Introdução

A geração atual tem vivenciado mudanças significativas em relação ao contexto digital, tendo em vista que acompanhou a expansão e popularização de tecnologias. O uso incessante das redes viabilizou a conexão entre pessoas ao redor do mundo e facilitou a captação de dados, organização das informações e a comunicação entre pessoas. Tal mudança representa uma nova maneira de interação entre os povos, em uma espécie de conectividade global, já que as informações são entregues de forma intensa e instantânea.

Com esse contexto, é inegável que a vida na sociedade foi diretamente influenciada por essas tecnologias. Essas tecnologias, inclusive, impulsionam a globalização, facilitando a conexão instantânea entre indivíduos. Essa nova maneira de conviver em sociedade fez com que todos precisassem passar por uma adequação a essa nova forma de interação e convivência em sociedade.

Da mesma maneira que os indivíduos em geral precisaram passar por esse processo de adequação às novas tecnologias, o direito também se preocupa em acompanhar mudanças na sociedade, tendo em vista que possui força normativa para, mas não se limitando, à resolução de conflitos oriundos dessa interação. A Constituição Federal de 1988, por exemplo, foi promulgada em um período em que o contexto do mundo digital se encontrava em processo embrionário, estava em seu início ainda (Fachin; Doré, 2024, p. 187-200).

Com isso, surge a preocupação de que se a atual Constituição é capaz de assegurar os direitos fundamentais dentro do mundo tecnológico, uma vez que é possível afirmar que tais mudanças ocorrem tão rápido que o direito muitas vezes não consegue acompanhar, o que acaba abrindo espaço para conflitos e inseguranças relacionados ao uso dessas tecnologias, como a privacidade mediante à coleta de dados, a liberdade de expressão nas redes sociais. os riscos de discriminações por decisões automatizadas e a responsabilização objetiva quando é um sistema que decide, de forma que se inicia a busca de possíveis ferramentas que possuam capacidade de enfrentar eventuais conflitos.

Ao falar-se de ferramentas que sejam capazes de enfrentar esses conflitos, é essencial tratar sobre a responsabilização dos agentes pelos danos causados. Nesse contexto, surge o conceito de *accountability*. Apesar de antiga, tal palavra não possui uma tradução direta para o português, contudo, traduz-se a ideia central do conceito: de forma implícita, a responsabilização pessoal pelos atos praticados e, de forma explícita, a exigente prontidão para prestação de contas, seja no âmbito público ou privado. Trata-se de responsabilidade, de obrigação e de responsabilização de quem ocupa um cargo a prestar contas segundo os

parâmetros da lei, estando envolvida a possibilidade de ônus, o que seria a pena para o não cumprimento (PINHO; SACRAMENTO, 2009, p. 1345-1346).

A concretização dos direitos fundamentais no contexto digital exige não apenas ferramentas que os protegem e responsabilizam de forma individual, mas também instrumentos capazes de responder aos danos coletivos oriundos da atuação dos sistemas tecnológicos. É diante desse cenário que a tutela coletiva surge como ferramenta fundamental, tendo em vista que permite que lesões de massa, algumas vezes invisíveis em sua individualidade, sejam enfrentadas de forma eficiente.

O processo é coletivo se a relação jurídica é coletiva, é aquele em que se postula um direito coletivo ou se afirma a existência de uma situação jurídica coletiva. A tutela jurisdicional coletiva é a proteção que se confere a uma situação jurídica coletiva ativa ou a efetivação de situações jurídicas (individuais ou coletivas) em face de uma coletividade (DIDIER Jr.; ZANETI Jr., 2014, p. 58).

Dessa maneira, a Constituição federal e o sistema jurídico brasileiro são estimulados a demonstrarem capacidade de enfrentarem esses conflitos em larga escala, especialmente aqueles produzidos por algoritmos e práticas automatizadas que impactam simultaneamente vários indivíduos. Assim, cita-se a tutela coletiva como uma via adequada para lidar com os danos em escala, garantindo a responsabilização e a reparação diante de riscos difusos próprios da sociedade inserida no meio digital.

Entre as tutelas coletivas, há a ação civil pública, que visa justamente a proteção de direitos que atingem a coletividade, e não apenas as partes envolvidas na ação. A ação pública não pode ser proposta por cidadãos, mas apenas por aqueles indicados no art. 5º da Lei n° 7.347/85, além do Ministério Público (art. 129, III, Constituição Federal/88), quais sejam: Defensoria Pública, União, Estados, Distrito Federal, Municípios, autarquias, empresas públicas, fundações ou sociedade de economia mista e associações que cumprirem os requisitos dispostos no artigo mencionado (BSBC Advogados, s.d.).

Entende-se por direitos e interesses coletivos os que têm como titulares as pessoas integrantes de um determinado grupo, categoria ou classe, enquanto os direitos e interesses difusos são os que têm como titulares as pessoas indeterminadas e ligadas por circunstâncias de fato (NORMASLEGAIS, s.d.). Com esses dispositivos, abriu-se a possibilidade de um amplo uso das ações civis públicas para tutela dos interesses coletivos e difusos (ZANATTA, 2020, p. 8). Esse fato é uma das características determinadoras do direito brasileiro, com grandes impactos para debates atuais, como o dos danos algorítmicos. Esses danos possuem a natureza difusa, levando em consideração que muitas vezes são resultados de decisões automatizadas

que afetam simultaneamente muitas pessoas, de maneira que a tutela coletiva assume o papel na recomposição desses danos.

Nesse cenário, o dano algorítmico se manifesta de várias maneiras que vão além de prejuízo financeiro direto, configurando-se, por exemplo, em viés algorítmico, fenômeno que ocorre quando erros sistemáticos nos algoritmos de máquinas produzem resultados injustos ou discriminatórios (IBM, s.d.). O mapeamento de danos e discriminação algorítmica iniciado e mantido por Tarcizio Silva (SILVA, 2023) apresenta uma linha do tempo com os mais diversos casos de danos algoritmos, que inclui desde o ano de 2010, com o caso das câmeras da marca nikon que não entendiam rostos asiáticos, de forma que a câmera apresentava dificuldade em identificar quando uma família asiática estava com os olhos abertos, pois em toda ocasião aparecia uma mensagem na tela questionando "alguém piscou?" e ninguém havia piscado (ROSE, 2010).

O dano algorítmico também pode manifestar-se com a opacidade ou falta de transparência, também nomeado de black box. Um sistema de IA "black box" ou "caixa preta" é uma característica de modelos de IA que apresentam opacidade, ou seja, não se compreende exatamente como o sistema opera internamente (IA RESPONSÁVEL, 2023). Isso torna-se um grande problema pois dificulta a correção de sistemas de aprendizado profundo quando eles reproduzem resultados indesejados, como, por exemplo, um veículo autônomo atropela um pedestre quando esperava-se que ele freasse, a natureza da caixa preta do sistema significa que não é possível rastrear o processo do pensamento do sistema e ver porque ele tomou essa decisão (BLOUIN, 2023). Nesse cenário, a ausência de transparência nos processos desses sistemas compromete a possibilidade de atribuição de responsabilidade, uma vez que torna difícil identificar a origem do erro ou o agente responsável pelo dano.

Em cenário de lesões massivas e responsabilidade opaca geradas pelos sistemas digitais, a resposta jurídica brasileira se consolida no arcabouço da tutela coletiva.

Nos últimos anos, várias ações civis públicas destacaram as disputas acerca da privacidade e da proteção de dados pessoais no Brasil. Em 2015, o Ministério Público Federal do Piauí ingressou com uma ACP contra a Google do Brasil, elaborando uma tese de que a leitura automatizada de mensagens do Gmail constituiria uma prática abusiva, tendo em vista a falta de consentimento informado por parte dos usuários (ZANATTA, 2020, p. 1).

Em 2018, uma outra ACP ganhou repercussão: o Instituto Brasileiro de Defesa do Consumidor (Idec) ajuizou ação contra a ViaQuatro, concessionária da Linha Amarela do metrô de São Paulo. O conflito surgiu por conta do anúncio de uma parceria com outra empresa com sede em Miami (EUA), para o lançamento das Portas Interativas Digitais (PIDs). Essas portas

funcionariam como painel publicitário capaz de realizar análises agregadas das emoções dos passageiros do metrô, a partir da coleta de imagens das câmeras instaladas acima dos painéis, imagens que eram processadas posteriormente e usadas para identificação das emoções das pessoas filmadas, registrando inofrmações como estimativa de idade e sexo. Na visão do Instituto, a conduta da empresa seria ilegal por violar o direito básico do usuário de serviços públicos de proteção de suas informações pessoais, descumprir parâmetros de tratamento de dados biométricos definidos na Lei geral de Proteção de Dados, descumprir o direito básico do consumidor de proteção contra práticas abusivas nos termos do Código de defesa do Consumidor, descumprir o direito constituconal de proteção da imagem, dentre outros. Em setembro do mesmo ano, a Justiça do Estado concedeu a liminar em favor do Instituto e determinou o desligamento das PIDs em toda a Linha Amarela do metrô (ZANATTA, 2020, p. 2-3).

Ao deparar-se com esses casos, é possível concluir que a ação coletiva, ao possibilitar uma reação rápida diante de ameaças sistêmicas com os PIDs, reforça a capacidade do ordenamento de enfrentar conflitos no contexto digital.

Em perspectiva comparada, é possível observar que o tema da responsabilização por danos vem sendo discutido por diversas jurisdições. A União Europeia, por exemplo, considerada a vanguarda no que tange à regulação do uso de IA, possui o AI Act, que estabelece critérios de risco e impõe deveres aos desenvolvedores e operadores, com multas que podem chegar de até 35 milhões de euros ou 7% do faturamento da empresa em caso de descumprimento (EUROPEAN COMMISSION, 2023). O Estados Unidos, por sua vez, apesar da regulação acontecer de maneira mais descentralizada, com cada estado caminhando de forma independente, o país apresentou, no início de 2025, novas diretrizes para IA, como a exigência de que os desenvolvedores dos sistemas mais avançados compartilhem resultados dos testes de segurança, desenvolvimento de padrões, ferramentas e testes para garantir que os sistemas de IA sejam seguros e confiáveis, abordagem da discriminação algorítmica de forma a melhorar a investigação e compreensão dos direitos relacionados à IA, dentre outros (URUPÁ, 2025).

No mês de outubro de 2025, inclusive, a Califórnia se tornou o primeiro estado norte-americano a regulamentar oficialmente os chatbots de companheirismo baseados em IA, a medida estabelece regras para empresas, obrigando-as a implementar protocolos de segurança e mecanismos de proteção específicos para crianças e usuários em situação de vulnerabilidade (IT FORUM, 2025).

Enquanto a *accountability* e a tutela coletiva fornecem mecanismos robustos para a reparação cível e a prevenção administrativa de danos algorítmicos, a discussão sobre a

responsabilidade penal surge como o próximo grande desafio do Direito. A ameaça de sanções penais é vista como um importante elemento de dissuasão que complementa a responsabilidade civil e administrativa.

O direito penal exige, para a responsabilização, a existência de uma conduta humana, voluntária e consciente, que produza um resultado típico, ilícito e culpável (SAPIR, 2025). Contudo, de qual maneira o direito conseguirá atribuir responsabilidade a resultados causados por quem não possui capacidade jurídica? É importante ressaltar que o ordenamento jurídico possui a Lei n° 14.155/2021, que intensificou a punição para crimes cibernéticos, como invasão de dispositivo, furto e estelionato cometidos de forma eletrônica ou pela internet (BRASIL, 2021). Contudo, não há, ainda, nenhuma responsabilização penal acerca dos danos algoritmos, causados pelo uso dos sistemas de IA.

Diante do cenário apresentado, encontra-se uma lacuna normativa relevante, já que os sistemas de IA, apesar de capazes de gerar resultados com potencial lesivo, não possuem personalidade jurídica nem consciência volitiva, elementos indispensáveis à imputação penal. Assim, as condutas danosas decorrentes de decisões automatizadas acabam recaindo em uma zona cinzenta de responsabilização, em que se torna difícil identificar o agente humano efetivamente responsável, seja o programador, o operador ou a própria entidade que utiliza a tecnologia.

Tal ausência de previsão legal específica mostra a necessidade de analisar os fundamentos da responsabilidade penal diante da autonomia crescente dos sistemas de IA, de modo a garantir que o avanço tecnológico não se traduza em uma lacuna de proteção jurídica e de tutela dos bens jurídicos fundamentais.

Referências Bibliográficas

FACHIN, Zulmar Antonio; DORÉ, Nayara Candotti Santana. Direitos fundamentais na era digital. In: ROVER, Aires José; BARRETO JUNIOR, Irineu Francisco; DINIS, Marisa Catarina da Conceição (org.). *Direito, governança e novas tecnologias I*. VII Encontro Virtual do CONPEDI. Florianópolis: CONPEDI, 2024. p. 187-200. Disponível em: https://site.conpedi.org.br/publicacoes/v38r977z/vsd2k7lt/4D5RBA8Xx083QP91.pdf. Acesso em 02 out. 2025.

DIDIER Jr, Fredie; ZANETI Jr, Hermes. Conceito de processo jurisdicional coletivo. *Revista do Ministério Público do Rio de Janeiro (MPRJ)*, n. 53, jul./set. 2014. Disponível em: https://www.mprj.mp.br/documents/20184/2489757/Fredie_Jr___Hermes_Jr.pdf. Acesso em: 02 out. 2025.

BSBC Advogados. Processo judicial in a nutshell – ação popular, ação civil pública e mandado de segurança. Disponível em: https://bsbcadvogados.com.br/acao-popular-acao-civil-publica-e-mandado-de-seguranca/. Acesso em: 02 out. 2025.

ZANATTA, Rafael A. F. *Tutela coletiva e coletivização da proteção de dados pessoais*. In: PALHARES, Felipe (org.). *Temas Atuais de Proteção de Dados Pessoais*. São Paulo: Revista dos Tribunais, 2020. p. 345-374. Disponível em: https://www.researchgate.net/publication/350852661_Tutela_coletiva_e_coletivizacao_da_protecao_de_dados_pessoais. Acesso em: 07 out. 2025.

MAZZEI, Rodrigo. A ação popular e o microssistema da tutela coletiva. In: GOMES JÚNIOR, Luiz Manoel; SANTOS FILHO, Ronaldo Fenelon (coord.). *Ação popular – aspectos relevantes e controvertidos.* São Paulo: RCS, 2006.

PINHO, José Antônio Gomes de; SACRAMENTO, Ana Rita Silva. *Accountability: já podemos traduzi-la para o português?* Revista de Administração Pública – RAP, Rio de Janeiro, v. 43, n. 6, p. 1343-1368, nov./dez. 2009. Disponível em: https://www.scielo.br/j/rap/a/g3xgtqkwFJS93RSnHFTsPDN/?format=pdf&lang=pt. Acesso em: 14 out. 2025.

NORMASLEGAIS. *Interesses Difusos, Coletivos e Individuais Homogêneos*. Disponível em: https://www.normaslegais.com.br/guia/interesses-difusos-coletivos-e-individuais-homogeneos.htm. Acesso em: 14 out. 2025.

EUROPEAN COMMISSION. *Artificial Intelligence Act*. Disponível em: https://artificialintelligenceact.eu/article/99/. Acesso em: 15 out. 2025.

URUPÁ, Marcos. Trump publica novas diretrizes de desenvolvimento de IA nos EUA. *Teletime*, 24 jan. 2025. Disponível em: https://teletime.com.br/24/01/2025/trump-publica-novas-diretrizes-de-desenvolvimento-de-ia-nos-eua/. Acesso em: 15 out. 2025.

IT FORUM. *Califórnia aprova primeira lei dos EUA para regular chatbots de companheirismo com IA*. Disponível em: https://itforum.com.br/noticias/california-aprova-lei-eua-regular-chatbots-ia/. Acesso em: 15 out. 2025.

IBM. *Viés algorítmico*. *In*: IBM Think. [S.l.]: [s.n.], [s.d.]. Disponível em: https://www.ibm.com/br-pt/think/topics/algorithmic-bias. Acesso em: 16 out. 2025.

SILVA, Tarcízio. Danos e Discriminação Algorítmica: mapeamento. *In*: Desvelar. [S.l.]: [s.n.], 2023. Disponível em: https://desvelar.org/casos-de-discriminacao-algoritmica/. Acesso em: 16 out. 2025.

ROSE, Adam. *Are Face-Detection Cameras Racist?* In: *Time Magazine*. Nova York, 22 jan. 2010. Disponível em: https://time.com/archive/6906847/are-face-detection-cameras-racist/. Acesso em: 16 out. 2025.

IA RESPONSÁVEL. *O que são sistemas de IA "black box"?* Blog IA Responsável, 2 set. 2023. Disponível em: https://www.iaresponsavel.com.br/2023/09/02/o-que-sao-sistemas-de-ia-black-box/. Acesso em: 16 out. 2025.

BLOUIN, Lou. *AI's mysterious 'black box' problem, explained.* University of Michigan-Dearborn, 6 mar. 2023. Disponível em: https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained. Acesso em: 16 out. 2025.

BASTOS, Fabrício Rocha. *Do Microssistema da Tutela Coletiva e a Sua Interação com o CPC/2015*. Revista do Ministério Público do Rio de Janeiro, n. 68, abr./jun. 2018. Disponível em: https://www.mprj.mp.br/documents/20184/1242829/Fabricio_Rocha_Bastos.pdf. Acesso em: 16 out. 2025.

SAPIR, Alan. *Quando o algoritmo comete o crime: IA e os limites da responsabilidade penal*. JOTA, 7 jun. 2025. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/quando-o-algoritmo-comete-o-crime. Acesso em: 16 out. 2025.

BRASIL. Lei n. 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. *Diário Oficial da União*, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 16 out. 2025.