácia e robustez, pois ele só prediz algo com que já tenha tido contato anterior. Por isso Inteligência Artificial e *Big Data* (grandes conjuntos de dados) andam juntos.

Se os dados de entrada e os dados de saída são conhecidos do programador, a máquina será programada para aprender de modo supervisionado (*supervised learning*-*SL*). Neste caso, o programador, na fase de treinamento, alimenta a máquina com os dados de entrada e também com os dados de saída, de modo a estabelecer o vínculo estatístico-matemático.

Aqui, porém, há uma subdivisão importante: a) o SL pode se dar por meio de *Statistical Machine Learning*, isto é, uma forma em que o algoritmo contém previamente fórmulas para calcular probabilidades e com base nelas gerar o *output*; ou b) por meio de *Deep Learning*-DL, em que o programador não cria totalmente as fórmulas de cálculo, mas apenas esboça um modelo em camadas aparentes de uma Rede Neural Artificial e depois alimenta essa rede com vastos volumes de dados de entrada,

associando-os aos dados de saída "corretos" (rotulados), deixando que o próprio algoritmo, por tentativas e erros, encontre os pesos adequados para cada variável de modo tal que essas associações se encaixem de forma correta. Essas tentativas e erros, quando encerradas, geram camadas profundas e ocultas na Rede Neural Artificial, que o próprio modelo cria e que sequer é do conhecimento do próprio programador.

Grosso modo, no *Statistical Machine Learning* o programador ensina a pergunta, a resposta certa e a forma de chegar a ela; no *Deep Learning*, o programador mostra a pergunta e a resposta certa, mas não diz como chegar a ela, cabendo ao modelo criar esse caminho. E o caminho criado pelo modelo pode ser extremamente eficaz — os modelos de DL têm atingido 95% de acurácia de predição —, embora ele estabeleça conexões que, para nós, humanos, não fazem sentido algum, em termos de relação de causa e efeito.

Adriano Mussa, após explicar como funciona um modelo preditivo baseado em *Statistical Machine Learning*, no qual o programador escolhe as variáveis relevantes (área do imóvel, localização, tempo de construção, etc.) e ensina a máquina qual peso dar a cada uma delas, estima como seria o processo de *Deep Learning* na mesma situação:

> Na prática, alimentamos os algoritmos de DL com a camada de *Input* – A e com os dados de resultado, *Output* – B, e são os algoritmos que buscam todas as combinações possíveis de variáveis, testando a criação de inúmeras camadas e neurônios para buscar, matematicamente, a melhor combinação e pesos, que expliquem os preços dos imóveis com a maior acurácia possível, com base em suas características. Em outras palavras, os algoritmos buscam aumentar a acurácia do modelo utilizando as inúmeras combinações de variáveis, criando neurônios e utilizando pesos que otimizem a sua performance, independentemente de elas fazerem ou não sentido para nós, seres humanos.[43]

Os modelos de DL, portanto, buscam extrair diretamente dos dados de entrada a combinação mais eficiente para chegar aos dados de saída, que por sua vez são rotulados conforme o objetivo do programador. Na concepção desse caminho lógico-matemático, o modelo acaba organizando camadas escondidas (*hidden layers*) de "neurônios artificiais" que atribuem pesos às diferentes combinações, preferindo aquelas cuja soma mais se aproxime do resultado de saída desejado. Em outras

[43] MUSSA, *op.cit*, p.86

palavras, as camadas ocultas trabalham otimizando funções matemáticas que sejam capazes de transformar os dados de entrada na resposta informada pelo desenvolvedor do modelo na fase de treinamento.

Mesmo o programador original do modelo não saberá completamente como a Rede Neural Artificial chegou àquela combinação, tal a quantidade de cálculos e de arranjos testados pela máquina. Essas camadas intermediárias, assim, formam uma verdadeira "caixa preta" que oculta a maior parte do processo decisório automático. Assim, se por um lado elas tornam o modelo extremamente robusto para obter as respostas desejadas, por outro elas tornam opaco o processo decisório. Nas camadas escondidas dos modelos está a virtude e o vício do DL.

Quanto mais complexo for o problema a ser resolvido pela Rede Neural Artificial, mais camadas ocultas de combinações e pesos podem ser criadas pelo modelo para aumentar a acurácia. Em compensação, mais obscuros se tornam os critérios de cálculo, ou seja, mais densa a caixa-preta.

Nos modelos de *Statistical Machine Learning*, em que o programador escolhe as variáveis que o modelo deve levar em conta, o que ocorre é que o modelo ficará limitado à visão humana de causalidade, que apenas leva em conta os vínculos fortes entre entrada e saída. Se o mesmo problema de negócio for apresentado a um modelo de *Deep Learning*, ele encontrará correlações que não ocorreriam à mente humana, por aparentemente não terem vínculo de causalidade com o resultado.

Um exemplo impressionante, lembrado por Kai Fu Lee,[44] é aquele do modelo criado por uma empresa chinesa para decidir automaticamente sobre a concessão de pequenos empréstimos com base em dados do celular do interessado. Uma Rede Neural Artificial, devidamente treinada com milhões de dados históricos de pequenos empréstimos, descobriu que o nível de bateria médio do celular ao longo do dia, a data de nascimento ou a velocidade de digitação do pedido de empréstimo pelo celular do interessado, tinham correlação com a classificação dele como bom ou mau pagador (os bons pagadores geralmente tinham a bateria do celular mais carregada, por exemplo).

Como isso se dá? Após ter acesso a um vasto conjunto de dados de bons e maus pagadores, o modelo de DL, na fase de treinamento, é apresentado a esses dados, tendo o programador previamente informado (rotulado ou etiquetado) os dados de saída

[44] *Op. cit.*, p.139.

(bons ou maus pagadores). A rede neural então, ante os dados de entrada (os mais diversos dados extraídos dos celulares, tais como tempo de uso diário, nível médio de bateria, sites que navega comumente, etc.), não procura "entender" o porquê de aquele ser um bom ou mau pagador — como faria um ser humano, que pensa em termos de causa e efeito — mas sim criar uma função matemática que ligue de maneira ótima os dados de entrada dos bons pagadores aos dados de saída respectivos, rotulados pelo programador. E o mesmo processo é feito com o telefone de muitos maus pagadores. Ao final desse treinamento, o modelo terá encontrado padrões nos bons e nos maus pagadores, levando em conta elementos que, para um ser humano, seriam completamente irrelevantes, tal como a carga média da bateria do celular, referida acima. Por isso que é apenas metafórica a comparação dos processos decisórios automatizados com a inteligência humana. O que a máquina faz é algo muito diferente do pensamento humano, embora chegue a resultados parecidos e eventualmente com maior acurácia. Edsger Dijkstra, a esse propósito, afirmou: "A questão de saber se um computador pode pensar não é mais interessante que a questão de saber se um submarino pode nadar".[45]

Uma descoberta como essa (que a carga média da bateria do celular influencia na probabilidade de que o contrato seja cumprido) pode representar um *insight* comercial que dá ao operador do modelo uma vantagem relevante, em relação aos concorrentes, sobretudo quando se pensa em grande escala. Mas pode também representar, a depender de qual seja o elemento diferenciador revelado pelos dados, uma fonte involuntária de discriminação de pessoas, grupos ou ideias.

A grande revolução do aprendizado de máquina ocorreu justamente com o *Deep Learning-DL*, e a maioria das atuais aplicações daquilo que se chama de "Inteligência Artificial" nada mais é do que DL. Durante muito tempo, entre os anos 1970 até os anos 1990, prevaleciam nas aplicações de IA os chamados Sistemas Especialistas, que eram mecanismos inteligentes baseados em regras.[46] O programador avaliava o problema do mundo real e tentava modelá-lo por meio de regras, que depois seriam aplicadas por um motor de inferência a novos dados de entrada. A deficiência dessa abordagem é que, por vezes, muito difícil e laborioso criar as regras específicas para cada situação, e mais ainda para as exceções que se intersectam com a regra em alguns pontos. Um programa de reconhecimento da imagem de um gato, por exemplo, dependeria de

[45] NORVIG, Peter Peter; NORVIG, Peter. *Inteligência Artificial*. 3. ed. Rio de Janeiro: Elsevier, 2013. Tradução de Regina Célia Simille, p. 932.
[46] SEJNOWSKI, Terrence J. *A revolução do aprendizado profundo*. Rio de Janeiro: Alta Books, 2019. Traduzido por Carolina Gaio, p. 35-37.

escrever em código minuciosamente o que "é" um gato e centenas, talvez milhares de regras sobre o que não é um gato, mas sim uma onça, um puma, ou outro felino. Ora, não é assim que funciona a mente humana, a mais avançada forma de inteligência que conhecemos. Simplesmente sabemos muitas coisas que não podemos verbalizar em termos estritos. Aquilo que chamamos de "senso comum", por exemplo, é constituído de um vasto conhecimento sobre leis físicas e sociais que não podem ser codificadas, tanto mais porque não sabemos exatamente quais são elas, embora as apliquemos no dia a dia.

Nos anos 1980, Douglas Lenat, por meio de um projeto chamado CYC,[47] tentou codificar o "senso comum" de um ser humano. O programa chegou a acumular mais de 1 milhão de regras, sem, no entanto, conseguir abranger algo que um humano comum aprende ainda na infância.

De fato, há muitas coisas que um ser humano sabe, mas não consegue expressar em palavras, e muito menos de forma quantitativa. Santo Agostinho escreveu que sabia o que era o tempo, mas bastava alguém pedir-lhe para dizer o que era, que não sabia mais.[48] Esse célebre pensamento ilustra a maneira como funciona a inteligência humana. Muita coisa é aprendida simplesmente por exemplos e repetições de padrões, sem a necessidade de que a mente analise todos os aspectos e relações do objeto conhecido.

O *Deep Learning* parte de uma abordagem diferente, mais próxima do funcionamento do cérebro humano. As dificuldades enfrentadas pela abordagem baseada em regras e heurísticas, estimulou os pesquisadores em IA a buscar saídas que fossem mais factíveis. Segundo Sejnowski,[49] quatro coisas indicavam que era ruim trilhar pelo caminho da criação de regras para desenvolver um sistema inteligente, porque: a) o cérebro humano trabalha primeiro com reconhecimento de padrões, as regras surgem depois; b) é preciso uma prática repetitiva para que o cérebro domine atividades mais complexas; c) o cérebro não se orienta por regras no dia a dia, embora possa trabalhar com elas em um nível mais profundo do pensamento; e, finalmente, d) nossos cérebros têm bilhões de neurônios que se intercomunicam, o que sugere que ele trabalha com processamento paralelo dos dados de entrada e não com processamento linear (arquitetura de Von Neumman).

---

[47] https://www.cyc.com/the-cyc-platform. Acesso em 20 dez 2020

[48] "O que é, por conseguinte, o tempo? Se ninguém mo perguntar, eu sei; se o quiser explicar a quem me fizer a pergunta, já não sei". (AGOSTINHO, Santo. *Confissões*. São Paulo: Companhia das Letras, 2017. Tradução de Lorenzo Mammì. Edição do Kindle, p. 237.)

[49] SEJNOWSKI, *op. cit.*, p. 41-42.

Foi essa abordagem que permitiu a maior parte dos progressos efetivos na área de IA aplicada a negócios. Os modelos de *deep learning* muitas vezes atingem 95% de acurácia, em certas tarefas, o que era impensável antes do uso dessa técnica. E esse nível de acurácia, como explica Adriano Mussa, não é raro em *Deep Learning*:

> Esse percentual elevado de acurácia dos algoritmos de *Deep Learning* não é exceção. Ele tem sido observado em uma infinidade de aplicações de setores e contextos diferentes, mostrando sua forte robustez.[50]

Assim, os modelos de *Deep Learning* asseguram aa principais vantagens do uso de IA em negócios ou qualquer aplicação que dependa de julgamentos: rapidez, economia e acurácia.

## 5. Os riscos das decisões automatizadas

Como demonstrado no item anterior, a maior parte das decisões automatizadas que são atualmente colocadas em prática resultam de modelos de *Deep Learning* em Redes Neurais Artificiais. Convém, assim, ter presente que os riscos que foram levados em conta pelo próprio legislador estão associados a esse método de tratamento de dados.

O primeiro e mais conhecido risco das decisões automatizadas decorrentes de DL é o da opacidade. Pelo próprio volume de cálculos e pela quantidade de dados necessária para a concepção de um modelo de DL, não é acessível sequer para os desenvolvedores o processo exato por meio do qual o modelo chegou a esta ou aquela predição ou mesmo decisão, e isso naturalmente pode levantar desconfianças e suposições em relação à higidez do modelo, eventualmente exigindo uma coadjuvação humana para que ele possa ser colocado em prática. Terrence Sejnowski[51] exemplifica bem o problema com o caso dos diagnósticos médicos:

> Embora possam dar resposta correta para um problema, atualmente não sabemos como as redes neurais chegam a ela. Por exemplo, suponha que uma paciente chegue a um pronto-socorro com uma dor aguda no peito. Trata-se de um infarto agudo do miocárdio, o que precisa de intervenção imediata, ou simplesmente um caso grave de indigestão? Uma rede treinada para diagnosticar pode ser mais precisa do que o médico responsável pela triagem; mas, sem uma explicação sobre como

[50] MUSSA, *op. cit.*, p. 91.
[51] *Op. cit.*, p. 134.

> a rede tomou a decisão, a relutância em confiar nela seria plausível. Os médicos também são treinados para acompanhar o que equivale a algoritmos, séries de testes e pontos de decisão que os orientam em casos de rotina. O problema é que há casos raros, que estão fora do escopo de seus 'algoritmos', enquanto uma rede neural treinada com muito mais casos, mais do que a média dos médicos verá em toda uma vida, pode muito bem dirimir sobre esses casos raros. Mas você confiaria mais no diagnóstico estatisticamente mais sólido de uma rede neural, sem explicação de como foi feito, do que no de um médico com um diagnóstico plausível?

A opacidade também pode decorrer de fatores comerciais. O desenvolvedor do modelo pode até saber explicar como se chegou a certa decisão, mas a exposição desse caminho poderia revelar o seu "segredo comercial ou industrial", que na verdade é a sua fonte de ganhos com o modelo.

A LGPD cuida do ponto, na esteira do GDPR, estabelecendo no art. 20, §1º, um direito à explicação em caso de decisão automatizada, como primeira linha contra a opacidade, mas respeitado o segredo comercial e industrial — e é difícil, na prática, conciliar essas duas coisas.

Se a explicação não for dada pelo controlador ao titular dos dados, sob o argumento da existência de segredo comercial ou industrial, então a Autoridade Nacional de Proteção de Dados - ANPD pode ser acionada para fazer uma verificação sobre possíveis vieses discriminatórios (LGPD, art. 20, §3º). No capítulo seguinte avalia-se melhor essa questão, mas de logo chama a atenção a estreiteza da norma, que deixa duas importantes questões em aberto: a) E se a explicação for negada com outro fundamento, que não o segredo comercial ou industrial? (Por exemplo, a alegação de que o próprio controlador não sabe exatamente como o modelo funciona); b) E se não houver discriminação, mas sim outro tipo de violação a direitos individuais?

Os tecnólogos têm tentado criar modelos que sejam capazes de ser autoexplicativos, a chamada Inteligência Artificial Explicável (XAI, na sigla em inglês para *Explanable Artificial Intelligence*). Mas aqui a questão esbarra na autorreferência. É que o próprio cérebro humano é também uma caixa-preta. De fato, a objeção de que um modelo opera com uma caixa-preta pode ser aplicada também ao cérebro humano. Não há até aqui conhecimento objetivo e minucioso sobre os processos decisórios humanos, exceto que se sabe que há muito mais viés e irracionalidade do que se imaginava. Eventuais explicações humanas, muitas vezes, são meramente retóricas. Modelos de XAI podem

recair no mesmo impasse. O risco de opacidade, portanto, permaneceria sendo um problema insolúvel.

Outro ponto, ainda sobre a opacidade, é que a concepção de uma decisão automatizada envolve o tratamento de muitos dados e a revelação do seu processo para um titular poderia ensejar a violação da intimidade de outros titulares, cujos dados também foram levados em conta na decisão, para efeito de comparação, e a quem pode não interessar a divulgação do processo decisório.

Um segundo risco criado pelas Redes Neurais Artificiais de *Deep Learning* é que elas dependem de um grande volume de dados para funcionarem bem, o que gera uma corrida por dados pessoais. Com efeito, a acurácia das decisões automatizadas criadas por Redes Neurais Artificiais depende fundamentalmente de um vasto conjunto de dados (*Big Data*), especialmente na fase de treinamento e validação, e também para evoluir na fase de aplicação. Essa necessidade faz com que aumentem os riscos ligados à privacidade, porque os desenvolvedores buscarão sempre ter acesso ao máximo de dados pessoais para criarem, validarem e aplicarem modelos preditivos e decisórios de alto desempenho. Com o advento da Internet 5G e a implantação da Internet das Coisas, estima-se que a coleta de dados crescerá exponencialmente, já que atividades triviais do dia a dia e até da intimidade doméstica, como abrir uma geladeira, fechar uma porta, ou ligar uma lâmpada, poderão ser incorporadas à internet e gerarão dados pessoais suscetíveis de serem usados em modelos preditivos. Presumivelmente, isso multiplicará muitas vezes os riscos à privacidade.

Um terceiro risco, ligado ao anterior, é que, além de precisarem de um grande volume de dados, as Redes Neurais expressam apenas o conhecimento que se pode extrair desses dados, não mais que isso. Logo, se há no conjunto de dados de treinamento um viés, proposital ou não, esse viés se replicará indefinidamente nas decisões.

O caso mais conhecido sobre isso ocorreu em Los Angeles (EUA),[52] e dizia respeito ao reconhecimento facial em locais públicos. Descobriu-se que um modelo de reconhecimento facial da polícia cometia mais erros em relação a negros do que em relação a brancos, porque, enquanto os "procurados", na fase de aplicação do modelo, eram na maior parte pessoas negras, na fase de treinamento o modelo fora apresentado

[52] GARVIE, Clare; FRANKLE, Jonathan. Facial-Recognition Software Might Have a Racial Bias Problem: Depending on how algorithms are trained, they could be significantly more accurate when identifying white faces than African American ones. *In*: THE ATLANTIC. *The Atlantic*, 6 abr. 2016. Disponível em: https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/. Acesso em: 22 dez. 2020.

a um número maior de faces brancas, tornando-se naturalmente melhor em reconhecer estas do que outras.

Tal situação pode se repetir em muitas outras áreas. A escolha dos dados de treinamento não é um ato neutro; muito menos o é a rotulação dos dados de saída, feita pelos programadores. Aqui a escolha envolve aspectos ideológicos, muitas vezes inconscientemente. Como explica Terrence Sejnowski:

> Todas as redes neurais que classificam entradas são tendenciosas. Em primeiro lugar, a escolha das categorias de classificação incorpora um viés que reflete o preconceito humano na forma como esmiuçamos o mundo. Por exemplo, seria útil treinar uma rede para detectar ervas daninhas em gramados. Mas como identificá-la? A erva daninha de um homem pode ser a flor silvestre de outro. A classificação é um problema muito mais amplo, que reflete vieses culturais. Essas ambiguidades precisam integrar os conjuntos de dados usados para treinar a rede.[53]

Pior ainda, com a aplicação do modelo em massa, produzem-se *loopings* que reforçam o viés original. Cathy O´Neal[54] exemplifica esse fenômeno com os modelos de otimização do policiamento ostensivo. Como esses modelos usam dados relativos a pequenas infrações, tais como perturbação da ordem, posse de pequena quantidade de droga e vadiagem, os policiais acabam sendo enviados para patrulhar regiões pobres, onde normalmente acontecem essas infrações. Com o aumento do patrulhamento, aumentam também as prisões por essas pequenas contravenções, o que induz a realimentação e o reforço por *feedback* ao modelo para aumentar o patrulhamento nesses locais.

Ainda no campo dos vieses e seu ciclo vicioso de reforço, observa Caathy O'Neal também que, embora a cor da pele e a condição social não sejam incluídas no modelo como parâmetros para a inferência, o fato é que os dados escolhidos (sobre pequenos delitos) para esse tipo de policiamento acabam funcionando como *proxies* para a raça e a pobreza, já que apenas negros e hispânicos da periferia são presos, segundo a autora, por esse tipo de crime nos Estados Unidos. Um indivíduo branco que pratique ações semelhantes num campus universitário dificilmente deparará com uma patrulha policial.

---

53 SEJNOWSKI, *op. cit.*, p. 135.
54 O'NEIL, Cathy. *Weapons of math destruction:* how big data increases inequality and threatens democracy. New York:Crown Publishers, 2016. Ebook.

Há um quarto risco, não menos grave, no uso de mecanismos inteligentes para formulação de decisões automatizadas. É que a grandeza que é escolhida para ser otimizada pode subdimensionar outras questões relevantes. Assim, se o modelo visa ao lucro — e a maioria visa a isso, naturalmente — a função de lucro deve ser otimizada pelo modelo, no que não há nada de ilegal ou imoral. Acontece que essa otimização, quando feita em termos matemáticos, é implacável. O modelo não se deterá diante de nenhuma circunstância, a não ser que programado para isso, para aumentar os lucros. Como mecanismo de Inteligência Artificial Fraca ou Estreita, o modelo não é capaz de contextualizar as decisões para além dos dados que lhes foram apresentados, de modo que se o lucro é o que deve ser maximizado, ele fará isso *per fas et per nefas*.

Eventualmente, essa "objetividade" inexorável pode produzir danos imensos, sobretudo quando aplicada em grande escala. E aqui se chega a um risco transversal de todos os modelos matemáticos para produzir decisões automatizadas: a escala. É a escala que gera os maiores danos.

Como explica Cathy O´Neal[55], é a escala transforma o que seria um pequeno incômodo em algo com a força de um tsunami. Ao estabelecer um ciclo de decisão em um número imenso de casos idênticos, o modelo em larga escala acaba influenciando o ambiente de duas formas: a) ele reforça em massa um padrão, inferido de situações anteriores (que podem ser injustas); b) ele induz o comportamento futuro das pessoas, que tentarão se ajustar ao modelo.

A escala das decisões automatizadas gera um problema adicional. A regulamentação ou qualquer ação legal que vise a solucionar um problema gerado por algoritmos pode não conseguir atingir o seu objetivo, justamente por não ser escalável. Ou seja, enquanto decisões automatizadas são tomadas *on-line* e em massa, as soluções legislativas tendem a depender de uma análise artesanal, caso a caso. A brutal diferença de velocidade e de volume pode levar a norma à completa ineficácia prática. Assim, as regulamentações precisarão contar com mecanismos de implementação escaláveis. Nesse sentido, observam Kearns & Roth:[56]

> Regulations and laws certainly have a crucial role to play—as we have emphasized throughout, the specification of what we want algorithms to do and not do for us should remain firmly in the

[55] O'NEIL, *op. cit.*, p. 48.
[56] KEARNS; ROTH, *op. cit.,* p.192.

> human and societal arenas. But purely legal and regulatory approaches have a major problem: they don't scale. Any system that ultimately relies solely or primarily on human attention and oversight cannot possibly keep up with the volume and velocity of algorithmic decision-making. The result is that approaches that rely only on human oversight either entail largely giving up on algorithmic decision-making or will necessarily be outmatched by the scale of the problem and hence be insufficient. So while laws and regulations are important, we have argued in this book that the solution to the problems introduced by algorithmic decision-making should itself be in large part algorithmic.[57]

Em resumo, os principais riscos dos mecanismos de decisão automatizada são: a) opacidade; b) necessidade de grande volume de dados, com riscos à privacidade; c) viés; d) subdimensionamento de grandezas diversas daquela buscada pelo controlador dos dados; e) escala.

## 6. Conclusão

O presente trabalho buscou investigar o que são as decisões automatizadas, quais são os riscos e benefícios que elas trazem, bem como analisar de que maneira o recente marco legal brasileiro sobre o tema, a Lei Geral de Proteção de Dados, trata essa inovação tecnológica. A metodologia adotada para desenvolver o problema de pesquisa gerou algumas conclusões.

Verificou-se que existe a necessidade doutrinária de definir o que é e de como se forma uma decisão automatizada, à luz da LGPD. Intentando atingir esse objetivo, esboçou-se a seguinte definição: decisão automatizada é todo julgamento feito exclusivamente por máquina, com base em predição decorrente de tratamento automatizado de dados pessoais de entrada, segundo um modelo ou algoritmo condicionado por dados de treinamento, que afete imediatamente interesse juridicamente tutelado de pessoa natural, excetuados aqueles que tenham fins particulares e não econômicos, jornalísticos ou científicos.

---

[57] Regulamentos e leis certamente têm um papel crucial a desempenhar - como enfatizamos ao longo do texto, a especificação do que desejamos que os algoritmos façam e não façam por nós deve permanecer firmemente nas arenas humana e social. Mas as abordagens puramente legais e regulatórias têm um grande problema: elas não escalam. Qualquer sistema que, em última análise, dependa única ou principalmente da atenção e supervisão humanas, não pode acompanhar o volume e a velocidade da tomada de decisão algorítmica. O resultado é que as abordagens que dependem apenas da supervisão humana implicam em desistir amplamente da tomada de decisão algorítmica ou serão necessariamente superadas pela escala do problema e, portanto, insuficientes. Portanto, embora as leis e os regulamentos sejam importantes, argumentamos neste livro que a solução para os problemas introduzidos pela tomada de decisão algorítmica deve ser em grande parte algorítmica (tradução nossa).

A investigação permitiu demonstrar a relação que pode ser estabelecida entre perfilização e decisões automatizadas, evidenciando como a a LGPD trata essa questão. Como visto, as decisões automatizadas podem ser realizadas com ou sem definição de perfis, da mesma forma como a definição de perfis pode ocorrer sem que dela decorra uma decisão automatizada.

Por outro lado, a definição de perfis e as decisões automatizadas não constituem necessariamente atividades separadas, a decisão automatizada pode ou não depender de perfilização, de acordo com o interesse do desenvolvedor na concepção do modelo.

Todavia, a LGPD atenua essas distinções, uma vez que, segundo a sua redação, deve-se admitir que a perfilização, mesmo não sendo seguida de uma decisão automatizada, mas sim de uma decisão humana assistida por máquina, seja considerada como uma decisão automatizada por equiparação, tendo em vista que seu artigo 20 afirma expressamente que estão incluídas entre as decisões automatizadas aquelas "destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade".

Foram analisados também benefícios e riscos dessa forma decisória. Demonstrou-se que um dos principais benefícios que faz com que as empresas e governos busquem por processos decisórios automatizados é o aumento da capacidade e da velocidade de resposta a demandas repetitivas e a redução de custos, quando máquinas tentam imitar a racionalidade humana, tomando decisões em massa, diante de um conjunto relevante de dados que permitem construir um modelo replicador das decisões.

Na outra ponta do processo decisório, restou evidente que também é possível encontrar benefícios, na medida que os consumidores e usuários de serviços públicos encontram respostas cada vez mais personalizadas e, consequentemente, mais adequadas às necessidades específicas de cada indivíduo ou família.

Entre os principais riscos das decisões automatizadas, cinco foram identificados: a) opacidade; b) necessidade de grande volume de dados, com riscos à privacidade; c) viés; d) subdimensionamento de grandezas diversas daquela buscada pelo controlador dos dados; e) escala.

O risco da opacidade decorre de modelos de *Deep Learning* e consiste na ideia de que o processo exato pelo qual levou a uma ou outra decisão carrega tantos dados e exige

inúmeros cálculos que não é acessível nem mesmo para seus desenvolvedores, levantando dúvidas e desconfianças em relação à higidez do processo de decisão automatizada. Em outros casos, a opacidade pode decorrer de questões estratégicas, uma vez que, mesmo tendo um caminho conhecido pelos desenvolvedores, divulgar o processo decisório pode não ser interessante por revelar segredos comerciais ou industriais.

A pesquisa levou a concluir também que a LGPD tratou desse risco e garantiu o direito à explicação em casos de decisões automatizadas, tentando equilibrar a defesa contra a opacidade e ao mesmo tempo garantir a preservação ao segredo comercial e industrial.

O segundo risco identificado consiste no fato de que as decisões automatizadas são dependentes de um grande volume de dados para funcionarem corretamente, fato que gera uma corrida desenfreada por dados e isso, consequentemente, põe em risco a privacidade das pessoas.

O terceiro risco encontrado consiste nas decisões automatizadas se basearem apenas no que se pode extrair dos dados e em nada mais. Assim, caso exista no conjunto de dados de treinamento um viés, proposital ou não, esse viés se replicará indefinidamente nas decisões.

O quarto e o quinto riscos encontrados estão, de certa forma, conectados. O quarto risco consiste no uso de mecanismos inteligentes para a formulação de decisões inteligentes, uma vez que a grandeza que é escolhida para ser otimizada pode subdimensionar outras questões relevantes, direcionando a decisão mais para uma posição ou outra de acordo com os interesses envolvidos e quando aplicadas em escalas grandes podem produzir danos enormes. E esse problema da escala foi o quinto risco encontrado, tendo em vista a escala transforma o que seria um simples problema de uma decisão automatizada em um problema gigantesco, reforçando em massa um padrão, induzindo comportamentos futuros e a correção desse grande volume de decisões inadequadas pode ser totalmente ineficaz por precisar de análises humanas, bem mais lentas.

Desse modo, percebe-se que as decisões automatizadas já podem ser consideradas um novo paradigma, trazendo muitos benefícios e riscos, alguns já enfrentados pelo marco legal brasileiro que trata sobre o tema, a Lei Geral de Proteção de Dados, e outros que ainda vão precisar ser enfrentados.

## Referências


ABREU, Jacqueline de Souza. Tratado de Proteção deTratamento de Dados Pessoais para Segurança Pública: contornos do regime jurídico pós-LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. Edição do Kindle.

AGGARWAL, Charu C. *Neural Networks and Deep Learning*: a textbook. New York: Springe, 2018.

AGOSTINHO, Santo. *Confissões*. São Paulo: Companhia das Letras, 2017. Tradução de Lorenzo Mammì. Edição do Kindle.

AGRAWAL, A; GANS, J.; GOLDFARB. *Máquinas preditivas:* a simples economia da Inteligência Artificial. Rio de Janeiro: Alta Books, 2018. Tradução de Wendy Campos.

AMBROSE, Meg Leta; AMBROSE, Ben M.. When robots lie a comparison of auto-defamation law. *2014 Ieee International Workshop On Advanced Robotics And Its Social Impacts*, [S.L.], p. 56-61, set. 2014. IEEE. <http://dx.doi.org/10.1109/arso.2014.7020980>.

ANDREW Ng: Artificial Intelligence is the New Electricity. Stanford: Stanford Graduate School of Business, 2 fev. 2017. 1 vídeo (1h 27 min). Publicado por Stanford Graduate School of Business. Disponível em: <https://www.youtube.com/watch?v=21EiKfQYZXc>. Acesso em 30 dez. 2020.

ANDRADE, Manuel A. Domingues. *Teoria geral da relação jurídica*. Coimbra: Almedina, 1992. v. 1.

BREEN, Jason. YouTube or YouLose? Can YouTube Survive a Copyright Infringement Lawsuit. *Bepress Legal Series.Working Paper 1950*, Los Angeles, p. 1-37, 18 jan. 2007. Disponível em: <https://law.bepress.com/cgi/viewcontent.cgi?article=9209&context=expresso>. Acesso em: 10 dez. 2020.

BINNS, Reuben; GALLO, Valeria. Automated Decision Making: the role of meaningful human reviews. *In*: ICO. *Information Commissioner's Office*. 12 abr. 2019. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/ai-blog-automated-decision-making-the-role-of-meaningful-human-reviews/>. Acesso em: 11 jan. 2021.

CHACE, Calum. *Surviving AI*: the promise and peril of artificial intelligence. Oxford: Three Cs, 2015. Kindle Edition.

CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. *Journal Of Law, Information And Science*, v. 2, n. 4, jan. 1993. Disponível em: <http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/JlLawInfoSci/1993/26.html?query=>. Acesso em: 10 dez. 2020.

CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, Washington, D.c., v. 85, n. 6, p. 1249-1313, ago. 2008. Disponível em: <https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview>. Acesso em: 17 jul. 2020.

CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: toward a framework to redress predictive privacy harms. *Boston College Law Review*, Boston, v. 55, n. 1, p. 93-128, 29 jan. 2014. Disponível em: <https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>. Acesso em: 17 jul. 2020.

ERTEL, Wolfgang. Introduction. *Undergraduate Topics In Computer Science*, p. 1-21, 2017. Springer International Publishing. <http://dx.doi.org/10.1007/978-3-319-58487-4_1>.

GARVIE, Clare; FRANKLE, Jonathan. Facial-Recognition Software Might Have a Racial Bias Problem: Depending on how algorithms are trained, they could be significantly more accurate when identifying white faces than African American one. *In*: THE ATLANTIC. *The Atlantic*, 6 abr. 2016. Disponível em: <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/>. Acesso em: 22 dez. 2020.

HANNÁK, Anikó; WAGNER, Claudia; GARCIA, David; MISLOVE, Alan; STROHMAIER, Markus; WILSON, Christo. Bias in Online Freelance Marketplaces: Evidence from TaskRabbit and Fiverr. *In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, New York, p. 1914–1933, Fev. 2017.

HILDEBRANDT, Mireille. Privacy as Protection of the Incomputable Self: from agnostic to agonistic machine learning. *Theoretical Inquiries In Law*, Tel Aviv, v. 20, n. 1, p. 83-121, jan. 2019. Disponível em: <https://www7.tau.ac.il/ojs/index.php/til/article/view/1622/1723>. Acesso em: 17 jul. 2020.

HITACHI-UTOKYO LABORATORY (H-UTOKYO LAB). *Society 5.0*: a people-centric super-smart society. Tokyo: Springer, 2018. Edição do Kindle.

ICO. What does the UK GDPR say about automated decision-making and profiling?. *In*: ICO. *Information Commissioner's Office*. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/>. Acesso em: 11 jan. 2021.

JUSTICE AND CONSUMERS (Europea Union). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. *In*: JUSTICE AND CONSUMERS (Europea Union). *European Commission*. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>. Acesso em: 11 jan. 2021.

KEARNS, Michael; ROTH, Aaron. *The Ethical Algorithm*: the science of socially aware algorithm design. New York: Oxford University Press, 2019. Edição Kindle.

KELLY, Kevin. *Inevitável*: as 12 forças tecnológicas que mudarão nosso mundo. Rio de Janeio:Alta Books, 2019, Tradução de Cristina Yamagami.

KUBAT, Miroslav. *An Introduction to Machine Learning*. 2. ed. Coral Gables: Springer, 2017.

LEE, Tian-Shyug; CHEN, I-Fei. A two-stage hybrid credit scoring model using artificial neural networks and multivariate adaptive regression splines. *Expert Systems with Applications*, [*s. l.*], v. 28, n. 4, p. 743-752, mai. 2005.

LÉVY, Pierre. *As tecnologias da inteligência*: o futuro do pensamento na era da informática. São Paulo: Editora 34, 1993. Tradução de Carlos Irineu da Costa.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY (ed.). *MIT Technology Review*. Self-driving cars. Topics. Disponível em: <https://www.technologyreview.com/topic/smart-cities/self-driving-cars/>. Acesso em: 02 jun. 2020.

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

MIT TECHNOLOGY REVIEW INSIGHTS. How AI is humanizing health care: Artificial intelligence is helping health-care professionals do their jobs better, giving them the tools to build a smarter, more efficient ecosystem. *In*: MASSACHUSETTS INSTITUTE OF TECHNOLOGY (ed.). *MIT Technology Review*. [*S. l.*], 22 jan. 2020. Disponível em: <https://www.technologyreview.com/2020/01/22/276128/how-ai-is-humanizing-health-care/>. Acesso em: 2 jun. 2020.

MONTI, Andrea. Tribunale di Milano: Ord. 24 marzo 2011. *In*: MONTI, Andrea. *ICT LEX*: Diritto, politica, cultura della Rete. [*S.l.*], 24 mar. 2011. Disponível em: <https://www.ictlex.net/?p=1285>. Acesso em: 7 jan. 2021.

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

NORVIG, Peter Peter; NORVIG, Peter. *Inteligência Artificial*. 3. ed. Rio de Janeiro: Elsevier, 2013. Tradução de Regina Célia Simille.

O'NEIL, Cathy. *Weapons of math destruction:* how big data increases inequality and threatens democracy. New York:Crown Publishers, 2016. Ebook.

PERRY, Walter L.; MCINNIS, Brian; PRICE, Carter C.; SMITH, Susan C.; HOLLYWOOD, John S. *Predictive Policing*: The Role of Crime Forecasting in Law Enforcement Operations. [*S. l.*]: RAND Corporation, 2013. E-book.

RAHWAN, Iyad *et al*. Machine behaviour. *Nature*, [*s. l.*], v. 568, p. 477–486, 24 abr. 2019. Disponível em: <https://www.nature.com/articles/s41586-019-1138-y>. Acesso em: 2 jun. 2020.

SCHILLER, Arnold; WEISKOPF, Tobias. Automated Censorship in the Digital Space. *In*: YOUNG EUROPEAN FEDERALISTS (Europe). *The New Federalist*, 1 maio 2019. Tradução de Nora Teuma. Disponível em: <https://www.thenewfederalist.eu/automated-censorship-in-the-digital-space?lang=fr>. Acesso em: 9 dez. 2020.

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

THOMSON, Amy; BODONI, Stephanie. Google CEO Thinks AI Will Be More Profound Change Than Fire. *In*: *Bloomberg*. [*S. l.*], 22 jan. 2020. Disponível em: <https://www.bloomberg.com/news/articles/2020-01-22/google-ceo-thinks-ai-is-more-profound-than-fire>. Acesso em: 2 jun. 2020.

WEBER, Max. A objetividade do conhecimento nas ciências sociais. In: FERNANDES, Florestan (org.). *Weber*: sociologia. São Paulo: Ática, 1999. Coleção Grandes Cientistas Sociais.

**Como citar:**

REIS, Nazareno César Moreira; FURTADO, Gabriel Rocha. *Decisões automatizadas: definição, benefícios e riscos*. **Civilistica.com**. Rio de Janeiro, a. 11, n. 2, 2022. Disponível em: <http://civilistica.com/decisoes-automatizadas/>. Data de acesso.

civilistica.com
Recebido em:
28.10.2021
Aprovado em:
10.8.2022