A RESPONSABILIDADE CIVIL APLICADA A AGENTES AUTÔNOMOS DE INTELIGÊNCIA ARTIFICIAL NO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

CIVIL LIABILITY APPLIED TO AUTONOMOUS ARTIFICIAL INTELLIGENCE AGENTS IN THE PROCESSING OF SENSITIVE PERSONAL DATA

Rackel Farias Madeira[1]

Anamaria Sousa Silva[2]

RESUMO: O presente artigo tem como objetivo analisar o tratamento atribuído pela Lei nº 13.709, de 14.8.2018 (Lei Geral de Proteção de Dados), bem como por legislações pátrias correlatas e posições doutrinárias diversas, à responsabilização civil atribuída a agentes autônomos de inteligência artificial (IA) no contexto da proteção de dados pessoais sensíveis. Através de pesquisa bibliográfica e análise documental, buscou-se identificar as lacunas legislativas mais relevantes na disciplina deste tópico, para, posteriormente, suscitar alternativas viáveis a seu preenchimento. Ao final, o estudo demonstrará quais modalidades de responsabilização civil poderão ser adotadas no intuito de contribuir à efetiva salvaguarda dos direitos individuais na era digital.

Palavras-chave: responsabilidade civil; inteligência artificial; sistemas autônomos; dados pessoais sensíveis; Lei Geral de Proteção de Dados (LGPD).

ABSTRACT: The present article aims to analyze the treatment provided by the Brazilian Law No. 13,709, dated August 14, 2018 (General Data Protection Law), as well as related Brazilian legislation and various theories regarding the civil liability assigned to

[1] Graduanda em Direito pela Universidade Federal do Maranhão (UFMA). Lattes: http://lattes.cnpq.br/1892241496943291.

[2] Doutorado em Direito - Cooperação Internacional - pela Universidade de Nagoya - Graduate School of International Development - Japão (2000) - l - revalidado pela Universidade Federal de Santa Catarina. Mestrado na mesma área - Universidade de Nagoya - Graduate School of International Development - Japão (1997), revalidado pela UFSC. Graduação em Direito pela Universidade Federal do Maranhão (1993) Professora visitante da Universidade Federal do Maranhão durante o período de 2001-2003. Professora-bolsista DCR - CNPq - nível 2A - na Universidade Federal do Maranhão durante o período de 2004-2006. Professora adjunta da Universidade Federal do Maranhão (UFMA). Doutora em Direito - Cooperação Internacional pela Universidade de Nagoya - Japão. Lattes: : http://lattes.cnpq.br/7633585207951429.

autonomous agents of artificial intelligence (AI) in the context of sensitive personal data protection. Through bibliographic research and documentary analysis, we sought to identify the most relevant legislative gaps in the regulation of this topic, with the subsequent proposal of viable alternatives for its addressing. In conclusion, this study will demonstrate which forms of civil liability may be adopted to contribute to the effective safeguarding of individual rights in the digital age.

Keywords: civil liability; artificial intelligence; autonomous systems; sensitivedata; Brazilian General Data Protection Law (LGPD).

1 INTRODUÇÃO

O estudo em questão pretende apresentar perspectivas de responsabilização civil de agentes autônomos de inteligência artificial (IA) frente à violação de diretrizes normativas fornecidas pela Lei Geral de Proteção de Dados (LGPD) em relação ao tratamento de dados pessoais sensíveis.

A relevância dessa investigação se perfaz na constatação de que a inteligência artificial constitui uma ferramenta cada vez mais recorrente no dia a dia do cidadão contemporâneo, seja na elaboração de conteúdo personalizado em redes sociais, realização de procedimentos médicos complexos e estabelecimento de padrões que permitem prever a rentabilidade de investimentos ou até mesmo quais localidades possuem maior probabilidade de serem afetadas por mudanças climáticas. Trata-se, portanto, de um advento tecnológico que encontra repercussões nas esferas pública e privada, de forma que cabe à ciência jurídica encontrar mecanismos de regulamentação de tais efeitos.

Dentre as possíveis questões carentes de tutela jurisdicional advindas da utilização da IA por empresas e instituições, pode-se destacar a coleta, o processamento e armazenamento de dados pessoais, vez que o manejo destes é sujeito às diretrizes estabelecidas pela LGPD. De fato, não obstante a referida lei enfatize a importância da adoção de medidas de segurança a fim de garantir a proteção da privacidade dos usuários, o conteúdo fornecido por estes é frequentemente instrumentalizado no intuito de aprimorar a inteligência artificial, incluindo potenciais dados pessoais sensíveis.

Para a finalidade desta pesquisa, serão considerados principalmente os agentes de inteligência artificial que correspondem a modelos de linguagem treinados a partir de grandes conjuntos de dados obtidos online (*large language models*, ou LLMs), como GPT-3, GPT-3.5 e GPT-4, desenvolvidos pelo laboratório de pesquisa OpenAI. Nesse contexto inserem-se os *chatbots* (a exemplo do ChatGPT) e o Auto-GTP, aplicativo que utiliza o sistema GPT-4 no intuito de desempenhar tarefas autônomas, sem necessidade de direcionamento por parte do usuário.

Desta feita, tomando por base as metodologias de pesquisa bibliográfica e análise documental, investigou-se a possibilidade de responsabilização civil do gerenciador de dados pessoais sensíveis a partir de diferentes visões, atribuídas, sobretudo, pela legislação pátria, europeia, projeto de lei em trâmite e posicionamentos doutrinários. Verifica-se que, no que pese o expressivo aumento de publicações nessa seara, restam lacunas normativas no ordenamento brasileiro em respeito à modalidade de responsabilização adotada.

Este estudo discute soluções introduzidas pelas fontes elencadas em diálogo com a LGPD, abordando decisões dos tribunais superiores pertinentes ao ponto, o Regulamento Geral de Proteção de Dados (RGPD), o Projeto de Lei n. 2.338/2023, posicionamentos recentes da Agência Nacional de Proteção de Dados (ANPD) e preceitos avindos das contribuições teóricas de Caitlin Mulholland e Walter Aranha Capanema, dentre outros.

2 AGENTES AUTÔNOMOS DE INTELIGÊNCIA ARTIFICIAL E DADOS PESSOAIS SENSÍVEIS EM FACE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): CONCEITOS FUNDAMENTAIS

Uma das definições mais célebres de inteligência artificial é a proposta por John McCarthy, um dos pioneiros da IA. Para McCarthy (1956), "inteligência artificial é a ciência e a engenharia de fazer máquinas inteligentes, especialmente programas de computador inteligentes". Esse entendimento foi difundido a princípio pelo cientista no artigo *"Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*",

publicado em 1956 e considerado um marco histórico da área por ter sido o primeiro a apresentar formalmente a ideia de que máquinas poderiam ser programadas para imitar a inteligência humana.

Décadas mais tarde, Andrew Ng introduziu uma delimitação mais atual para aprendizado de máquina (*machine learning*): “aprendizado de máquina é o campo de estudo que dá aos computadores a habilidade de aprender sem serem explicitamente programados" (NG, 2017).

Em outras palavras, inteligência artificial é uma área da ciência da computação que se dedica ao estudo e desenvolvimento de algoritmos e sistemas capazes de realizar tarefas que, tradicionalmente, exigem inteligência humana.

Por sua vez, agentes autônomos, segundo o entendimento de RUSSELL e NORVIG (2013, p. 35), são “entidades de software ou hardware que se movem em algum ambiente, percebem o ambiente por meio de sensores, agem no ambiente por meio de atuadores e podem operar sem intervenção humana direta".

Tais agentes utilizam técnicas de inteligência artificial para coletar informações, analisá-las e tomar decisões com base em regras e objetivos pré-definidos. Assim, são capazes de autoaprimoramento ao valer-se de estratégias como aprendizado de máquina, ajustes de algoritmos, avaliação de resultados e análise de dados.

De fato, para os autores supramencionados, “a análise de dados é o coração da inteligência artificial, permitindo que sistemas computacionais aprendam a partir de exemplos e experiências" (*Ibidem*, p. 17). Isso porque os algoritmos de *machine learning* analisam conjuntos de dados a fim de identificar padrões entre as variáveis presentes, a partir dos quais o algoritmo poderá inferir informações e fazer previsões sobre dados inéditos, não utilizados no treinamento do modelo.

Nesse cenário, dados precisam ser coletados, armazenados e processados em grande quantidade e qualidade, fazendo-se necessário que sejam representativos e variados o suficiente para que o modelo possa generalizar suas conclusões e fazer previsões precisas, então gerando novos dados.

Conquanto no contexto normativo brasileiro atual não exista uma lei em vigor que discipline exclusivamente o uso da inteligência artificial, a LGPD pode ser aplicada a algumas questões relacionadas ao seu uso, uma vez que estabelece regras para o tratamento de dados pessoais (incluindo aqueles que possam vir a ser utilizados por sistemas de inteligência artificial), exigindo que empresas obtenham consentimento do titular para coletar e tratar suas informações e que tomem medidas para garantir a segurança de dados.

A definição de dado pessoal consta no artigo 5º, inciso I, da LGPD, que dispõe: "dado pessoal: informação relacionada à pessoa natural identificada ou identificável". Do mesmo modo, comentam BLUM e RABELO (2020, p. 51):

> Dados pessoais são informações relacionadas a uma pessoa natural identificada ou identificável, como nome, endereço, número de telefone, número de CPF, informações de cartão de crédito, dados biométricos, informações de localização, registros de atividades de navegação na internet, informações de saúde, entre outras, desde que essas informações permitam a identificação ou possam tornar identificável a pessoa natural a quem se referem.

Logo, adota-se o entendimento de que dados pessoais são informações relacionadas à pessoa natural identificada ou identificável, direta ou indiretamente, por meio de identificadores como nome, número de identificação, endereço, dados de localização, dentre outros. O tratamento desses dados deverá ser realizado com o consentimento do titular ou em outras situações previstas em lei (conforme o art. 7º, inciso II, LGPD). Para mais, determina que isso ocorra de forma transparente e segura, garantindo a privacidade e proteção dos dados pessoais (art. 6º).

Por outro lado, a mesma lei estabelece, em seu artigo 5º, inciso II, que dados pessoais sensíveis

> [...] são dados pessoais 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.

O conceito é também explorado por NASCIMENTO e PEREIRA (2020, p. 50), que elucidam:

> Dados pessoais sensíveis são aqueles que, em razão de sua natureza, estão associados a maior risco à privacidade ou geram maior impacto à esfera íntima das pessoas, tais como informações sobre saúde, orientação sexual, origem racial, convicções religiosas e filosóficas, dentre outras.

Dados pessoais sensíveis são, portanto, informações que, se indevidamente divulgadas ou utilizadas contra alguém, podem gerar prejuízos significativos a sua vida privada, dignidade e intimidade, sendo de suma importância sua proteção para garantir a autonomia dos titulares. Desta forma, a denominação utilizada ("sensíveis") advém do fato de que se forem manejados de forma imprópria, podem causar graves danos ao cidadão, como discriminação, estigma, exclusão social, perda de oportunidades e violação ao princípio da dignidade da pessoa humana.

Entendimento consonante é o de MUHOLLAND (2021, p. 02):

> Mais importante do que identificar a natureza própria ou conteúdo do dado - conforme o rol do artigo 5º. II, LGPD - é constatar a potencialidade discriminatória no tratamento de dados pessoais. Isto é, a limitação para o tratamento de dados se concretizaria na proibição de seu uso de maneira a gerar uma discriminação, um uso abusivo e não igualitário de dados.

Ilustrativamente, a autora citada narra casos em que o perfilamento (*profiling*) a partir do uso de dados pessoais sensíveis ocasionou tratamento discriminatório. Em um deles, ocorrido nos Estados Unidos,

> [...] algumas seguradoras utilizaram dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez.

Destarte, em face das possibilidades geradas pela utilização prejudicial desses dados pessoais, a LGPD estabelece mecanismos de proteção mais restritivos em relação

a outras modalidades de *data*, exigindo que empresas e organizações adotem medidas técnicas e administrativas adequadas e proporcionais ao risco envolvido.

No caso dos algoritmos autônomos de inteligência artificial, sua capacidade de coletar, armazenar e processar grandes quantidades de dados pessoais sensíveis os torna aptos a cometer violações de segurança, de forma que as medidas disciplinadas pela LGPD se tornam particularmente relevantes nesse contexto.

Tais medidas incluem a adoção de algoritmos de criptografia, o controle de acesso aos dados, a anonimização dos dados pessoais sensíveis e a realização de avaliações de impacto à privacidade, entre outras. Determina, ainda, que as empresas que utilizam inteligências artificiais informem aos titulares de dados como estes serão coletados, tratados e utilizados. Além disso, prevê que esses titulares terão direito a solicitar acesso, correção e exclusão de seus dados pessoais sensíveis coletados e tratados por meio de inteligências artificiais (arts. 6º a 30).

Observa-se, contudo, que, embora a LGPD evidencie a importância da efetiva proteção de dados pessoais sensíveis no contexto das inteligências artificiais, não há menção à imputação de responsabilidade civil a sistemas autônomos de inteligência artificial. A pauta, cuja relevância torna-se incontestável com a evolução exponencial do *machine learning* nos últimos anos, segue carente de regulação do legislador.

3 RESPONSABILIDADE CIVIL E A PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS

Com o avanço da tecnologia e o crescente uso de sistemas automatizados de processamento de dados, como inteligência artificial e *big data*, a responsabilidade civil pelos danos causados ao titular de dados adquire contornos notáveis. No tocante aos dados pessoais sensíveis, o motivo pelo qual essa discussão assume significado primordial possui relação com a natureza das informações compartilhadas, visto que tais dados tratam de elementos confidenciais e privados.

De acordo com DINIZ (2018, p. 36), “A responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responda, por alguma coisa a ela pertencente, ou de simples imposição legal”.

Em outras palavras, a responsabilidade civil é um instituto do direito civil que trata da obrigação legal de reparar os danos causados a terceiros, decorrentes de um ato ilícito. Essa obrigação decorre do princípio de que todo aquele que causa um dano a outrem deve repará-lo, independentemente da existência de culpa, e implica na obrigação de indenizar um terceiro pelos danos que lhe foram causados em decorrência de um comportamento que viole as normas jurídicas ou os princípios éticos. A ação judicial, nesse caso, busca a reparação integral do dano causado, incluindo o ressarcimento dos prejuízos materiais e a compensação pelos danos morais sofridos pela vítima.

No contexto da proteção de dados pessoais, a LGPD estabelece regras claras para a coleta, uso, armazenamento e compartilhamento destes pelas empresas e instituições públicas, atribuindo responsabilidades específicas aos controladores e operadores, que devem adotar medidas técnicas e organizacionais adequadas para proteção dessas informações. Assim, as empresas que tratam dados pessoais são responsáveis pelos danos que causarem, tanto na esfera material quanto moral, decorrentes de falhas de segurança, perda ou vazamento de informações. Isso implica que, em caso de violação, a empresa (ou instituição) pode ser obrigada a indenizar o titular dos dados por danos morais e/ou patrimoniais.

De fato, versa: "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (art. 42).”

Não obstante, a aplicação de multas em caso de descumprimento da LGPD está prevista no art. 52, que fixa a competência da Autoridade Nacional de Proteção de Dados (ANPD) para aplicar sanções administrativas, incluindo advertência, multa simples ou diária, bloqueio dos dados pessoais, eliminação dos dados, suspensão do exercício da

atividade de tratamento de dados pessoais e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Ademais, essa legislação preconiza o direito dos titulares de dados pessoais a solicitar a reparação de danos causados por violações à lei, conforme estabelece o art. 5º, inciso V:

> O tratamento de dados pessoais deve ser realizado de forma transparente e com respeito às liberdades civis, aos direitos humanos e ao desenvolvimento econômico e tecnológico do país, nos termos desta Lei, em outras normas de proteção de dados pessoais e nas diretrizes da autoridade nacional. (...) VI - garantia da transparência no tratamento de dados, mediante informações claras e precisas sobre a realização do tratamento e os respectivos agentes, observados os segredos comercial e industrial.

Para mais, a supracitada lei estabelece a responsabilidade compartilhada entre controladores e operadores de dados pessoais, conforme anuncia o art. 42, parágrafo único: "O disposto no *caput* não exclui a responsabilidade solidária dos agentes de tratamento envolvidos, observados os artigos 23 a 25 desta Lei."

Quanto à natureza da responsabilidade civil decorrente do descumprimento da LGPD em relação a dados pessoais, há um debate em curso na doutrina jurídica. Isso porque, na realidade, a lei se limita a pontuar que “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente” (art. 45).

Nessa ótica, as normas da responsabilidade civil previstas na legislação em comento não possuem aplicação universal, uma vez que a sua incidência pode ser suplantada por normas específicas, tais como as disposições do Código de Defesa do Consumidor.

Justifica CAPANEMA (2020, p. 165):

> A responsabilidade surge do exercício da atividade de proteção de dados que viole a “legislação de proteção de dados”. Por essa expressão, o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. Deve-se aqui fazer uma analogia com o conceito de “legislação tributária” do art. 96 do CTN, para

> incluir não apenas as leis que versem sobre a proteção de dados, mas as normas administrativas regulamentares que serão expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades.

Com efeito, embora a responsabilidade civil esteja regulamentada na Seção III do Capítulo VI da LGPD, denominada "Da Responsabilidade e do Ressarcimento de Danos", verifica-se que não há especificação de qual regime de responsabilidade civil deverá ser adotado.

Conquanto decisões recentes dos tribunais venham demonstrando a tendência do Judiciário de privilegiar a adoção do regime de responsabilização subjetiva, casos que envolvem proteção de dados pessoais vêm suscitando manifestações diversas. Como exemplo, o Acórdão da 27ª Câmara de Direito Privado do TJ/SP apreciou a Apelação Cível nº 1008308-35.2020.8.26.0704 de 16 de novembro de 2021, discutindo a responsabilidade civil por incidente de vazamento de dados pessoais não sensíveis a partir de uma perspectiva inédita, em que o Ministro relator Alfredo Attié, do Tribunal de Justiça do Estado de São Paulo (TJSP), elabora seu voto nos autos da AC 1008308-35.2020.8.26.0704:

> A respeito do regime de responsabilidade civil previsto na LGPD[...], não se trata mais, como antigamente, de aplicação das regras da responsabilidade subjetiva ou objetiva, mas sim do que a doutrina vem definindo como responsabilidade ativa ou proativa, hipótese em que, às empresas não é suficiente o cumprimento dos artigos da lei, mas será necessária a demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. (TJSP; Apelação Cível 1008308-35.2020.8.26.0704; Relator (a): Alfredo Attié; Órgão: 27ª Câmara de Direito Privado; Comarca de São Paulo; Data do Julgamento: 16/11/2021).

A concepção de que se trata de uma responsabilidade especial é reiterada por MORAES e QUEIROZ (2019, p. 113-136), que afirmam:

> Esta responsabilidade especial, à semelhança do que ocorre no Regulamento europeu, está articulada em torno de três noções fundamentais, que devem ser somadas: i) dano, ii) violação da legislação de proteção dos dados por parte do controlador e/ou operador e iii) reparação. Com efeito, o regime demanda que o dano seja resultante de violação da LGPD e que tenha sido causado por um

> agente de tratamento dos dados para então impor a obrigação de ressarcir a parte lesada. [...] A nova lei, porém, introduz, secundando o regulamento europeu, uma mudança profunda em termos de responsabilização. Trata-se da sua união ao conceito de "prestação de contas". Esse novo sistema de responsabilidade, que vem sendo chamado de "responsabilidade ativa" ou "responsabilidade proativa" encontra-se indicada no inciso X do art. 6º, que determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também "demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, "não descumprir a lei, não é mais suficiente".

Infere-se, portanto, que a responsabilidade especial surge em substituição às regras da responsabilidade subjetiva ou objetiva. Neste regime de responsabilidade ativa (ou proativa), as empresas não podem se limitar ao cumprimento do texto legal, mas devem demonstrar a adoção de medidas eficazes que comprovem a observância e o cumprimento das normas de proteção de dados pessoais e sua eficácia. Essa responsabilidade especial está articulada em torno das noções fundamentais de dano, violação da legislação de proteção de dados e reparação.

Tal regime exige que o dano tenha sido resultado da violação da LGPD e causado por um agente de tratamento de dados para impor a obrigação de ressarcir a parte lesada. A legislação nacional introduz, em concordância com a europeia, uma profunda mudança em termos de responsabilização, unindo-a ao conceito de prestação de contas.

Realmente, a legislação de proteção de dados da União Europeia, conhecida como Regulamento Geral de Proteção de Dados (RGPD), estabelece princípios importantes relacionados à responsabilização pela proteção de dados pessoais, sendo os principais artigos que tratam desse assunto os de número 5 e 24.

Destaca-se, por exemplo, o Princípio da Integridade e Confidencialidade (art. 5.1.f), que assevera que "o responsável pelo tratamento deve garantir a segurança dos dados pessoais e protegê-los contra acesso não autorizado ou processamento ilegal". Por sua vez, o art. 24 estabelece a responsabilidade do encarregado pelo tratamento de dados pessoais ao afirmar que o responsável deve garantir que o tratamento conferido a eles esteja em conformidade com os princípios do RGPD, pugnando pela necessidade de programar medidas apropriadas para garantir o cumprimento das obrigações de proteção

de dados, incluindo a condução de avaliações de impacto da proteção de dados quando apropriado, paralelamente à designação de um encarregado de proteção de dados (DPO), quando necessário, e notificar violações de dados às autoridades competentes e às partes afetadas, caso aplicável.

Consequentemente, verifica-se que, para esse sistema de responsabilidade, a mera obediência à lei insuficiente.

Quanto a incidentes envolvendo dados sensíveis, o entendimento doutrinário dominante é de que a responsabilidade possui natureza objetiva (dano moral *in reipsa*). Ressalve-se, em todo caso, a existência de posições doutrinárias que preconizam a não diferenciação no regime de responsabilização por tratamento de dados pessoais, independentemente de serem estes sensíveis ou não. Compartilham dessa posição os juristas Caitlin Mulholland, Danilo Doneda e Rodrigo Gomes.

MULHOLLAND (2021, p. 11) justifica:

> [...] apesar do artigo 5º, II, da LGPD, trazer o conceito de dados sensíveis - exemplificado por um rol não taxativo, frise-se - deve-se considerar que o tratamento de dados que não estejam categorizados na lei como tal pode conduzir a resultados práticos discriminatórios, cujos efeitos a LGPD visa impedir justamente ao reconhecer e tutelar esta categoria de dados sensíveis. Isto é, a categoria de dados sensíveis não deve ser considerada como estruturalmente diversa da categoria de dados não sensíveis, na medida em que tanto uma, quanto outra estão sujeitas à potencialidade de tratamentos discriminatórios e geradores de danos a seus titulares. Sendo assim, não deve haver uma diferenciação de regimes de responsabilidade civil, baseada numa classificação dos dados como sensíveis ou não. Ou seja, o regime de responsabilidade civil adotado pela Lei Geral de Proteção de Dados Pessoais é único, independentemente da natureza do dado tutelado, se sensível ou não, pois a consequência de sua violação - o dano patrimonial ou moral, individual ou coletivo - independerá dessa categorização, devendo ser integralmente reparado.

Efetivamente, o art. 5º, II, da LGPD apresenta um rol não taxativo de dados sensíveis, de sorte que certas modalidades de tratamento de dados que não estão configuradas naquela Lei podem ser objetivo de responsabilização civil caso sua tutela ocasione resultados discriminatórios.

De todo modo, caso fosse adotada a responsabilização objetiva para dados sensíveis, deveria ser comprovado apenas o nexo causal entre a conduta e o dano, uma vez que o dano decorre de risco intrínseco à atividade desenvolvida pelo controlador. Igualmente, haveria necessidade de serem consideradas as implicações gravosas da utilização indevida das informações obtidas.

Com efeito, verifique-se o art. 6º, X, que traduz o princípio a responsabilização e prestação de contas, *in verbis*: "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Para MALDONADO e BLUM (2022),

> [...] é possível sustentar que a regra geral da LGPD é a responsabilidade civil subjetiva, na qual o elemento da culpa deverá ser demonstrado, admitida, em algumas hipóteses específicas, a responsabilidade civil objetiva, de acordo com a natureza da atividade de tratamento de dados pessoais, que realmente possa se enquadrar como atividade de risco.

Tendo em vista as possíveis consequências do manejo irresponsável de dados pessoais sensíveis, certamente que a atividade de tratamento destes se enquadraria em "atividade de risco". Nesse sentido vêm decidindo os tribunais, como se vislumbra no supracitado voto do Ministro relator Alfredo Attié, no qual exemplifica que: "[...] diferentemente seria a hipótese de vazamento de dados sensíveis, estes sim capazes de autorizar a condenação da ré por danos morais *in reipsa*, considerada a natureza dos dados violados".

Para fins deste estudo, compartilha-se da posição doutrinária que preceitua a responsabilização objetiva no contexto do tratamento de dados pessoais sensíveis, haja vista a natureza das informações manejadas.

4 LIMITES E ALCANCES DA PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS POR AGENTES AUTÔNOMOS DE INTELIGÊNCIA ARTIFICIAL

Em face das análises sustentadas até o presente momento, é possível tecer observações acerca de perspectivas de responsabilização civil de agentes autônomos de inteligência artificial. Nessa ótica, faz-se relevante, em princípio, discutir o que tal autonomia poderá significar para o direito.

RUSSEL e NORVIG (2013) explicam:

> A IA é autônoma quando pode tomar decisões sem intervenção humana. A autonomia pode se referir a tarefas específicas ou a um sistema que pode decidir a melhor forma de atingir um objetivo sem intervenção externa. A autonomia completa, em que a IA pode operar sem intervenção humana, é uma meta da pesquisa em IA, mas permanece inalcançável. (p. 11).

No que pese a visão desses pesquisadores, há de se ressaltar que durante os últimos anos verificou-se uma evolução exponencial das pesquisas referentes a IAs, de forma que o aprimoramento de modelos linguagem, como o mais recente de autoria da OpenAI, GPT-4 (Ope23), ensejam o vislumbre de inteligência artificial geral (AGI, ou *artificial general intelligence*), que é a capacidade de um agente inteligente alcançar habilidades cognitivas similares às de um ser humano.

De certo, o artigo "Sparks of Artificial General Intelligence: Early experiments with GPT-4", publicado em março de 2023, apresenta levantamentos baseados em experimentos que indicam uma evolução nesse sentido. Demonstra-se (BUBECK *et al*.):

> Pesquisadores em inteligência artificial (IA) têm desenvolvido e aprimorado grandes modelos de linguagem (LLMs) que apresentam notáveis capacidades em diversas áreas e tarefas, desafiando nossa compreensão de aprendizado e cognição. O mais recente modelo desenvolvido pela OpenAI, o GPT-4, foi treinado utilizando uma escala sem precedentes de poder computacional e dados. Neste artigo, relatamos nossa investigação sobre uma versão inicial do GPT-4, quando ainda estava em desenvolvimento ativo pela OpenAI. Argumentamos que esta versão inicial do GPT-4 faz parte de uma nova coorte de LLMs (junto com o ChatGPT e o PaLM da Google, por exemplo) que exibem uma inteligência mais geral do que os modelos de IA anteriores. Discutimos as crescentes capacidades e implicações desses modelos. Demonstramos que, além de sua maestria na linguagem, o GPT-4 pode resolver tarefas novas e difíceis que abrangem matemática, programação, visão, medicina, direito, psicologia e mais, sem a necessidade de estímulos especiais. Além disso, em todas essas tarefas, o desempenho do GPT-4 é impressionantemente próximo do desempenho humano e frequentemente

> ultrapassa significativamente modelos anteriores, como o ChatGPT. Dada a amplitude e profundidade das capacidades do GPT-4, acreditamos que ele poderia ser razoavelmente considerado uma versão inicial (embora ainda incompleta) de um sistema de inteligência artificial geral (IAG). Em nossa exploração do GPT-4, damos ênfase especial à descoberta de suas limitações e discutimos os desafios futuros para avançar em direção a versões mais profundas e abrangentes do IAG, incluindo a possível necessidade de buscar um novo paradigma que vá além da previsão da próxima palavra. Concluímos com reflexões sobre as influências sociais do recente salto tecnológico e as direções futuras de pesquisa. *(Tradução nossa*).

Partindo de análises similares, o jurista francês BAVAREZ (2023, n.p) prevê:

> O robô de conversação da OpenAI, ChatGPT, está revolucionando o cenário global ao democratizar o acesso à inteligência artificial com uma velocidade de desenvolvimento e disseminação sem precedentes. Apenas quatro meses se passaram entre o seu lançamento e a disponibilização no mercado da versão GPT-4, que já conta com mais de 100 milhões de usuários em todos os continentes. Prevê-se que esta seja substituída pela versão GPT-4.5 a partir de setembro, seguida por uma inteligência artificial integral anunciada para 2025. Esta última poderá não apenas superar a capacidade humana na busca por informações e conhecimento, bem como na produção de conteúdo, mas também rivalizar em termos de raciocínio e inovação.

Tais considerações acerca da autonomia da inteligência artificial importam às ciências jurídicas, visto que a possibilidade de responsabilização civil desses agentes depende da interpretação a eles dada enquanto objeto ou sujeito de direitos.

Para estudiosos que consideram IAs objetos de direito, criados e controlados por seres humanos, esses sistemas não possuem autonomia ou capacidade de tomar decisões independentes, tornando-os inaptos a serem sujeitos de direito. Um exemplo de posição nessa linha de raciocínio é apresentado por DANAHER (2018):

> Deveríamos considerar as IAs como sujeitos legais, mas não como personalidades jurídicas. Não devemos ser tão precoces em conceder aos sistemas de IA a gama completa de direitos legais que normalmente concedemos a pessoas naturais, pois fazê-lo ignoraria as diferenças muito reais e significativas entre seres humanos e sistemas de IA. (*Tradução nossa*).

Por outro lado, abordagens que sustentam que inteligências artificiais devem ser consideradas sujeitos de direito (ou seja, entidades autônomas e capazes de tomar

decisões independentes) alegam que esses agentes possuem uma forma de personalidade jurídica, com direitos e deveres próprios. Esse posicionamento é defendido, por exemplo, por CALO (2017), que leciona:

> Se continuarmos a tratar a IA como mera propriedade, estaremos limitando seu potencial e deixando de abordar as implicações éticas e sociais de seu uso. Precisamos começar a considerar as IAs como entidades que possuem interesses e direitos próprios, e que podem ser responsabilizadas por suas ações. (*Tradução nossa*).

De toda sorte, as atuais teorias de responsabilização civil desses agentes partem da premissa de que se tratam de objetos (e não sujeitos) de direito, podendo ser equiparados a coisas inanimadas, ainda que apresentem certo grau de autonomia. Esse raciocínio decorre, principalmente, da obrigatoriedade de intervenção humana para possibilitar processos de aprendizado a partir dos quais os dados serão manejados, justificando que a responsabilidade seja imputada aos envolvidos, já que tais ações, conforme o exposto, ainda precisam ser guiadas, mesmo que a princípio.

Dito isto, embora não mencione expressamente a IA, o art. 20 da LGPD trata do direito de revisão de decisões baseadas em tratamentos automatizados de dados pessoais ao dispor que "o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais [...]", o que inclui processos resultantes de *machine learning*. A despeito dessa menção, porém, não consta naquela legislação uma caracterização do que se entende por decisões automatizadas, possibilitando que tal terminologia abarque diversos outros cenários.

Para LIMA e SÁ (2020, p. 231),

> A reflexão sobre a discriminação é atual e relevante, pois os sistemas de IA estão sendo utilizados, em muitos países, com os mais diversos objetivos. Exemplo é o policiamento preditivo que, mediante a análise de dados disponíveis, busca prever onde o crime poderá ocorrer. Ocorre que os sistemas de predição e outros sistemas de IA não estão livres de distorções no resultado. Afinal, os dados são inseridos por programadores humanos que, mesmo involuntariamente, podem contaminá-los com seus preconceitos. A LGPD não discrimina as hipóteses em que o processamento totalmente automatizado de dados pode ocorrer. Limita-se a disciplinar o direito à explicação quando a

> decisão automatizada é tomada sem qualquer interferência humana. Assim, o tratamento de dados automatizados submete-se às regras gerais de utilização e tratamento de dados, especialmente aquelas previstas nos arts. 7º e 11.

Com efeito, não obstante as situações descritas encontrem equivalente nas consequências da utilização da inteligência artificial em tempos presentes, o excesso de generalidade com que a norma trata a automatização do processamento de dados poderia criar empecilhos à correta adequação dessas ocorrências ao texto normativo.

Em contrapartida, o recém-introduzido Projeto de Lei n. 2.338/2023 (PL nº 2.338/2023), que visa disciplinar acerca do uso das inteligências artificiais, inclui o direito de revisão de decisões automatizadas, abarcando "não apenas situações nas quais os interesses das pessoas são afetados – como também ocorre na LGPD –, mas também em casos nos quais o uso de sistemas de IA produzam efeitos jurídicos relevantes" (ANDP, 2023). O ponto de sobreposição, assim, reside justamente nos casos em que IAs venham a realizar tratamento de dados pessoais.

Cabe ressaltar que o projeto de lei entende tal responsabilização como princípio do "desenvolvimento, implementação e uso dos sistemas" (BRASIL, 2023), que deverão observar a boa-fé e, dentre outros, a "rastreabilidade das decisões durante o ciclo de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica" e a "prestação de contas, responsabilização e reparação integral de danos" (*Ibidem*).

De fato, a integralidade do Capítulo V, do PL nº 2.338/2023, é dedicada à responsabilidade civil dos agentes de inteligência artificial, associando os danos por estes causados à necessidade de reparação integral "independentemente do grau de autonomia do sistema". Em relação à modalidade de responsabilização aplicada, consta (art. 27):

> § 1º Quando se tratar de sistema de inteligência artificial de alto risco ou de risco excessivo, o fornecedor ou operador respondem objetivamente pelos danos causados, na medida de sua participação no dano.
> § 2º Quando não se tratar de sistema de inteligência artificial de alto risco, a culpa do agente causador do dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima. (p. 19).

Trata-se de uma adaptação da teoria do risco (teoria da responsabilização objetiva), similarmente ao que consta no parágrafo único do art. 927 do Código Civil, que versa: "haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem".

Assim, o PL nº 2.338/2023 preconiza que a natureza da responsabilidade do sistema de inteligência artificial depende de análise prévia da amplitude dos riscos apresentados por sua utilização, podendo ser objetiva ou não. Não o sendo, aplicar-se-á a inversão do ônus da prova em favor da vítima, conclusão que poderia advir do pressuposto de que o usuário é a parte vulnerável na relação, em paralelo ao que ocorre no Direito do Consumidor (arts. 4º c/c 6º, inciso VIII, do Código de Defesa do Consumidor [CDC]).

Quanto às hipóteses de não responsabilização (art. 28),

> Os agentes de inteligência artificial não serão responsabilizados quando:
> I – comprovarem que não colocaram em circulação, empregaram ou tiraram proveito do sistema de inteligência artificial; ou
> II – comprovarem que o dano é decorrente de fato exclusivo da vítima ou de terceiro, assim como de caso fortuito externo. (p. 20).

No tocante às hipóteses de responsabilização civil de sistemas autônomos de inteligência artificial por danos causados no âmbito das relações de consumo, o art. 29 preceitua a aplicação concomitante do CDC e do PL nº 2.338/2023.

Conquanto a atribuição de papel jurídico a tais regras sanaria certas questões relativas à atribuição de responsabilidade a esses agentes por ocasião do manejo de dados pessoais sensíveis, haveria confronto entre as abordagens apresentadas por LGPD (mais geral) e PL (mais específico).

Observe-se, contudo, que o princípio da especialidade se aplica quando mais de uma norma incide sobre o mesmo fato jurídico, tal que a norma especial afasta a incidência de norma geral (*lex specialis derogat legi generali*). No tocante ao regime de

responsabilização, a norma especial em questão (PL) contém os elementos da geral (LGPD), acrescida de pormenores que particularizam o fato.

Destarte, eventual aprovação e implementação das regulações contidas no PL nº 2.338/2023 poderia apresentar uma solução aparente ao problema da lacuna existente nesse âmbito, desde que observadas as diretrizes de proteção de dados preconizadas pela LGPD, desta feita aplicadas aos sistemas de inteligência artificial.

5 CONSIDERAÇÕES FINAIS

Embora a Lei Geral de Proteção de Dados (LGPD) tenha recebido notável contribuição do direito europeu, cabe relembrar que sua temática apenas na última década encontrou as primeiras reverberações no direito positivo nacional, sendo a própria publicação da legislação em comento datada de 14 de agosto de 2018, tendo entrado em vigor em setembro de 2020.

Com o crescimento de aplicações da inteligência artificial no dia a dia do brasileiro, além do consequente aumento do volume de dados manejados, observou-se o surgimento de adventos tecnológicos alheios à criatividade do legislador no momento da elaboração de tais instrumentos normativos, torna-se inevitável, em certa medida, que estes venham a apresentar lacunas, haja vista a impossibilidade de contemplação de aspectos ainda por emergir.

Contudo, em homenagem ao princípio da segurança jurídica, não é razoável que o titular de dados se encontre desprotegido frente a essas mudanças. Ressalte-se que, em se tratando de dados pessoais sensíveis, a vulnerabilidade do titular é especialmente evidenciada pelo conteúdo das informações e os efeitos que sua utilização irresponsável poderia causar.

Baseado nos resultados obtidos através da presente pesquisa e uma vez conceituados os temas congruentes, foram identificadas as principais propostas de responsabilização civil pelo manejo de dados pessoais sensíveis por parte de algoritmos autônomos de inteligência artificial. Argumentou-se em favor da responsabilização

objetiva (adoção da teoria do risco), em consonância com a doutrina majoritária vigente. Discutiu-se a abordagem introduzida pelo PL nº 2.338/2023, posicionando-o enquanto possível instrumento normativo futuro voltado à disciplina do tópico, embora apresente pontos controvertidos em relação à LGPD.

Evidenciou-se, por fim, que a disciplina formal da responsabilização civil dos sistemas supramencionados é não apenas possível, mas imperiosa, e poderia, em certa medida, ser alcançada a partir da adoção conjunta do PL nº 2.338/2023 (caso este venha a se transformar em Lei) e da LGPD, acrescidos de adequações.

REFERÊNCIAS

ALBIANI, Christine. **Responsabilidade Civil e Inteligência artificial**: Quem responde pelos danos causados por robôs inteligentes? Disponível em: https://bit.ly/3AtutOB. Acesso em: 25 abr. 2023.

ANPD. **Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre ouso da Inteligência Artificial**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 08 out. 2023.

BAZZAN, Ana Lucia; LABIDI, Samira. **Agentes autônomos**: uma introdução. Porto Alegre: Sociedade Brasileira de Computação, 2003, p. 17-31.

BAVAREZ, Nicolas. **La révolution ChatGPT**. Disponível em: https://www.lefigaro.fr/vox/societe/nicolas-baverez-la-revolution-chatgpt-20230416. Acesso em: 04 maio. 2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709, de 14 de agosto de 2018.

BRASIL. **Projeto de Lei N° 2338, de 2023.** Disponível em: https://shre.ink/nsFe. Acesso em: 07 out. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2021.

BUBECK, Sébastien *et al*. **Sparks of Artificial General Intelligence**: Early experiments with GPT-4. Disponível em: https://doi.org/10.48550/arXiv.2303.12712. Acesso em: 01 maio 2023.

CALO, Ryan, **Artificial Intelligence Policy**: A Primer and Road map. 07 ago. 2017.Disponível em: https://ssrn.com/abstract=3015350. Acesso em 03 maio 2023.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. In: **Cadernos Jurídicos**, n. 53, p. 163-170, 2020. Disponível em: https://bit.ly/3oRhAv9. Acesso em: 30 abr. 2023.

CHESTERMAN, Simon. Artificial Intelligence and The Limits of Legal Personality. In: **International & Comparative Law Quarterly**, 69(4), 819-844, 2020. Disponível em: https://bit.ly/3LB9ZIU. Acesso em: 30 abr. 2023.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. São Paulo: Saraiva, 2018.

JORDAN, Michael; MITCHELL, Thomas. Machine learning: Trends, perspectives, and prospects. In: **Science**, n. 349, p. 255-260, 2015. Disponível em: https://doi.org/10.1126/science.aaa8415. Acesso em 22 abr. 2023.

LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais: O Direito à Explicação nas Decisões Automatizadas. In: **Revista Brasileira de Direito Civil**. Belo Horizonte, v. 26, p. 227-246, out./dez. 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados Pessoais Comentada. 4 ed. Rio de Janeiro: Revista dos Tribunai, 2022.

MCCARTHY, John. **Proposal for the Dartmouth Summer Research Project on Artificial Intelligence**. Disponível em:https://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf. Acesso em: 23 abr. 2023.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutelada pessoa humana na LGPD. In: **Cadernos Adenauer**, ano XX, vol. 3, 2019.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). In:**Revista de Direitos e Garantias Fundamentais**, v. 19, 2018.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). In: **IBERC**: Instituto Brasileiro de Estudos de Responsabilidade Civil, 2021. Disponível em: https://bit.ly/3nf7DaI. Acesso em: 01 maio 2023.

NASCIMENTO, Juliana Abrusio; PEREIRA, Bianca Dazzi. **Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados**: desafios e perspectivas. Belo Horizonte: D'Plácido, 2020.

NG, Andrew. **Wha tis Machine Learning?** Disponível em: https://www.youtube.com/watch?v=LOuGmwpS01A. Acesso em: 23 abr. 2023.

RUSSELL, Stuart Jonathan; NORVIG, Peter. **Inteligência artificial**. Rio de Janeiro: Elsevier, 2013.

STANCIOLI, Brunello Souza; LOPES, Giovana Figueiredo Peluso. A personificação de agentes autônomos de inteligência artificial. In: **Revista de direito civil contemporâneo**. n. 23, p. 65-93, abr./jun, 2020. Disponível em: https://dspace.mj.gov.br/handle/1/3310. Acesso em 21 abr. 2023.

TJS. **Apelação Cível 1008308-35.2020.8.26.070**. Relator (a): Alfredo Attié; Órgão: 27ª Câmara de Direito Privado; Comarca de São Paulo; Data do Julgamento: 16/11/2021. Disponível em: https://images.jota.info/wp-content/uploads/2022/05/20210000929192.pdf. Acesso em: 26 abr. 2023.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 02 maio 2023.