© ***Cadernos de Dereito Actual*** Nº 16. Núm. Ordinario (2021), pp. 369-383
·ISSN 2340-860X - ·ISSNe 2386-5229

# Perspectivas sobre a responsabilidade civil por danos causados pelas aplicações de Inteligência Artificial no delineamento do perfil do consumidor no Brasil

Perspectives on civil liability for damages caused by Artificial Intelligence applications in identification of the consumer's profile in Brazil

**Sabrina Jiukoski da Silva**[1]
**Thatiane Cristina Fontão Pires**[2]
*Universidade Federal de Santa Catarina*



**Resumo:** O presente artigo tem como objetivo introduzir o problema da imputação da responsabilidade civil por danos causados pelas aplicações de Inteligência Artificial (IA) no delineamento do perfil comportamental do consumidor no Brasil, por meio do método dedutivo e da técnica de pesquisa bibliográfica. Para tanto, na primeira seção, traçar-se-á o conceito e as características da IA, notadamente a falta de limites em relação aos resultados que ela pode alcançar nas aplicações estratégicas de *marketing* para o delineamento do perfil do consumidor. Na segunda seção, passa-se à análise dos pressupostos da responsabilidade civil previstos na Lei Geral de Proteção de Dados Pessoais brasileria (LGPD) em face do tratamento irregular de dados, numa abordagem comparada com o regulamento análogo europeu (RGPD). Conclui-se, ao final, que os agentes devem ser responsabilizados independentemente de culpa no Brasil, uma vez que o elemento essencial de imputação é o tratamento irregular dos dados pessoais, sendo este observado quando ocorrer em inobservância da legislação de proteção ou frustrar a legítima expectativa de segurança dos titulares dos dados.

**Palavras-chave:** Responsabilidade Civil; Danos; Inteligência Artificial; Perfilização.

**Abstract:** This article aims to introduce the problem concerning liability imputation of damages caused by Artificial Intelligence (AI) applications in the process of identification of the consumer's profile in Brazil, through the deductive method and the bibliographic research technique. In the first section, the concept and characteristics of AI are identified, mainly the lack of limits on the results it can achieve in strategic marketing applications for identification of the consumer's profile. In the second section of this paper, the assumption of civil liability in the Brazilian

[1] Doutoranda e mestra em Direito pela Uni-versidade Federal de Santa Catarina (UFSC). Professora Substituta de Direito Civil da Universidade Federal do Rio de Janeiro (UFRJ). Bolsista CNPq. Membro do Grupo de Pesquisa de Direito Civil Contem-porâneo e do Instituto Brasileiro de Estudos de Responsabilidade Civil (IBERC).

[2] LL.M. em andamento na Universidade de Maastricht (Holland-High Potential Scholarship). Dou-toranda e mestra em Direito pela Universidade Federal de Santa Catarina (UFSC). Membro do Grupo de Pesquisa de Direito Civil Contem-porâneo.

Recibido: 12/07/2021
Aceptado: 06/09/2021

Data Protection Law regarding the irregular data processing are analyzed, in a comparative approach to the European analogue regulation (GDPR). The proposed analysis leads to the conclusion that agents must be held responsible regardless of negligence in Brazil, because the essential element of imputation is the irregular processing of personal data, once observed occurring in non-compliance with the protection legislation or frustrating the legitimate expectation of data subjects' security.

**Keywords:** Civil liability; Damages; Artificial Intelligence; Profiling.

## 1. Introdução

O avanço tecnológico mudou significativamente o hábito de compra dos consumidores. Pouco tempo atrás, era necessário dirigir-se às lojas físicas para a aquisição de bens e serviços. Para tanto, as possíveis influências externas para o ato de consumo eram propagandas realizadas nas mídias tradicionais. Na contemporaneidade, porém, o consumidor sequer precisa sair de casa para adquirir um produto ou serviço e, antes de tudo, utiliza-se de plataformas de busca, como *Google*, para pesquisar qual fornecedor tem o produto ou serviço mais indicado para as suas necessidades. Não satisfeito, consulta redes sociais, como *YouTube*, *Instagram* ou *Facebook*, para saber a opinião de outros consumidores, blogueiros e famosos acerca do produto escolhido para, então, tomar sua decisão.

Se na era pré-internet o obstáculo comercial era físico, diante da necessidade de aproximação entre os consumidores e os fornecedores, atualmente, todos os serviços, produtos e outros bens da informação podem ser acessados virtualmente. Nesse contexto, conforme Pedro Domingos, a dificuldade comercial passou a ser a previsão dos "cliques"[3].

Por conseguinte, as estratégias de *marketing* também passaram por uma mudança de paradigma. O foco empresarial migrou das mídias tradicionais para o ambiente virtual e passou a ser, sobretudo, o perfil comportamental do consumidor[4]. Entender o público-alvo, as características demográficas, o comportamento econômico para expandir as vendas, refinar produtos e preços, padronizar entregas e fornecer o *link* perfeito para cada tipo de usuário são, hoje, objetivos prementes do *marketing*, o que só se torna possível com o auxílio dos algoritmos[5] de Inteligência Artificial (IA).

Notável é o progresso proporcionado pelos algoritmos de IA ao *marketing* empresarial, posto que, em maior ou menor grau, essa tecnologia possibilita que programas de computador, em tempo real e em larga escala, por si próprios, passem a definir comportamentos humanos individuais ou de grupo – com base na análise do grande volume de dados pessoais deixados pelos usuários-consumidores no ambiente virtual – e direcionar campanhas publicitárias em conformidade com os

[3] DOMINGOS, P. *O algoritmo mestre*, Trad. Aldir José Coelho Corrêa da Silva, Novatec, São Paulo, 2017, p. 34.

[4] TORRES, C. *A bíblia do marketing digital: tudo o que você precisa saber sobre marketing e publicidade na internet e não tinha a quem perguntar*. Novatac, São Paulo, 2019. Cumpre consignar que o *marketing* engloba todas as composições criativas para se alcançar clientes e vendas, como infere-se: "[...] quando falamos em *marketing*, não se iluda, estamos falando também de vendas, de atrair novos clientes, de fidelizar os atuais, enfim, de fazer negócios. Como algumas empresas dividem as áreas de *marketing* e vendas em dois departamentos, muitas pessoas acabam criando a ideia equivocada de que são duas coisas distintas. Na verdade, vendas é parte do *marketing*. É um de seus resultados, mas não o único. Vender com rentabilidade, fidelizar clientes, expandindo o negócio e valorizando a marca no mercado, essa é uma das funções do *marketing*." (TORRES, C., *Op. cit*., p. 65).

[5] Em síntese, "um algoritmo é uma sequência de instruções que informa ao computador o que ele deve fazer" (DOMINGOS, P., *Op. cit*., p. 24).

dados tratados, atingindo resultados que seus criadores não eram capazes de alcançar.[6]

Esses sistemas são, hoje, classificados como semiautônomos, na medida que ainda possuem supervisão direta de seus programadores. Todavia, os sistemas de IA, sejam eles supervisionados ou não, têm o potencial de operar e decidir de forma verdadeiramente autônoma, ou seja, sem o aval ou, até mesmo, o conhecimento de seus programadores. E essas ações independentes dos sistemas de IA trazem novos desafios jurídicos e, portanto, demandam soluções de forma premente.[7]

Dentre as áreas sensíveis ao avanço tecnológico da IA, situa-se, notadamente, a prática de identificação de perfis comportamentais do consumidor, usualmente denominada pela expressão inglesa *profiling*[8], uma vez que as suas consequências negativas (danos) causadas aos mais diversos usuários-consumidores podem ser potencializadas, ainda mais, através do uso de aplicações de IA. Nesse contexto, o presente estudo tem como objetivo introduzir o problema da imputação de responsabilidade por danos causados pelas aplicações de Inteligência Artificial no delineamento do perfil comportamental do consumidor (perfilização), trazendo perspectivas da atual Lei Geral de Proteção de Dados (LGPD).

Para tanto, na primeira parte, é apresentado o conceito de IA, as suas principais características, notadamente a falta de limites em relação aos resultados que ela pode alcançar, bem como as estratégias de *marketing* que estão sendo delineadas com sua aplicação e os riscos e danos vivenciados pelos consumidores diante da perfilização.

Na segunda parte do artigo, a partir da caracterização do processo de perfilização como tratamento de dados pessoais, passa-se à análise dos pressupostos da responsabilidade civil previstos na LGPD em face do tratamento irregular de dados, introduzindo os principais debates doutrinários acerca da matéria, bem como aspectos-chave da normativa aplicáveis ao delineamento do perfil do consumidor, em abordagem comparada com o regulamento análogo europeu (Regulamento Geral de Proteção de Dados - RGPD).

---

[6] A exemplo, *Netflix, Amazon Prime* e *Disney+* utilizam algoritmos de IA para analisar dados como avaliações de filmes, compartilhamento nas redes sociais e histórico de filmes assistidos nas plataformas, para recomendar novos títulos aos assinantes, assim como entender por que as pessoas são emocionalmente atraídas por alguns conteúdos e por outros não (MACIEL, R. *Serviços como Netflix querem usar a IA para criar uma conexão emocional com você,* 2019). As redes varejistas, como *Renner* e *Target,* estão utilizando os algoritmos de IA para analisar o hábito de compra dos consumidores e tornar mais personalizada a venda de produtos em suas lojas (LOTUFO, É. *Com inteligência artificial, Renner quer "prever" venda de produtos, 2020*; e *TARGET: entenda como a loja monitora o comportamento do consumidor.* 2020).

[7] Para ilustrar, esse receio de lacunas de responsabilidade é uma das razões que levaram o Parlamento Europeu a aprovar, em 20 de outubro de 2020, uma resolução que inclui uma "Proposta de Regulamento do Parlamento Europeu e do Conselho sobre a responsabilidade pelo funcionamento de Sistemas de inteligência artificial". Essa proposta coloca mais pressão sobre a Comissão, que, com base no relatório apresentado pelo Grupo de Peritos em Responsabilidade e Novas Tecnologias - Formação de Novas Tecnologias (EG-NTF), publicou um relatório sobre as implicações de segurança e responsabilidade de IA, Internet das Coisas (Internet of Things - IoT) e robótica em fevereiro de 2020 e vem trabalhando em propostas legislativas há algum tempo. A propósito, cf. WENDEHORST, C. "Strict Liability for AI and other Emerging Technologies", *Journal of European Tort Law*, vol. 11, nº 2, 2020, pp. 150-180.

[8] Zanatta pontua que "No dicionário de língua inglesa, *profiling* (expressão inglesa de perfilização) significa "o ato ou processo de extrapolar informação sobre uma pessoa baseado em traços ou tendências conhecidas". Na tradição da ciência da informação anglo-saxônica, a perfilização se refere ao processo de construção e aplicação de um perfil de usuário (*user profile*) gerado por análises de dados computadorizadas". (ZANATTA, R. *Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais,* 2019, pp. 04-05).

## 2. A Inteligência Artificial aplicada às estratégias de *marketing* e o processo de perfilização

A programação de computadores, por muito tempo, resumiu-se ao processo de descrever as etapas necessárias para que uma máquina realizasse determinada tarefa e alcançasse um objetivo previamente determinado. A habilidade de acumular e aprender a partir de experiências, utilizando-se do aprendizado daí extraído, assim como a capacidade de agir de forma independente e tomar decisões de modo autônomo sempre foram características associadas à inteligência humana[9].

O desenvolvimento da inteligência artificial (IA), no entanto, promoveu uma verdadeira revolução nesse sentido, uma vez que possibilitou a mimetização da maneira como o cérebro humano funciona – e, consequentemente, da forma como os seres humanos aprendem e se comportam –, por meio de algoritmos aplicados em programas de computador. Isso permitiu que as máquinas passassem a aprender com as próprias experiências e a executar, com maior ou menor grau de autonomia, tarefas semelhantes às humanas[10].

Desse modo, os algoritmos de IA se distanciaram dos algoritmos tradicionais de computação, por possuírem capacidade de atuar de forma autônoma, a partir de experiências acumuladas, extraindo conhecimento e tomando decisões independentemente de seus criadores[11]. Assim como os humanos, portanto, as soluções de IA podem aplicar regras, aprender a partir de novos dados e informações e se adaptar às mudanças em seu ambiente[12].

Klaus Schwab sinaliza que os sistemas de IA estão sendo responsáveis por progressos impressionantes na última década, impulsionados tanto pelo aumento exponencial da capacidade de processamento, quanto pela disponibilidade de grandes quantidades de dados pessoais[13]. Muitos algoritmos de IA aprendem a partir de rastros de dados que os seres humanos deixam no ambiente digital e, mediante a análise de tais informações, apresentam sugestões, automatizando processos de decisão. Isso facilita e torna mais ágeis as conclusões empresariais com base em dados ou em experiências vividas[14].

Dito de outro modo, à medida que os seres humanos passaram a estar conectados diariamente ao ambiente virtual – dependendo cada vez mais de seus *smartphones*, computadores e assistentes virtuais –, o volume, a velocidade e a variedade de dados pessoais deixados no ambiente virtual cresceram significativamente e, com isso, as empresas visualizaram uma grande oportunidade de melhoramento de seu *core business*[15].

Mas esse melhoramento, grande parte através de estratégias de *marketing*, só é possível com a criação de bancos de dados específicos e de ferramentas cognitivas artificiais. Daí por que o progressivo interesse empresarial nos sistemas

---

[9] FONTÃO PIRES, T.C.; PETEFFI DA SILVA, R. "A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu", *Revista Brasileira de Políticas Públicas*, v. 7, nº 3, 2017, p. 238-254.

[10] DUAN, Y.; EDWARDS, J. S.; DWIVEDI, Y. K. "Artificial intelligence for decision making in the era of big data - evolution, challenges and research agenda", *International Journal of Information Management,* nº 48, 2019, p. 63–71.

[11] FONTÃO PIRES, T.C.; PETEFFI DA SILVA, R., *Op. cit*.

[12] CANHOTO, A.I.; CLEAR, F. "Artificial intelligence and machine learning as business tools: A framework for diagnosing value destruction potential", *Business Horizons*, nº 63, 2020, p. 183-193.

[13] Os incisos I e II do artigo 5º da LGPD definem, respectivamente, dados pessoas como "informação relacionada a pessoa natural identificada ou identificável" e dados pessoais sensíveis como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

[14] SCHWAB, K. *A Quarta Revolução Industrial*. Trad. Daniel Moreira. Edipro, São Paulo, 2016.

[15] Diz respeito à principal atividade de uma companhia.

de IA, em seu subcampo do *machine learning*[16], que é responsável, propriamente, pela habilidade de realizar o cruzamento de dados e extrair deles conhecimento de forma autônoma.

Pedro Domingos[17] pontua que as empresas passam por três estágios de crescimento na contemporaneidade e, ao final, necessitam do auxílio do *machine learning* para permanecerem no mercado de consumo, visto que esses algoritmos de aprendizagem fazem o papel de conciliadores, unindo fornecedores e consumidores.

Na primeira fase, as empresas fazem tudo manualmente. Ou seja, os proprietários conhecem pessoalmente seus clientes e encontram ou recomendam produtos ou serviços caso a caso. Com o crescimento da empresa, porém, isso já não é possível, e uma segunda fase se inicia. Trata-se da fase em que a empresa se depara com a necessidade de usar programas de computador. São necessários, então, programadores, consultores e gerentes de bancos de dados, e milhões de linhas de código são escritas para automatizar aquelas funções empresariais que, logicamente, podem ser automatizadas. Dessa forma, um número muito maior de consumidores é atendido, porém, de forma não personalizada, pois decisões são tomadas de acordo com categorias demográficas elementares, e os programas de computador empregados são rígidos demais para satisfazer a infinita versatilidade humana. Após um determinado ponto, não são encontrados programadores e consultores suficientes para fazer tudo que é necessário, momento em que a empresa passa a adotar o *machine learning.*[18]

Para tanto, os sistemas de IA possuem três componentes básicos de funcionamento. O primeiro deles é, justamente, os dados de entrada (*in-put)*, ainda que não estruturados, como imagens, falas e conversas. O segundo componente é composto por algoritmos de *machine learning*, responsáveis pelo processamento dos dados de entrada. Tais algoritmos podem ser: (i) supervisionados[19] (quando recebem de seus programadores um modelo rotulado para que possam aprender o padrão e, a partir dele, executar tarefas e desenvolver regras a serem aplicadas); (ii) não supervisionados (quando recebem apenas um conjunto de dados de treinamento com entradas sem rótulos e a tarefa do algoritmo é encontrar a melhor maneira de agrupar os pontos de dados e estabelecer como eles podem estar relacionados); e, por fim, (iii) de reforço (quando recebem um conjunto de dados de treinamento e uma meta a ser alcançada, sendo sua obrigação encontrar a melhor combinação de ações para alcançar essa meta). O terceiro, e último, componente da IA é, pois, a

[16] Em tradução livre, literalmente, aprendizagem de máquina. Isso significa que, quando um problema é dado para a IA resolver, os seus desenvolvedores não fornecem um algoritmo específico que descreve o passo a passo para alcançar a solução. Pelo contrário, é fornecida apenas uma descrição do problema em si, o que permite à IA construir o caminho para chegar a uma solução, ou seja, a tarefa da IA é buscar por uma solução através do seu próprio aprendizado. A propósito: POOLE, D.; MACKWORTH, A. *Artificial Intelligence: Foundations of Computational Agents,* Cambridge University Press, Cambridge (UK), 2010.

[17] DOMINGOS, P., *Op. cit*.

[18] A título de exemplo, sem *machine learning*, *Amazon* precisaria codificar, precisamente, os gastos de todos os seus clientes em um programa de computador, assim como *Facebook* teria que escrever um programa que selecionasse as melhores atualizações a serem exibidas para cada usuário; por sua vez, *Walmart,* que vende milhões de produtos, precisaria tomar bilhões de decisões complexas todos os dias. Desse modo, as empresas aplicam algoritmos de aprendizagem às montanhas de dados pessoais acumulados e deixam que eles, por si próprios, rompam a sobrecarga de informações e apontem o que os consumidores buscam ou querem adquirir naquele determinado momento (DOMINGOS, P., *Op. cit*.).

[19] Importante sinalizar, desde logo, que mesmo o processo de *machine learning* supervisionado, em que a função do algoritmo é inferida a partir de pares de dados de entrada e de saída rotulados, deve permitir que o algoritmo determine corretamente os rótulos (*labels*) para instâncias não previstas. Assim, diversas são as razões do porquê o algoritmo resultante possa vir a se comportar, posteriormente, de maneira imprevisível, notadamente erros no processo de rotulagem (*labelling*). Cf. WENDEHORST, C., *Op. cit*.

decisão resultante desse processo algoritmo ou uma seleção de resultados para ações humanas futuras, isto é, para a tomada de decisão empresarial futura[20].

Os algoritmos de aprendizagem no *marketing* normalmente recebem dados e uma meta a ser alcançada. Assim sendo, classificam-se como não supervisionados e são utilizados para garantir resultados considerados mais assertivos na tomada de decisão.[2122] São, ainda, projetados e utilizados tanto em decisões estratégicas, quanto em decisões táticas e operacionais. Dentre essas, destacam-se, essencialmente, a otimização automática de campanhas, a identificação de perfis comportamentais de consumidores – individuais ou em grupos –, prevendo tanto comportamentos de compra futuras, quanto estratégias para obter um maior número de consumidores e padronização de preços.

Como exemplo típico de aplicação de IA ao *marketing*, Thomas Davenport *et al.* elenca a otimização de preços, visto que o preço de um produto ou serviço deve ser baixo o suficiente para atrair clientes, mas alto o suficiente para permitir que a empresa obtenha lucros. Outro uso, consequentemente, está na identificação do perfil dos clientes: os altamente propensos a comprar, os muito improváveis de comprar e, por fim, aqueles intermediários. Depois disso, é possível direcionar a publicidade aos clientes intermediários, pois, via de regra, são os consumidores que podem fornecer os maiores retornos financeiros.[23]

Em outros casos, ainda, os sistemas de IA chegam a iniciar conversas por mensagens instantâneas ou chamadas telefônicas com potenciais clientes e, em seguida, os direcionam para um vendedor (humano). Do mesmo modo, entregam produtos sem que os consumidores se envolvam no processo de escolha e compra propriamente dito. Isto é, os clientes preenchem pesquisas de estilo e a IA avalia esses estilos, cria *links* e envia notas pessoais. O resumo dessas descobertas, após os cliques dos usuários, é encaminhado a estilistas de moda, que selecionam roupas adequadas com o perfil de cada consumidor e enviam os produtos selecionados. Outros sistemas de IA, por fim, incluem reconhecimento facial, varreduras biológicas, análises de estímulos (a exemplo do DNA e das temperaturas corporais).[24]

As possibilidades dos sistemas de IA no *marketing* são ilimitadas, contudo, como pontua Bruno Bioni, o ato de consumo está sendo modelado[25] e, mais do que isso, o direcionamento comportamental algorítmico e todas as ações daí decorrentes estão influenciando os consumidores, como também estão aumentando o controle sobre os usuários, ocasionando práticas discriminatórias e abusivas, além de causar danos às pessoas.

Dito de outra maneira, inúmeros são os dados sensíveis disponíveis no ambiente virtual – dados que revelem a origem racial ou étnica, o gênero, a preferência sexual, as opiniões políticas e as convicções religiosas – e a conectividade e a capacidade cognitiva da IA apresentam muitos desafios. Como enfatizam Canhoto e Clear, a IA pode se conectar a inúmeros ambientes externos, de modo que os dados coletados e verdadeiramente minerados serão desconhecidos por seus criadores, além de poderem vir a ser corrompidos, mostrarem-se incompletos ou enganosos. Os algoritmos de IA podem produzir resultados incompreensíveis para os seres

---

[20] CANHOTO, A.I.; CLEAR, F., *Op. cit.*

[21] CANHOTO, A.I.; CLEAR, F., *Op. cit.*

[22] Complementando, Duan, Edwards e Dwivedi enfatizam que "A nova onda de sistemas de IA tem melhorado a capacidade de usar dados para fazer previsões e tem reduzido, substancialmente, o custo de realizar tais previsões". No original: "*The new wave of AI systems has improved an organisation's ability to use data to make predictions and has substantially reduced the cost of making predictions"* (DUAN, Y.; EDWARDS, J. S.; DWIVEDI, Y. K., *Op. cit*., p. 63).

[23] DAVENPORT, T.; GUHA, A.; GREWAY, D.; BRESSGOTT, T.B. "How artificial intelligence will change the future of marketing", *Journal of the Academy of Marketing Science*, nº 48, 2020, p. 24–42.

[24] DAVENPORT, T.; GUHA, A.; GREWAY, D.; BRESSGOTT, T.B. *Op. cit.*

[25] BIONI, B.R. *Proteção de dados pessoais: a função e os limites do consentimento,* Forense, Rio de Janeiro, 2019, p. 122.

humanos, o que os torna impossíveis de corrigir ou controlar, como quando os *bots*[26] de negociação de IA do *Facebook* desenvolveram sua própria linguagem. Ou ainda, podem apresentar limitações na conversão de recursos complexos em formatos binários e criar *loops*, tornando-se complexos para seus programadores.[27] Mais do que isso, nesse processo, a depender do conteúdo da amostra de dados tratada, podem vir a direcionar oportunidades, potencializar padrões negativos e fomentar publicidades abusivas.

Exemplos de ações discriminatórias e abusivas realizadas por algoritmos de inteligência artificial e que se tornaram conhecidas no Brasil são, respectivamente, o *geoblocking* e o *geopricing.* O primeiro trata de um conjunto de ações que impedem determinados consumidores, diante de suas origens geográficas, de acessar e comprar produtos ou serviços como, por exemplo, locação de veículos e reservas de hotéis que, por vezes, têm o preço alterado conforme a região do consumidor. O segundo trata da precificação diferenciada de produtos e serviços, também com base em origens geográficas. Ou seja, o preço de determinado produto ou serviço variará de acordo com a região que o consumidor está (que é identificada através do número do IP). Dessa forma, não apenas as experiências dos usuários serão diferentes, mas também as ofertas que serão feitas dependendo da região, riqueza, gênero, raça e idade dos consumidores.[28]

Com a introdução de sistemas de IA mais avançados, a probabilidade de danos deve aumentar. Isso porque é intrínseco à inteligência artificial: (a) o ímpeto de se auto aperfeiçoar; (b) o desejo de ser racional; (c) a busca pela preservação da utilidade das suas funções; (d) a prevenção da falsificação de seus resultados operacionais ou das suas propriedades funcionais; (e) o desejo de adquirir recursos e usá-los de forma eficiente.[29] Essas aspirações são, apenas, objetivos intermediários e convergentes que levam ao objetivo final para o qual a IA foi criada. Ao alcançar tais objetivos intermediários, visando atingir o objetivo final, a IA pode causar danos a terceiros[30].

Como corolário lógico, essa propagação dos sistemas de IA no *marketing* empresarial permite a enunciação de uma série de questões jurídicas, principalmente no que tange à disciplina da responsabilidade civil. Os exemplos do *geoblocking* e o *geopricing* ilustram que a operação da IA e seus possíveis desdobramentos podem causar danos, assim como muitos outros em que os sistemas de IA podem tomar decisões independentes, sem transparência e, por vezes, não imaginadas por seus programadores.

## 3. LGPD e a responsabilidade civil do uso de aplicação de Inteligência Artificial no delineamento do perfil do consumidor

Ao se tratar da Inteligência Artificial (IA), duas das principais características novas que podem suscitar dúvidas acerca das noções de responsabilidade civil tradicionais são a autonomia e a opacidade. O termo autonomia refere-se, justamente, a essa certa falta de previsibilidade no que diz respeito à reação do

[26] *Bot*, diminutivo de *robot*, também conhecido como *Internet bot* ou *web robot*, é uma aplicação de *software* concebido para simular ações humanas repetidas vezes de maneira padrão, da mesma forma como faria um robô (KONGTHON, A. et al. "Implement-ing an online help desk system based on conversational agent", *Proceedings of the International Conference on Management of Emergent Digital EcoSystems*, nº 69, 2009).
[27] CANHOTO, A.I.; CLEAR, F., *Op. cit.*
[28] MARTINS, G.M. "O *geopricing* e *geoblocking* e seus efeitos nas relações de consumo", en FRAZÃO, A.; MULHOLLAND, C. (Coords.), *Inteligência Artificial e Direito*: ética, regulação e responsabilidade, Thomson Reuters Brasil, São Paulo, 2019, p. 636-637.
[29] MUEHLHAUSER, L.; SALAMON, A. "Intelligence explosion: evidence and import", en EDEN, A. (Ed.) et al. *Singularity hypotheses: a scientific and philosophical assessment*, Springer, Heidelberg, 2012, p. 15-42.
[30] FONTÃO PIRES, T.C.; PETEFFI DA SILVA, R., *Op. cit*.

*software* a circunstâncias não antecipadas. Trata-se, em particular, de situações em que a codificação do *software* ocorreu total ou parcialmente com a ajuda de *machine learning* – muito embora a noção de IA deva ser mais ampla e mais neutra do ponto de vista tecnológico –, tornando difícil prever como o *software* reagirá a cada situação específica no futuro.[31]

Embora o comportamento imprevisto em situações não antevistas pelo programador também possa ocorrer com o *software* de tipo tradicional, algoritmos criados com a ajuda de *machine learning* não podem ser facilmente analisados, especialmente quando métodos sofisticados de *deep learning*[32] foram empregados. Essa opacidade do código – chamado "efeito caixa-preta" (*black box effect*) – significa que não é fácil explicar por que a IA se comportou de uma maneira particular em uma dada situação. Tarefa ainda mais difícil seria rastrear esse comportamento de volta a qualquer ponto que pudesse ser chamado de "defeito" do código programado ou qualquer falha no processo de desenvolvimento.[33]

Nesse contexto, as propostas aos desafios impostos pela IA usualmente se dividem entre medidas de prevenção (*ex ante response*) ou de responsabilidade (*ex post response*). Uma abordagem puramente econômica – que tem sido a abordagem predominante, por exemplo, nos Estados Unidos da América – insiste que as medidas de prevenção devem ser tomadas apenas quando o custo geral dessas medidas ainda seja inferior ao custo geral do dano provável de ser causado. Se, porém, o custo das medidas preventivas excederia o custo total do dano provável, tais medidas não são necessárias, ou não deveriam ser tomadas, porque simplesmente deixar que o dano ocorra, compensando-se as vítimas posteriormente, seria mais eficiente.[34] Alguns iriam mais longe, dizendo que isso é verdade mesmo quando nenhuma compensação é concedida (fórmula de Kaldor-Hicks[35]).[36]

Por sua vez, a Europa sempre seguiu um caminho diferente, por várias razões, incluindo que a morte, lesões corporais e (outras) violações dos direitos fundamentais não podem ser simplesmente reduzidas a um valor monetário. Outrossim, defende-se que a abordagem puramente econômica muitas vezes não leva em conta o real custo de acidentes, por exemplo, o dano econômico causado por uma falta geral de confiança por parte dos consumidores e outros danos coletivos, bem como questões sociais.[37] Tais considerações apontam que medidas de prevenção e de responsabilidade não devem ser totalmente independentes umas das outras. Pelo contrário, uma conexão mais estreita entre ambas as respostas é aconselhável.[38]

Isso significa dizer, *inter alia*, que se o risco vier a se materializar, a pessoa responsável pelo dano será, justamente, aquela que deveria ter evitado o risco através da adoção de medidas de prevenção. Nesse contexto, a regulamentação de um *standard* mínimo de segurança a ser adotado deve determinar, até mesmo, a

---

[31] WENDEHORST, C., *Op. cit*.

[32] O *deep learning,* ou simplesmente aprendizagem profunda, é uma subdivisão do machine learning e pode ser definido, em apertada síntese, como "o uso de redes neurais em multiníveis para encontrar padrões em imensos corpos de dados". No original: "*Deep learning (DL) is the use of multilevel neural networks to find patterns in huge bodies of data*" (BODEN, M. "On deep learning, artificial neural networks, artificial life, and good-old fashioned AI", *Oxford University Press's Blog,* 2016).

[33] WENDEHORST, C., *Op. cit*.

[34] Cf. KOLSTAD, C.; ULEN, T.; JOHNSON, G. "Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?", *The American Economic Review*, 1990.

[35] Em apertada síntese, a fórmula Kaldor-Hicks afirma que um resultado é proveitoso se quem obteve o ganho poderia, hipoteticamente, compensar aquele que sofreu a perda. Cf. a respeito: KALDOR, N. "Welfare Propositions of Economics and Interpersonal Comparisons of Utility", *The Economic Journal*, nº 549, 1939; bem como: HICKS, J.R. "The Foundations of Welfare Economics", *The Economic Journal*, nº 696, 1939.

[36] WENDEHORST, C., *Op. cit*.

[37] WENDEHORST, C., *Op. cit*.

[38] Chega-se a afirmar que é da natureza e do propósito da imputação de responsabilidade a função de prevenir o dano. Cf. European Group on Tort Law. *Principles of European Tort Law (PETL)*, art. 10:101, parte 2: "*Damages also serve the aim of preventing harm*".

distribuição do ônus da prova quanto ao nexo de causalidade e possíveis excludentes (ao se provar que as medidas de segurança foram adotadas).[39]

Não raramente, os dados tratados no âmbito do *marketing* serão de cunho pessoal dos usuários-consumidores, enquadrando-se, pois, na categoria de tratamento de dados pessoais. Nesse ponto, seja por uma questão de tradição jurídica, seja em função da evidente inspiração da recente Lei Geral de Proteção de Dados (LGPD) brasileira em relação à normativa análoga europeia (Regulamento Geral de Proteção de Dados - RGPD), é natural a comparação com o velho continente.[40]

No cenário europeu, o RGPD impõe ao controlador a obrigação de aplicar medidas técnicas adequadas para assegurar e poder comprovar que o tratamento de dados está sendo realizado em conformidade com o diploma normativo, sem perder de vista o contexto e a finalidade do tratamento de dados, bem como os riscos para os direitos e liberdades das pessoas naturais.[41] Nota-se, pois, a opção pela conjunção de medidas de prevenção com a de eventual responsabilidade nos casos de não atendimento do padrão mínimo de segurança, que engloba, *v.g.*, a declaração de consentimento livre dos usuários, bem como a existência de um interesse legítimo para a atividade de tratamento.[42]

Em sentido similar, a responsabilidade civil no âmbito da LGPD tem em conta, em primeiro lugar, a natureza da atividade de tratamento de dados, que a norma procura restringir às hipóteses com fundamento legal (art. 7º), bem como que o tratamento não compreenda dados além do que o estritamente necessário (princípio da finalidade, art. 6º, III), nem seja inadequado ou desproporcional em relação à sua finalidade (art. 6º, II).[43]

No que tange mais especificamente à obrigação de indenizar dos agentes de tratamento[44], o artigo 42 estabelece a regra geral para sua configuração, ao passo que o artigo 43 prevê as hipóteses excludentes de responsabilidade, dentre as quais se destaca a possibilidade de prova, por parte dos agentes de que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados (inciso II) – ou seja, o padrão mínimo de segurança foi devidamente adotado.

Da simples leitura dos artigos citados, percebe-se que o legislador nacional optou por não definir, expressamente, a modalidade de responsabilidade civil a ser aplicada no âmbito da LGPD. Como corolário, a doutrina civilista nacional apresenta forte discussão sobre o fundamento de imputação do dever de indenizar, em que se defrontam dois princípios ético-jurídicos: o princípio da culpa e o do risco.

Sustenta-se, de um lado, que a legislador optou por consagrar a responsabilidade subjetiva, pois, dentre tantos argumentos presentes na doutrina, o

[39] WENDEHORST, C., *Op. cit*.
[40] Cf. WERLANG PAIM, B.; RUTHES GONÇALVES, L. "A responsabilidade civil no tratamento de dados pessoais pelas aplicações de inteligência artificial", en WACHOWICZ, M. (Org.). *Proteção de dados pessoais em perspectiva*: *LGPD e RGPD na ótica do direito comparado*, Gedai, UFPR, Curitiba, 2020, p. 451-480.
[41] WERLANG PAIM, B.; RUTHES GONÇALVES, L., *Op. cit.*
[42] Cf. UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*, Preâmbulo, parágrafos 24 e 40 a 49.
[43] SCHERTEL MENDES, L.; DONEDA, D. "Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados", *Revista de Direito do Consumidor*, vol. 120, ano 27, 2018, p. 469-483.
[44] Conforme a definição da própria legislação, os agentes de tratamento são os controladores e os operadores de dados (art. 5º, inc. IX). O controlador "é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" e o operador, por sua vez, é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, inc. VI e VII da LGPD).

legislador teria adotado uma espécie de culpa normativa[45], afastando-se da concepção clássica de culpa e se alicerçando em uma visão objetiva, pautada na adequação do tratamento à norma.[46] De outro lado, afirma-se que a omissão legislativa dá-se porque a atividade de tratamento de dados pessoais possui um risco próprio ou intrínseco e, portanto, se configura objetiva à luz parágrafo único do artigo 927 do Código Civil (CC/2002).[47] Finalmente, há quem defenda que não é possível ter uma abordagem unitária, uma vez que a sistemática da norma apresenta ora viés objetivo, ora subjetivo.[48]

Cumpre aqui fazer uma crítica pontual aos defensores da culpa normativa, visto que o que se pretende por meio da expressão é, em verdade, fazer alusão ao critério objetivo do conceito de ato ilícito, ou seja, a antijuridicidade. A tradição nacional tem a antijuridicidade como elemento da responsabilidade civil a partir da locução "violar direito" (art. 186 do CC/2002), que, agora, está presente no *caput* do art. 42 e no inc. II do art. 43 ambos da LGPD ("violação à legislação de proteção de dados pessoais").

Dito de outro modo, culpa e antijuridicidade não se confundem, posto que, consoante elucida Rafael Peteffi da Silva, "o juízo de antijuridicidade conecta-se com o desvalor que recai sobre o fato que está em contradição com o interesse preponderante declarado pela norma [ato contrário à norma], afastando-se definitivamente de um juízo de culpabilidade".[49] Por tal motivo se afirma que a antijuridicidade está igualmente presente na responsabilidade objetiva, notadamente porque "o ordenamento jurídico cobre com o manto da antijuridicidade os fatos causadores de danos que estiverem dentro da área de atuação de determinado agente, ainda que a conduta *normalmente* desenvolvida, apesar de perigosa, não seja considerada, *per se*, ilícita"[50].

A partir desses pressupostos, a responsabilidade civil dos agentes de tratamento deve ser interpretada como sendo objetiva, por se tratar de uma atividade que, por sua natureza, implica em riscos para os direitos dos usuários (parágrafo único do artigo 927 do CC/2002), além de ser normalmente desenvolvida pelos operadores e controladores.

Outrossim, no que concerne especificamente aos danos causados por aplicações de IA, frisa-se que a responsabilidade subjetiva não responde adequadamente aos desafios colocados pelas tecnologias digitais emergentes, visto que tanto a autonomia, quanto a opacidade tornam difícil rastrear o dano a qualquer tipo de intenção ou negligência por parte de um ator humano.[51]

---

[45] GUEDES, G.S.C.; MEIRELES, R.M.V. "Término do Tratamento de Dados", en FRAZÃO, A.; TEPEDINO, G.; DONATO OLIVA, M., *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*, Thomson Reuters Brasil, São Paulo, 2019, p. 219-241.

[46] Também são partidários dessa corrente: BIONI, B.R.; DIAS, D. "Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor", *Civilistica.com*, v. 9, nº 3, 2020, p. 1-23.

[47] Nesse sentido: SCHERTEL MENDES, L.; DONEDA, D., *Op. cit*.; e GODINHO, A.M.; QUEIROGA NETO, G.R.; MORAIS TOLÊDO, R.C. "A responsabilidade civil pela violação a dados pessoais", *Revista IBERC*, v. 3, n. 1, 2020.

[48] A propósito: BRUNO, M.G.S. "Da responsabilidade e do ressarcimento de danos", en MALDONADO, V.N.; BLUM, R.O. (coords.), *LGPD: Lei Geral de Proteção de dados comentada*. 2. ed. rev., atual. e ampl., Thomson Reuters Brasil, São Paulo, 2019. p. 322-331; SCHREIBER, A. "Responsabilidade civil da Lei Geral de Proteção de Dados Pessoais", en DONEDA, D.; SARLET, I.W.; MENDES, L.S.; RODRIGUES JUNIOR, O.L.; BIONI, B.R., *Tratado de proteção de dados pessoais,* Forense, Rio de Janeiro, 2021, p. 319-338.

[49] PETEFFI DA SILVA, R. "Antijuridicidade como requisito da responsabilidade civil extracontratual: amplitude conceitual e mecanismos de aferição", *Revista de Direito Civil Contemporâneo*, vol. 18, ano 6, 2019, p. 169-214.

[50] PETEFFI DA SILVA, R., Op. cit., p. 198.

[51] WENDEHORST, C., *Op. cit*. O mesmo se aplica aos fenômenos de complexidade, abertura e vulnerabilidade dos ecossistemas digitais, bem como às novas tecnologias distribuídas de livro-

Os agentes de tratamento de dados devem ser, portanto, responsabilizados, independentemente da comprovação de culpa, podendo-se afirmar que a LGPD consagrou uma cláusula geral de responsabilidade civil objetiva[52], cujo elemento essencial para imputação é o tratamento irregular dos dados pessoais coletados.

Consoante a LGPD, o tratamento de dados pessoais será irregular nas hipóteses de: (i) inobservância da legislação de proteção (art. 44, *caput*); e (ii) fornecimento de segurança inferior àquela que o titular dos dados pode esperar, sendo relevante, para tal configuração, o modo pelo qual o tratamento é realizado, o resultado e os riscos que razoavelmente dele se esperam, e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44, *caput* e incisos). Assim, respondem pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no artigo 46 desta Lei, der causa ao dano (art. 44, parágrafo único).

Por fim, o artigo 45 da LGPD remete à aplicabilidade do Código de Defesa do Consumidor (CDC) às hipóteses de violação do direito do titular dos dados no âmbito das relações de consumo. O marco regulatório brasileiro abrange, portanto, todas as operações de tratamento de dados pessoais realizadas no território nacional (art. 3º), englobando também as operações de dados nas relações consumeristas. Por derradeiro, a leitura do *standard* mínimo da LGPD deve ser realizada em conjunto com as diretrizes do microssistema consumerista.

Como se vê, o legislador vinculou o tratamento irregular dos dados pessoais a dois critérios: a observância da legislação de proteção e a legítima expectativa de segurança. A proteção contra o tratamento irregular não visa, contudo, a uma segurança absoluta, já que o tratamento de dados não pode ser considerado irregular simplesmente em razão de as expectativas subjetivas do titular terem sido frustradas.[53] Trata-se, pois, de um parâmetro objetivo, consubstanciado na expectativa legítima do público em geral, aferida não pela análise individual da vítima, mas por meio da concepção coletiva da sociedade de consumo, ou melhor, da sociedade de informação[54].

É evidente o paralelo com o código consumerista ao se adotar o critério segurança na LGPD. A doutrina aponta tratar-se de uma fórmula indeterminada, que estará sempre vinculada à casuística,[55] predominando, no aspecto, a corrente que entende ser objetivo o critério de segurança. Para Guilherme Reinig, "o critério objetivo tem como vantagem exigir do juiz que procure, ao decidir o caso concreto,

---

razão (DLT), como *blockchain*, em que o risco é diluído pela interação de um número muito grande de diferentes pessoais, muitas das quais guardam anonimato.

[52] O termo "responsabilidade civil objetiva" é utilizado, aqui, em sentido amplo, para qualquer forma de responsabilidade sem culpa. Isso engloba, pois, a responsabilidade desencadeada pela violação de determinadas leis ou padrões específicos (*non-compliance liability*), cujo objetivo inclui a prevenção de danos do tipo em questão, bem como a responsabilidade por defeito do produto. Não se ignora, porém, o entendimento segundo o qual o termo deva ser, indiscutivelmente, reservado para as formas de responsabilidade baseadas quase exclusivamente na causalidade e que, como tais, não exigem qualquer tipo de não conformidade ou defeito ou mau desempenho. Em defesa do uso estrito do termo responsabilidade objetiva: WENDEHORST, C., *Op. cit*.

[53] No ponto, fazendo-se um paralelo com a legislação consumerista acerca do defeito do produto, a defectibilidade do produto se baseia numa falta de segurança que o público em geral pode legitimamente esperar. O parâmetro para a verificação do defeito, assim como na Diretiva 85/74/CEE (art. 6º), são as legítimas expectativas de segurança. (LIMA REINIG, G.H. *A responsabilidade do produtor pelos riscos do desenvolvimento,* Atlas, São Paulo, 2013).

[54] Para maiores esclarecimentos, ver: VASCONCELLOS E BENJAMIN, A. H. "Da qualidade de produtos e serviços, da prevenção e da reparação dos danos.", em OLIVERA, Juarez., *Comentários ao Código de Proteção do Consumidor,* Saraiva, São Paulo, 1991, p. 60.

[55] Nesse sentido, VIEIRA SANSEVERINO, P.T. *Responsabilidade Civil no Código do Consumidor e a Defesa do Fornecedor,* Saraiva, São Paulo, 2010, p. 125; LIMA REINIG, G.H., *Op. cit.*, p. 30; e VASCONCELLOS BENJAMIN, A.H., *Op. cit.*, p. 60.

generalizar ao máximo os fundamentos de sua decisão, a fim de que a mesma solução possa ser aplicada a casos semelhantes"[56].

A despeito da adoção de critérios objetivos, a noção de segurança no ambiente digital é nebulosa, sobretudo ao se subsumir as circunstâncias relevantes elencadas pelo legislador às aplicações de IA, nas quais a autonomia é uma característica previsível que, por sua vez, pode gerar resultados inesperados. Nesse ponto, adverte Dominique Guinard, "a segurança dos objetos inteligentes é tão forte quanto seu enlace mais fraco"[57]. Ou seja, as soluções de segurança ainda não estão consolidadas entre controladores e operadores, sendo ainda objeto de debate. Nesse contexto, ao menos hipoteticamente, a autonomia da IA traz novamente à tona o problema dos riscos indetectáveis pelo estado dos conhecimentos científicos e técnicos, tratado pela teoria do risco do desenvolvimento.[58]

Outro aspecto sensível diz respeito ao fato de a LGPD vincular o resultado e os riscos esperados à noção de consentimento, confidencialidade e finalidade. Os dados pessoais estão caracterizados na legislação, em regra geral, como informações relacionadas à pessoa natural identificada ou identificável (art. 5º, inc. I)[59], e essas informações só podem ser coletadas e tratadas mediante o consentimento pelo titular (art. 7º, inc. I), sendo vedado o tratamento de dados pessoais mediante vício de consentimento (art. 8º, *caput* e § 3º)[60].

Infere-se, portanto, que o instituto do consentimento passa a figurar como instrumento, por excelência, da manifestação da escolha individual. Se, por um lado, tal aspecto privilegia a autodeterminação informativa[61], por outro lado, passa a figurar como instrumento de legitimação de situações potencialmente abusivas.

A exemplo, muito embora o regulamento europeu de proteção de dados tenha tratado expressamente do fenômeno da perfilização, garantindo ao titular dos dados o direito de não estar sujeito a decisões baseadas somente em processamento automático, acabou por excepcionar essa regra caso a decisão esteja apoiada no consentimento explícito do titular dos dados.[62] Ocorre que, e não é demais pontuar, uma análise puramente literal dos dispositivos aplicáveis pode levar a crer que o consentimento "pode ser dado [pura e simplesmente] validando uma opção ao visitar um sítio *web* na *Internet*, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto"[63]. Argumenta-se, assim, que o consentimento não pode ser dissociado da noção de finalidade prevista no regulamento.

---

[56] LIMA REINIG, G.H., *Op. cit.*, p. 31. O autor aponta críticas tanto ao critério subjetivo quanto ao critério objetivo de segurança legitimamente esperada, pois ambos são imprecisos. A imprecisão é própria do conceito de defeito estipulado, mas o critério objetivo, como aponta, é mais adequado para as análises dos casos concretos. Partindo, assim, da ideia de que a segurança deve ser analisada a partir da segurança legitimamente esperada pelo consumidor médio (LIMA REINIG, G.H., *Op. cit.*, p. 31-32).

[57] No original: "*After all, the security of a smart object is only as strong as its weakest connected link*" (GUINARD, D. *The Politics Of The Internet Of Things*. 2016).

[58] A propósito: LIMA REINIG, G.H.; AMARAL CARNAÚBA, D. "Responsabilidade civil e novas tecnologias: riscos do desenvolvimento retornam à pauta", *Revista Consultor Jurídico*, 2019.

[59] O legislador brasileiro tomou o cuidado de conceituar os dados pessoais sensíveis e os dados anonimizados (art. 5º, inc. II e III).

[60] A legislação elenca hipóteses em que o tratamento de dados pode ser realizado sem o consentimento do titular, vide *caput* e incisos do art. 7.

[61] DONEDA, D. *Da privacidade à proteção de dados pessoais*, Renovar, Rio de Janeiro, 2006, p. 366. O surgimento do direito à autodeterminação informativa tem suas origens no ordenamento jurídico alemão. A ideia central é garantir o direito de autodeterminação dos indivíduos no sentido de poder controlar e fiscalizar o levantamento de seus dados pessoais e relativos à sua vida privada (DONEDA, D., *Op. cit.*, p. 196).

[62] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Seção 4, artigo 22, (1) e (2), alínea c.

[63] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Preâmbulo, Parágrafo 32.

No mesmo sentido, a fiel observância dos termos da LGPD também deverá acarretar o desvinculamento da ideia de consentimento do simples "eu aceito" ou "eu concordo" ao final de grandes textos de política de privacidade presentes no acesso a sítios eletrônicos, aplicativos e redes sociais. Os termos de uso generalistas, complexos e em letras muito pequenas, que permitem coletar todo e qualquer tipo de dado para fins de "melhoria dos serviços" ou de "compartilhamento com terceiros", não são suficientes para configurar o consentimento dos usuários. O consentimento deverá referir-se a finalidades determinadas, pois o tratamento de dados só poderá ocorrer com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (inc. I do art. 6º). Importante frisar que as autorizações genéricas para o tratamento de dados pessoais serão nulas (§ 4º do art. 8).

Esse aspecto final deve representar um grande desafio para as ações de *compliance* junto aos agentes de tratamento de dados que atuam nos processos de perfilização mediante a aplicação de IA, porquanto a conexão com a finalidade precípua do tratamento poderá ser perdida no decorrer do processo, sobretudo diante das características de autonomia e opacidade dessa nova tecnologia.

## 4. Considerações Finais

O problema da imputação de responsabilidade civil por danos causados pelas aplicações de Inteligência Artificial (IA) tem ensejado inúmeros debates no âmbito acadêmico. Está claro que a IA, por suas características próprias, não encontra limites teóricos e que inúmeros danos podem derivar do seu uso. Dentro desse universo de possíveis aplicações, tratou-se do uso da IA no delineamento do perfil comportamental do consumidor. A relevância do problema exposto é tangível e tende a afetar cada vez mais a sociedade, já que as empresas estão investindo nessa área para crescimento de mercado.

A partir da caracterização do processo de perfilização como atividade de tratamento de dados pessoais dos usuários-consumidores, bem como das diferentes abordagens jurídicas da questão, verificou-se que os agentes de tratamento de dados devem ser responsabilizados independentemente de culpa, em consonância com os diplomas normativos aplicáveis (LGPD e CDC). Trata-se, assim, de modalidade de responsabilidade objetiva, cujo elemento essencial de imputação será o tratamento irregular dos dados pessoais, sendo este observado quando ocorrer em inobservância da legislação de proteção ou frustrar a legítima expectativa de segurança dos titulares dos dados.

Dessarte, questões relativas à segurança dos titulares passam a ser pauta de análise, pois as características de autonomia e opacidade da IA fazem reavivar o problema dos riscos indetectáveis pelo estado dos conhecimentos científicos e técnicos.

Por derradeiro, apontou-se como aspecto merecedor de especial atenção a importância conferida pela legislação de proteção ao consentimento do titular dos dados. Se, por um lado, tal aspecto privilegia a autodeterminação informativa, por outro lado, passa a figurar como instrumento de legitimação de situações potencialmente abusivas.

## Referências

BIONI, B.R. *Proteção de dados pessoais*: *a função e os limites do consentimento*, Forense, Rio de Janeiro, 2019.

BIONI, B.R.; DIAS, D. "Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor", *Civilistica.com*, v. 9, nº 3, 2020, p. 1-23.

BODEN, M. "On deep learning, artificial neural networks, artificial life, and good-old fashioned AI.", *Oxford University Press's Blog*. Disponível em:https://blog.oup.com/2016/06/artificial-neural-networks-ai/. Acesso em: 30 jun. 2021.

BRUNO, M.G.S. "Da responsabilidade e do ressarcimento de danos", en MALDONADO, V.N.; BLUM, R.O. (coords.), *LGPD: Lei Geral de Proteção de dados comentada*. 2. ed. rev., atual. e ampl., Thomson Reuters Brasil, São Paulo, 2019. p. 322-331.

CANHOTO, A.I.; CLEAR, F. "Artificial intelligence and machine learning as business tools: A framework for diagnosing value destruction potential", *Business Horizons*, nº 63, 2020, p. 183-193.

CORACCINI, R. *Walmart transforma megastore em laboratório de inteligência artificial,* 2019. Disponível em: encurtador.com.br/gjCKS. Acesso em: 22 jun. 2021.

DAVENPORT, T.; GUHA, A.; GREWAY, D.; BRESSGOTT, T.B. "How artificial intelligence will change the future of marketing", *Journal of the Academy of Marketing Science*, nº 48, 2020, p. 24–42.

DOMINGOS, P. *O algoritmo mestre*, Trad. Aldir José Coelho Corrêa da Silva, Novatec, São Paulo, 2017.

DONEDA, D. *Da privacidade à proteção de dados pessoais,* Renovar, Rio de Janeiro, 2006.

DUAN, Y.; EDWARDS, J. S.; DWIVEDI, Y. K. "Artificial intelligence for decision making in the era of big data - evolution, challenges and research agenda", *International Journal of Information Management,* nº 48, 2019.

FONTÃO PIRES, T.C.; PETEFFI DA SILVA, R. "A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu", *Revista Brasileira de Políticas Públicas*, v. 7, nº 3, 2017, p. 238-254.

GODINHO, A.M.; QUEIROGA NETO, G.R.; MORAIS TOLÊDO, R.C. "A responsabilidade civil pela violação a dados pessoais", *Revista IBERC*, v. 3, n. 1, 2020.

GUEDES, G.S.C.; MEIRELES, R.M.V. "Término do Tratamento de Dados", en FRAZÃO, A.; TEPEDINO, G.; DONATO OLIVA, M., *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*, Thomson Reuters Brasil, São Paulo, 2019, p. 219-241.

GUINARD, D. *The Politics Of The Internet Of Things*, 2016. Disponível em: < https://techcrunch.com/2016/02/25/the-politics-of-the-internet-of-things/> Acesso em: 10 jul. 2021.

HICKS, J.R. "The Foundations of Welfare Economics", *The Economic Journal*, nº 696, 1939.

KALDOR, N. "Welfare Propositions of Economics and Interpersonal Comparisons of Utility", *The Economic Journal,* nº 549, 1939.

KOLSTAD, C.; ULEN, T.; JOHNSON, G. "Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?", *The American Economic Review*, 1990.

KONGTHON, A. et al. "Implement-ing an online help desk system based on conversational agent", *Proceedings of the International Conference on Management of Emergent Digital EcoSystems*, nº 69, 2009.

LIMA REINIG, G.H. *A responsabilidade do produtor pelos riscos do desenvolvimento.* Atlas, São Paulo, 2013.

LIMA REINIG, G.H.; AMARAL CARNAÚBA, D. "Responsabilidade civil e novas tecnologias: riscos do desenvolvimento retornam à pauta", *Revista Consultor Jurídico*, 2019. Disponível em <https://www.conjur.com.br/2019-nov-25/direito-civil-atual-riscos-novas-tecnologias-retornam-pauta>. Acesso em 10 jul. 2021.

LOTUFO, E. *Com inteligência artificial, Renner quer prever venda de produtos,* 2020. Disponível em: encurtador.com.br/bemtN . Acesso em: 22 jun. 2021.

MACIEL, R. *Serviços como Netflix querem usar a IA para criar uma conexão emocional com você,* 2019. Disponível em: encurtador.com.br/aprX4. Acesso em: 22 jun. 2021.

MARTINS, G.M. "O *geopricing* e *geoblocking* e seus efeitos nas relações de consumo", en FRAZÃO, A.; MULHOLLAND, C. (Coords.), *Inteligência Artificial e Direito*: ética, regulação e responsabilidade, Thomson Reuters Brasil, São Paulo, 2019.

MUEHLHAUSER, L.; SALAMON, A. "Intelligence explosion: evidence and import", en EDEN, A. (Ed.) et al. *Singularity hypotheses: a scientific and philosophical assessment*, Springer, Heidelberg, 2012, p. 15-42.

PETEFFI DA SILVA, R. "Antijuridicidade como requisito da responsabilidade civil extracontratual: amplitude conceitual e mecanismos de aferição", *Revista de Direito Civil Contemporâneo*, vol. 18, ano 6, 2019, p. 169-214.

POOLE, D.; MACKWORTH, A. *Artificial Intelligence: Foundations of Computational Agents,* Cambridge University Press, Cambridge (UK), 2010.

SCHERTEL MENDES, L.; DONEDA, D. "Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados", *Revista de Direito do Consumidor*, vol. 120, ano 27, 2018, p. 469-483.

SCHREIBER, A. "Responsabilidade civil da Lei Geral de Proteção de Dados Pessoais", en DONEDA, D.; SARLET, I.W.; MENDES, L.S.; RODRIGUES JUNIOR, O.L.; BIONI, B.R., *Tratado de proteção de dados pessoais,* Forense, Rio de Janeiro, 2021. p. 319-338.

SCHWAB, K. *A Quarta Revolução Industrial*. Trad. Daniel Moreira. Edipro, São Paulo, 2016.

*TARGET: entenda como a loja monitora o comportamento do consumidor.* 2020. Disponível em: https://www.traycorp.com.br/conteudo/target-e-o-comportamento-do-cliente/. Acesso em: 22 jun. 2021.

TEPEDINO, G. "Desafios da Lei Geral de Proteção de Dados (LGPD)", *Revista Brasileira de Direito Civil – RBDCivil,* v. 26, 2020, p. 11-15.

TORRES, C. *A bíblia do marketing digital: tudo o que você precisa saber sobre marketing e publicidade na internet e não tinha a quem perguntar*. Novatac, São Paulo, 2019.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho,* 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em 15 jul. 2021.

VASCONCELLOS E BENJAMIN, A. H. "Da qualidade de produtos e serviços, da prevenção e da reparação dos danos.", em OLIVERA, Juarez., *Comentários ao Código de Proteção do Consumidor,* Saraiva, São Paulo, 1991.

VIEIRA SANSEVERINO, P.T. *Responsabilidade Civil no Código do Consumidor e a Defesa do Fornecedor.* Saraiva, São Paulo, 2010.

WENDEHORST, C. "Strict Liability for AI and other Emerging Technologies", *Journal of European Tort Law*, vol. 11, nº 2, 2020, pp. 150-180. Disponível em: < https://doi.org/10.1515/jetl-2020-0140>. Acesso em: 15 jun. 2021.

WERLANG PAIM, B.; RUTHES GONÇALVES, L. "A responsabilidade civil no tratamento de dados pessoais pelas aplicações de inteligência artificial", en WACHOWICZ, M. (Org.). *Proteção de dados pessoais em perspectiva*: *LGPD e RGPD na ótica do direito comparado*, Gedai, UFPR, Curitiba, 2020, p. 451-480.

ZANATTA, R. *Perfilização, Discriminação e Direitos do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais,* 2019. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais. Acesso em: 22 jun. 2021.