1. Introdução.

A cultura de vigilância digital, intensificada pelo uso de tecnologias como o reconhecimento facial, levanta importantes questões sobre privacidade, discriminação e direitos humanos. Este artigo, baseado em uma reflexão histórica e política, examina as falhas dos sistemas de reconhecimento facial nos estádios de futebol, destacando suas implicações para a população negra e a perpetuação de práticas discriminatórias. A partir do ativismo digital e da mobilização do Direito, propomos uma análise crítica dessas tecnologias na modernidade digital.

A implementação de tecnologias de reconhecimento facial em estádios de futebol tem sido amplamente promovida como uma solução para melhorar a segurança e proporcionar maior conforto aos torcedores. No entanto, uma análise mais profunda revela uma série de preocupações relacionadas à privacidade, aos direitos fundamentais, e ao potencial uso indevido dessa tecnologia para a perseguição de grupos historicamente marginalizados.

Assim, no contexto de acessibilidade aos estádios de futebol no Brasil, a tecnologia de reconhecimento facial tem sido apresentada como uma ferramenta eficaz ao garantir maior celeridade e conforto aos torcedores, no momento da entrada, em relação ao sistema de ingressos impressos, já que, exigem impressão de um termo de ciência das regras estabelecidas; assinatura e apresentação desse documento em guichê próprio, além de outros documentos comprobatórios de identificação e condição de meia-entrada para, só então, obter o ingresso definitivo e conseguir acessar o portão próprio com a categoria do ingresso.

Lado outro, tem-se adotado, para além do uso administrativo nos estádios e do respeito ao estatuto do torcedor e do consumidor, o uso desse sistema para fins de segurança pública, com o fim de identificar indivíduos procurados pela justiça sob o argumento do cumprimento de ordem judicial. Os defensores argumentam que a rápida identificação de infratores potenciais pode dissuadir comportamentos violentos e criar um ambiente mais seguro para os torcedores e para a sociedade. No entanto, casos de falhas como no Rio de Janeiro demonstram que a tecnologia pode falhar frequentemente, levantando questões sobre sua confiabilidade e justiça.

Em testes realizados no Rio de Janeiro, a tecnologia de reconhecimento facial apresentou falhas significativas logo nos primeiros dias de implementação. Essas falhas não apenas levantam questões sobre a eficácia da tecnologia, mas também sobre os riscos de falsas identificações e as consequências legais e sociais associadas.

Foucault (2022), em suas análises sobre o poder disciplinar, destaca como as tecnologias de vigilância são frequentemente apresentadas sob o pretexto de promover a ordem e a segurança, mas acabam servindo a interesses de controle social. Da mesma forma, Negri (2020) critica a retórica que cerca a implementação de tecnologias emergentes, alertando para a tendência de atribuir a esses sistemas capacidades que eles efetivamente não possuem, criando uma falsa sensação de segurança e eficiência.

2. Decolonialidade e cultura da vigilância na era digital, aprofundando condutas estigmatizantes.

A vigilância digital moderna, intensificada por tecnologias de reconhecimento facial, é frequentemente justificada como uma ferramenta para aumentar a segurança pública. No entanto, a implementação dessas tecnologias nos estádios de futebol tem mostrado uma série de falhas e vieses raciais, conforme apontado por estudos recentes e reportagens da mídia. Em um teste no Rio de Janeiro, o sistema de reconhecimento facial falhou no segundo dia de operação, levantando questões sobre sua eficácia e precisão.

As falhas desses sistemas não são meramente técnicas, mas refletem problemas mais profundos relacionados ao design e implementação das tecnologias. Algoritmos de reconhecimento facial, quando treinados em conjuntos de dados enviesados, tendem a replicar e amplificar esses vieses. Isso se traduz em taxas mais altas de falsos positivos e negativos para pessoas negras, exacerbando as desigualdades raciais já presentes na sociedade. A falha no Rio de Janeiro é apenas um exemplo de como esses sistemas podem ser ineficazes e prejudiciais quando não são cuidadosamente monitorados e ajustados.

É nesse sentido que, o surgimento de uma nova forma de organização social, tendo por elemento estrutural a informação, trouxe consigo significativos avanços tecnológicos que impulsionaram a economia mundial, tais como o surgimento da internet, da robótica e dos primeiros sistemas de Inteligência Artificial (IA) capazes de simular o raciocínio humano.

Em pouco tempo, a partir do uso de técnicas de aprendizado de máquina (machine learning) e tratamento de dados em massa (big data), foram criados sistemas inteligentes que desenvolveram a capacidade de solucionar problemas com custo menor e eficiência muito maior do que os seres humanos. Isso possibilitou que decisões relevantes, que sempre foram tomadas por indivíduos, fossem totalmente delegadas para os algoritmos dos computadores. Acontece que o uso cada vez crescente dos algoritmos em decisões relevantes subtraiu da sociedade um prévio e necessário debate ético e jurídico em torno do tema. Isso porque, se por um lado a delegação de capacidade decisória às máquinas oferece melhorias significativas para empresas e governos, por outro, pode implicar riscos significativos no que tange à garantia dos direitos humanos e fundamentais das pessoas.

É dentro desse contexto que surge o principal problema das decisões algorítmicas, qual seja, a ocorrência de discriminações, sobretudo contra grupos sociais mais vulneráveis. Tal problema ocorre, basicamente, por dois motivos principais: i) a opacidade, que faz com que muitas vezes nem mesmo os desenvolvedores saibam ao certo as razões pelas quais os algoritmos chegaram às suas conclusões; ii) a qualidade do banco de dados utilizados para "rodar" os algoritmos, que podem trazer consigo vieses implícitos à programação ou adquiri-los posteriormente com a interação em rede, tornando as decisões automatizadas um campo fértil para ocorrência de discriminações.

Nessa direção, o implemento de uma política criminal atuarial, ao se afastar da pesquisa das determinações do crime para ceder lugar à gestão criminal, afronta aos direitos humanos e contribuem para um retrocesso do ponto de vista social.

Quanto à Política criminal, trata-se de uma ligação entre a criminologia e o direito penal, traduzindo a linguagem indutiva, interdisciplinar e empírica da criminologia para os

operadores do direito penal que atuam de forma dedutiva e dogmática. A Política criminal transforma os aportes da criminologia em opções concretas de atuação do direito penal, sendo uma dessas correntes, a política criminal atuarial.

O conceito de política criminal atuarial surge na década dos anos de 1970, nos EUA. Tendo como origens os parole boards (conselhos/comissões para a concessão de livramento condicional) que buscavam critérios mais objetivos para suas atuações. Assim, começa a ganhar espaço, a fim de auxiliar os membros dessas comissões a decidirem quanto ao livramento condicional ou não, um novo modelo baseado em preenchimento de planilhas, checklists e emprego de métodos matemáticos e estatísticos.

Diante do elevado número de reincidência, onde estudiosos chegaram a afirmar que muitos criminosos eram reincidentes necessários, somada à necessidade prática da incidência do princípio da eficiência, surgiu a necessidade de uma nova penologia ("new pelonogy").

A nova penologia não tinha qualquer interesse em punir, intimidar ou reabilitar os indivíduos: seu propósito era apenas o de utilizar a pena criminal de modo sistemático para o controle mais geral de determinados grupos de risco mediante neutralização de seus membros salientes, isto é, a gestão de uma permanente população perigosa, pelo menor preço possível.

Dentro de um breve recorte histórico acerca da persecução dos trabalhadores pelos direitos sociais, cabe destacar que, os direitos humanos têm bases filosóficas em diversas vertentes religiosas, isto é, não há uma predileção por determinada matriz.

As primeiras ideias de direitos individuais são inerentes aos seres humanos por sua natureza humana que cedem esses direitos ao soberano, de acordo com os ideais absolutistas de Thomas Hobbes quem inaugurou as primeiras ideias de direitos individuais dentro do contexto experimentado por esse pensador na época.

Entretanto, John Locke acaba por ser reconhecido como primeiro a inserir a narrativa sobre direitos humanos. Para ele, os direitos do homem eram desvinculados dos direitos do soberano. Muitos desses pensamentos se deram por conta da influência do iluminismo e, assim, rompe-se o paradigma da monarquia e direciona-se em defesa da república.

Embora fosse sabido que os direitos de liberdade defendidos por esse filósofo eram apenas para um determinado grupo, já que, era investidor de empresas escravistas e entusiasta do trabalho de idosos e pessoas doentes.

A aplicação da tecnologia de reconhecimento facial em contextos públicos levanta preocupações sobre seu uso atuarial, no qual indivíduos são vigiados e controlados com base em perfis estatísticos. Esse uso pode resultar em discriminação sistemática contra grupos historicamente marginalizados, que são desproporcionalmente visados pelas forças de segurança. Foucault (2022) argumenta que tais práticas são reflexos de uma biopolítica que visa gerir a população com base em cálculos de risco, reforçando a marginalização de determinados grupos sociais.

Não por outra razão, não se vê a implementação de sistemas de reconhecimento facial para fins de identificação para infratores da legislação tributária ou trabalhista. O que,

dessa forma, demonstra um projeto de aprofundamento na perseguição dos mesmos grupos estigmatizados que já faz parte da clientela desse histórico modelo de segurança pública.

Conforme ensina Dieter, a política criminal atuarial se baseia na predição de riscos e na gestão de comportamentos desviantes com base em dados estatísticos. Essa abordagem frequentemente falha em considerar a individualidade e a complexidade das situações, tratando indivíduos como meros números dentro de um sistema de controle. A aplicação dessa lógica em contextos como os estádios de futebol pode resultar na vigilância excessiva e injusta de torcedores que se enquadram em determinados perfis, perpetuando estigmas e discriminações.

Nilo Batista (2003) complementa essa visão ao destacar que a utilização de tecnologias de reconhecimento facial pode resultar em práticas discriminatórias, especialmente contra minorias raciais e étnicas. Batista (2003) critica a falta de transparência e a ausência de mecanismos eficazes de responsabilização para aqueles que implementam essas tecnologias. Ele enfatiza que a proteção dos direitos fundamentais deve ser uma prioridade, e qualquer uso de tecnologia que comprometa esses direitos deve ser rigorosamente regulamentado e supervisionado.

Em defesa do emprego dessa tecnologia para fins de segurança pública, as secretarias de segurança pública argumentam que a própria Lei Geral de Proteção de Dados (Brasil, 2018) permite o uso de dados pessoais para fins de segurança pública não havendo, dessa forma, qualquer ilegalidade.

Porém, no contraponto dessa política atuarial, consta na Declaração Universal dos Direitos Humanos, a qual o Brasil é signatário, que ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação.

Nessa medida, os artigos contidos na LGPD (Brasil, 2018) acerca do uso de dados pessoais, independentemente de autorização, deveriam ser submetido ao controle de convencionalidade.

Michel Foucault (2022), em suas análises sobre a justiça e as intervenções das forças de ordem, ressalta o caráter discricionário das sanções e o tratamento diferencial dos ilegalismos. Para Foucault (2022), certas práticas que são toleradas em determinadas épocas ou contextos podem ser severamente punidas em outros, dependendo da sensibilidade da sociedade e dos interesses das autoridades vigentes. Isso demonstra como a aplicação de tecnologias de vigilância, como o reconhecimento facial, pode ser utilizada de forma seletiva para reforçar estruturas de poder existentes e marginalizar ainda mais certos grupos sociais.

Foucault (2022) também discute o conceito de sociedades de normalização, onde a lei funciona mais como uma norma reguladora do que como uma imposição jurídica rígida. Nessa perspectiva, o crescente uso de práticas normalizadoras descentraliza o sistema jurídico, favorecendo uma inflação legislativa que busca controlar indivíduos por meio de regulamentações que vão além do alcance judicial tradicional. A implementação de tecnologias de vigilância pode, portanto, ser vista como uma extensão dessas práticas de

controle, visando regular e disciplinar comportamentos desviantes com base em critérios de risco predefinidos.

A perspectiva decolonial propõe uma análise crítica das tecnologias de vigilância, destacando como estas perpetuam hierarquias de poder e discriminação racial. A naturalização da barbárie, agora mediada por aparatos tecnológicos, reflete uma continuidade histórica de práticas opressivas. No Brasil, a transição do período da abolição da escravatura para a República não incorporou a população negra como parte integrante do projeto de Estado-nação, perpetuando exclusões e hierarquias de humanidade (Foucault, 1975).

Historicamente, a vigilância foi utilizada como uma ferramenta de controle sobre corpos negros e indígenas, desde a época da escravidão até os dias atuais. A transição do Brasil Império para a República não alterou fundamentalmente essas dinâmicas de poder, mas as transformou e adaptou às novas realidades socioeconômicas. A utilização de tecnologias de vigilância digital, como o reconhecimento facial, é uma continuação dessas práticas, agora justificadas sob o pretexto de segurança pública e modernidade tecnológica.

2.1. Das conquistas históricas dos direitos humanos às falhas tecnológicas.

Atualmente, as falhas nos sistemas de reconhecimento facial nos estádios de futebol exemplificam os riscos e desafios de confiar nessas tecnologias para segurança pública. Além das questões técnicas, essas falhas levantam preocupações significativas sobre os direitos fundamentais, incluindo o direito à privacidade e à não discriminação. A Lei Geral de Proteção de Dados (LGPD) impõe restrições ao uso de dados pessoais, mas a aplicação prática dessas normas é frequentemente inadequada.

Essas falhas têm implicações diretas para os direitos humanos. Por exemplo, falsas identificações podem levar a prisões injustas e assédio de indivíduos inocentes. Além disso, a falta de transparência na operação desses sistemas pode dificultar a responsabilização e a correção de erros. A LGPD oferece um quadro legal para proteger os dados pessoais, mas a eficácia dessa proteção depende da implementação rigorosa e da fiscalização contínua. A ausência dessas medidas resulta em um ambiente onde os direitos dos indivíduos são frequentemente comprometidos.

Nesse caminho, cabe destacar que, os direitos humanos têm bases filosóficas em diversas vertentes religiosas, isto é, não há uma predileção por determinada matriz. As primeiras ideias de direitos individuais são inerentes aos seres humanos por sua natureza humana que cedem esses direitos ao soberano, de acordo com os ideais absolutistas de Thomas Hobbes quem inaugurou as primeiras ideias de direitos individuais dentro do contexto experimentado por esse pensador na época.

Entretanto, John Locke acaba por ser reconhecido como primeiro a inserir a narrativa sobre direitos humanos. Para ele, os direitos do homem eram desvinculados dos direitos do soberano. Muitos desses pensamentos se deram por conta da influência do iluminismo e, assim, rompe-se o paradigma da monarquia e direciona-se em defesa da república.

Embora fosse sabido que os direitos de liberdade defendidos por esse filósofo eram apenas para um determinado grupo, já que, era investidor de empresas escravistas e entusiasta do trabalho de idosos e pessoas doentes.

Naquele contexto histórico, o diálogo com as elites burguesas eram fundamentais para a realização de transformações daquelas sociedades. Vejamos, por exemplo, que Montesquieu contestava a monarquia do ponto de vista da separação dos poderes, Rousseau do ponto de vista da democracia e Locke, na abordagem dos direitos do homem.

Assim, os fundamentos dos direitos humanos devem, então, ser buscados nos testemunhos, ou seja, nas experiências sociais historicamente situadas. lá foi apontado que a matriz a partir da qual os direitos humanos são reivindicados é o processo de configuração da sociedade moderna, sua economia financeira, a necessidade de conter os abusos que, a partir de seus privilégios, impuseram reis, senhores e religiosos ao trânsito de mercadorias e pessoas e ao livre desenvolvimento de suas consciências (GALLARDO, 2019).

Comerciantes e banqueiros necessitavam que mercadorias e dinheiro fluíssem sem restrições ou com regulações gerais (legislação): exigiram, portanto, liberdade de trânsito e impostos previamente discutidos e aprovados em assembleia por aqueles que deviam pagá-los. Denunciavam, assim, na prática e mediante a configuração de instituições, como ilegítima a autoridade senhorial que expropriava arbitrariamente sua riqueza, lesionava seus trabalhos e que alegava ter um fundamento divino ou natural.

Esse mesmo fundamento divino foi questionado e substituído pela tese do consenso ou contrato social, o que implicava uma autonomia da vontade, até então sujeita à autoridade religiosa.

Para essa livre vontade ideológica, a legitimidade do governo era consequência da adesão ou do consentimento individual de quem seria governado. Uma vez questionado o fundamento divino de reis e senhores, o poder econômico e cultural da igreja (papado) e dos religiosos também foi posto em dúvida contra esta última autoridade e seus privilégios se exigiu (e se lutou com as armas) para obter a liberdade de consciência religiosa e culto, liberdade de consciência sem mais e liberdade de expressão.

2.2. Da reflexão histórica e punitivista na experiencia brasileira com sistema de vigilância.

A reflexão sobre a herança colonial e as práticas punitivas é essencial para entender a perpetuação de discriminações no uso de tecnologias de vigilância. A transição do Brasil Império para a República não incluiu a população negra de forma significativa no novo tecido social, resultando em uma exclusão sistemática que se perpetua até hoje. A vigilância digital moderna, embora apresentada como neutra e objetiva, muitas vezes replica esses padrões históricos de opressão.

As práticas punitivas têm uma longa história de serem usadas para manter as hierarquias sociais e políticas. Durante o período colonial e pós-colonial, o sistema de justiça criminal foi utilizado para controlar e oprimir a população negra e indígena. Na era digital, essas práticas continuam sob a forma de vigilância algorítmica e policiamento preditivo. Essas

tecnologias não são neutras; elas são moldadas pelos mesmos preconceitos e estruturas de poder que influenciam a sociedade em geral.

Dentro desse contexto de discriminação algorítmica (BARROSO; MELLO, 2024), os algoritmos são treinados sobre os dados existentes, que, a seu turno, expressam comportamentos humanos passados e presentes, repletos de vieses e preconceitos, profundamente determinados por circunstâncias históricas, culturais e sociais (HORTA, 2019). Tendem, por tal razão, a reproduzir estruturas sociais atuais e pretéritas de inclusão e exclusão. Nessa medida, dados sobre empregabilidade retratam uma menor contratação de mulheres, negros e indígenas, inclinação esta desprovida de relação com sua capacidade e produtividade, mas que pode induzir à reprodução de comportamentos futuros; dados sobre segurança pública, registram maior propensão à reincidência e violência envolvendo pessoas negras, não necessariamente porque sejam mais violentos, mas eventualmente porque vivem em contextos sociais mais adversos (LARSON, 2016); dados sobre custos com a saúde tendem a superdimensionar os gastos de alguns grupos e minimizar os gastos de outros, por motivos não necessariamente relacionados às suas condições físicas; dados sobre risco de crédito majorarão os riscos e, consequentemente, os custos de financiamento daqueles com menor status econômico e social, mesmo quando tenham logrado aprimorar suas condições, a depender das circunstâncias de coleta dos dados (PASQUALE, 2016). Nessa medida, constata-se que alguns algoritmos de contratação podem tender a descartar mulheres; criminalizar homens negros; dificultar o acesso dos mais pobres ao crédito. Em tais condições, o modo de funcionar da IA pode ser profundamente reforçador de desigualdades existentes, em detrimento dos grupos mais vulneráveis da sociedade (HUQ, 2020, p. 29-34; SILBERG; MANYIKA, 2019, p.3).

Em 2014, (Peron; Alvarez, 2020), o governo do estado de São Paulo anunciou uma parceria com a Microsoft e o Departamento de Polícia de Nova York para importar o sistema de vigilância Detecta, baseado no Domain Awareness System (DAS) de Nova York. O DAS foi desenvolvido após os ataques de 11 de setembro de 2001 como uma resposta ao terrorismo doméstico, com o objetivo de aumentar a capacidade da polícia em antecipar e reagir a ameaças. Caracterizado por câmeras inteligentes integradas a bancos de dados criminais e de imagens, o sistema pode construir modelos estatísticos a partir da mineração de dados públicos e suas interações com plataformas de dados criminais, prevendo padrões de crimes.

Desde a sua adoção, o Detecta causou uma série de falhas operacionais e em 2016, o Tribunal de Contas do Estado de São Paulo (TCE/SP) revelou que o sistema não funcionava bem. As funções de policiamento preditivo eram inexistentes, a integração de dados era frágil, e a quantidade de recursos humanos e tecnológicos disponíveis era insuficiente. Além disso, muitos departamentos policiais não tinham acesso ao sistema e as câmeras não estavam devidamente espalhadas pela cidade, comprometendo o adequado monitoramento.

Assim, a implementação do Detecta em São Paulo pode ser comprovada sob a ótica da governamentalidade e da cultura de controle, conceitos desenvolvidos por Michel Foucault(2022). O sistema introduz um novo regime de visibilidade na cidade, onde câmeras “inteligentes” são usadas para monitorar e controlar o comportamento dos cidadãos. Essa vigilância constante cria uma cultura de controle baseada no medo e na desconfiança, onde a segurança pública é reorganizada para priorizar a prevenção e a

repressão de desvios. A colaboração público-privada nesse contexto exacerba essa dinâmica, com empresas de segurança desempenhando um papel central na implementação e manutenção do sistema.

É nessa direção que, na avaliação do TCE/SP, o Detecta perpetua e intensifica práticas discriminatórias e segregacionais. O sistema, ao incorporar algoritmos de análise de imagem, reforça visões preexistentes e resulta em uma vigilância desproporcional sobre populações marginalizadas, especialmente nas periferias. Os dados revelam um aumento na violência policial e no tráfico de drogas desde a introdução do sistema, enquanto a criminalidade geral teve apenas uma leve redução. Esses resultados sugerem que o Detecta não apenas falha no cumprimento de suas promessas de segurança, mas também agrava a desigualdade social e racial na cidade.

Dentro dessa ordem de ideias, resta cristalino que o Detecta promove uma forma de vigilantismo comunitário, no qual algumas associações de moradores e empresas privadas são incentivadas a participar ativamente da segurança pública. Programas como o Vizinhança Solidária exemplificam essa dinâmica, incentivando os moradores, apenas de determinados bairros da cidade, a instalar câmeras e monitorar suas localidades. Esse envolvimento ativo da comunidade não só reforça a desconfiança, mas também institucionaliza uma cultura de suspeitas e controle social. A participação de empresas privadas na vigilância cria uma rede de segurança que combina interesses públicos e privados, muitas vezes em detrimento das liberdades individuais e dos direitos humanos.

Diante do exposto, a governança da segurança pública em São Paulo, moldada pelo Detecta, revelou uma complexa rede de interações entre agentes públicos, privados e parte da população. Essa rede, organiza-se em torno de uma lógica de prevenção e controle, onde tecnologias de vigilância são usadas para modular a circulação de pessoas e prevenir desvios comportamentais. Essa abordagem tende a legitimar práticas repressivas e excludentes, intensificando a segregação espacial e social. A dependência de tecnologias de vigilância e a colaboração público-privada criam um ambiente onde a segurança é gerida por uma lógica de medo e controle, em detrimento de uma abordagem mais inclusiva e equitativa.

Por fim, a implementação do Detecta em São Paulo, um sistema próprio para atividade de segurança pública, expõe as limitações e contradições de um sistema de vigilância que, embora prometendo eficiência e segurança, acaba por reforçar estruturas de poder e exclusão. A dependência de tecnologias de vigilância e a colaboração público-privada criam um ambiente onde a segurança é gerida por uma lógica de medo e controle, em detrimento de uma abordagem mais inclusiva e equitativa.

2.2 Das responsabilidades cabíveis aos responsáveis pelos danos causados por falhas nos sistemas de reconhecimento facial nos estádios brasileiros

Como exposto, a responsabilidade civil algorítmica é pautada por uma função preventiva e precaucional, que possui o objetivo de inibir atividades potencialmente danosas, em detrimento de uma função estritamente reparatória e/ou sancionadora. Porém, quando as medidas preventivas não são suficientes e há a ocorrência de um dano, surge um direito subjetivo da parte prejudicada obter uma resposta do Estado-Juiz à solução jurídica da sua demanda através das normas legais de responsabilização.

O modelo individualista das teorias subjetivas, exclusivamente apoiadas na culpa como nexo de imputação, mostra-se insuficiente para contemplar a responsabilização por discriminações causadas por algoritmos de IA. O ponto essencial do impasse da teoria subjetiva está no fato de que o estado da arte em termos de inovações tecnológicas torna extremamente difícil a identificação da culpa do agente, notadamente em razão da autonomia e imprevisibilidade das modernas técnicas de machine learning.

Esse impasse nos leva a duas indagações: i) poderíamos condenar o programador/desenvolvedor do algoritmo ou a empresa que adquire a tecnologia mesmo sem a demonstração da culpa de sua parte, ou seja, mesmo que tenha adotado todas as medidas possíveis para minimizar a ocorrência dos danos? ii) caso nenhum dos agentes envolvidos tenha culpa no evento danoso, é justo que uma vítima de discriminação fique sem a devida reparação?

Para responder a tais indagações, imprescindível se analisar o principal fundamento contemporâneo da obrigação de indenizar, que é a existência de um dano injusto. A injustiça do dano pode ocorrer tanto por haver sido injustamente causado por alguém como pelo fato de ser injusto que o suporte quem o sofreu. Assim, instala-se um fundamento para a responsabilidade civil contemporânea, independentemente de culpa de quem quer seja, cuja autossustentabilidade se dá unicamente pela produção do dano injusto em desfavor da vítima, revelando como causa final almejada a concretização dos paradigmas do justo e do equânime.

Nesse diapasão, destaca MULHOLLAND (2019) que a qualificação do dano com sendo injusto afasta de sua análise e interpretação a antes necessária investigação da conduta do agente para a conceituação da responsabilidade civil por meio da noção subjetiva do ato ilícito. Por conseguinte, pela teoria do dano injusto, analisa-se a perspectiva da vítima e não do ofensor, razão pela qual a investigação da culpabilidade perde relevância ante ao próprio dano sofrido e à necessidade de sua reparação integral.

Pode-se dizer, pois, que na estrutura da responsabilidade civil contemporânea, a culpa deixou de ter papel principal e se tornou mera coadjuvante. Por outro lado, o dano deixou de ser coadjuvante e passou a ser protagonista. Destarte, a utilização de um regime de responsabilização fundado na culpa do agente, no que tange, especialmente, às decisões algorítmicas discriminatórias, deve ceder espaço para a necessidade de reparação dos danos injustamente sofridos pelas vítimas, o que torna muito mais coerente a análise da responsabilidade algorítmica a partir das teorias objetivas da responsabilidade.

Sob esta perspectiva, alguns autores identificaram a disciplina da responsabilidade pela guarda do animal ou da coisa (art.936 do CC) como fundamento para a submissão da IA ao regime de responsabilidade objetiva. Sustenta-se, no primeiro caso, a exigência de similar ordem de inteligência e de imprevisibilidade tanto dos animais quanto dos algoritmos de machine learning. Já no paralelo entre com a guarda da coisa inanimada, afirma-se que tanto as coisas quanto os softwares de IA consistem em bens sob custódia de uma pessoa, que deve responder por seus atos.

Cerka et all, citados por TEFFÉ e MEDON (2019), são contrários à equiparação de sistemas inteligentes a animais, diante da falta de bases similares para aproximá-los, já que as atividades de uma IA são baseadas num processo algorítmico que se avizinha mais do processo racional humano do que dos instintos e sentidos dos animais. Assim,

presume-se que uma IA possa vir, de certo modo, a compreender as consequências de suas ações, o que seria uma marca distintiva em relação ao caso dos animais, levando a uma impossibilidade de se adotar um regime de responsabilidade civil objetiva, nos moldes da teoria da guarda de um animal.

Caitlin MULHOLLAND (2019) também rejeita essa tese, ao fundamento de que faltaria o elemento da sujeição do bem ao controle humano para que fosse possível transportar a tese da responsabilidade da guarda do animal ou da coisa para as decisões autônomas tomadas pela IA. Nesse mesmo raciocínio, a Resolução de 16 de fevereiro de 2017 do Parlamento Europeu dispõe que, quanto mais autônomos os robôs são, menos podem ser encarados como simples instrumentos nas mãos de humanos, como as coisas ou os animais.

Destarte, como consequência dessa expansão de estruturas tecnológicas autônomas, a potencialidade e probabilidade danosas serão incrementadas em decorrência da imprevisibilidade dos resultados alcançados pela IA e da inimputabilidade da tecnologia, o que poderia, em tese, afastar a obrigação de indenizar, razão pela qual refuta-se a tese da responsabilidade da guarda do animal ou coisa.

A teoria que parece mais promissora é a da responsabilidade objetiva em razão da atividade de risco pela utilização de sistemas de IA, sobretudo em razão da amplitude das cláusulas previstas nos artigos 927, § único e 942 do Código Civil de 2002. Através destes dispositivos, tanto a empresa desenvolvedora do software quanto aquela que o adquire/utiliza seriam responsáveis solidárias pela reparação do dano em razão do risco criado a terceiros.

Nessa linha, uma das interpretações possíveis do artigo 927, § único, do CC, é a de que, quando o legislador se refere a atividade que, pela sua natureza, implica risco aos direitos de outrem, poder-se-ia interpretar extensivamente o conceito de atividade para qualificar os sistemas de IA como bens perigosos – por gerarem, potencialmente, danos qualitativamente graves e quantitativamente numerosos – como é o caso da discriminação algorítmica. Trata-se da aplicação da teoria do risco criado, que se satisfaz com a constatação objetiva da relação de causalidade entre o risco de uma atividade e o dano injusto, ou seja, independentemente da obtenção de qualquer proveito, diferenciando-se, portanto, da teoria do risco-proveito, que será adiante analisada.

Antes, é importante destacar que o problema da teoria do risco-criado é comum à sua aplicação nos diversos ramos do direito, localizando-se no campo hermenêutico, tendo em vista que o termo "atividade de risco" é um conceito jurídico indeterminado. Diante da plurissignificação do termo, atividade de risco será aquilo que a doutrina e a jurisprudência considerarem como tais, ou seja, na prática, por se tratar de tema ainda pouco comum no cotidiano forense, não há como saber se o intérprete, em determinado caso concreto, irá ou não entender que um sistema de IA se enquadra no conceito de atividade de risco que justifica o reconhecimento da responsabilidade objetiva.

Em que pese a indeterminação prévia do conceito de atividade de risco, a práxis tem demonstrado que delegar capacidade decisória a sistemas autônomo de IA é um risco inerente à atividade e potencialmente apto a gerar discriminações a grupos vulneráveis. A título de exemplo, estudos indicam que os algoritmos de reconhecimento facial e de imagens replicaram estereótipos contra a mulher, anunciaram certas oportunidades de

emprego apenas para homens, traçaram perfis discriminatórios de homossexuais e trataram de forma desigual trabalhadores transgêneros, dentre outros casos de discriminação algorítmica relatados que servem de sustentação à maior potencialidade do risco.

Outra interpretação possível do artigo 927, § único, do CC e que também abrangeria tanto o desenvolvedor do software quanto a empresa que o utiliza é, para SCHREIBER (2019), a teoria do risco-proveito, cujo suporte doutrinário é a noção de que aquele que extrai proveito de certa atividade responda também pelos riscos que ela traz. De acordo com essa teoria, que se fundamenta na máxima "ubi emolumentum, ibi ônus", todos aqueles que auferem lucro/proveito de uma atividade perigosa devem arcar com o ônus decorrente dos danos que causarem.

Outra possibilidade bastante promissora é a identificação da possibilidade de aplicação dos artigos 12 a 17 do CDC para se atribuir responsabilidade objetiva e solidária a todos os integrantes da cadeia de consumo pelos danos decorrentes de fato do produto ou serviço, o que abrangeria os desenvolvedores de software ou algoritmos; aquele que simplesmente fornece o produto (ou qualquer comerciante eventualmente participante da relação de consumo) e os usuários/adquirentes do programa. Nesse caso, ainda que nem todos os casos de discriminação algorítmica se enquadrem numa relação de consumo, haveria a possibilidade de equiparar todas as vítimas da discriminação ao conceito de consumidor, nos termos do artigo 17 do CDC.

Isto posto, considerando a qualificação do dano como injusto e a fundamentação principiológica da solidariedade social, entendemos que a teoria civilista do risco e a da responsabilidade pelo fato do produto e do serviço, que se extrai do CDC, são as teorias mais adequadas para que tanto os desenvolvedores do software quanto o adquirente/usuário da tecnologia e, ainda, qualquer comerciante que aufira lucro com a utilização da IA atividade sejam responsáveis, objetiva e solidariamente, por eventuais danos causados a terceiros.

Quanto à solidariedade entre os agentes empresariais, cumpre destacar que a própria LGPD prevê que os controladores e operadores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente pela reparação, a não ser que comprovem que não realizaram o tratamento de dados, que realizaram de forma regular ou que o dano foi decorrente de culpa exclusiva da vítima (artigo 42, §1º, inciso II c/c artigo 43).

Sendo assim, muito embora, como regra, os agentes responsáveis pela discriminação algorítmica sejam os desenvolvedores do software (aqueles que põem o produto no mercado) e os usuários/adquirentes do programa, e estes estejam em posições jurídicas distintas dos controladores e operadores de que trata a LGPD, a solução do legislador pátrio pode ser utilizada de forma analógica para tratar a questão da reparação da discriminação ou mesmo surgir com uma fonte supletiva para a garantir a responsabilização solidária.

Portanto, transportando as noções de responsabilidade civil do ordenamento jurídico brasileiro para o âmbito das decisões automatizadas, entendemos que a teoria mais adequada para solucionar os casos de discriminação algorítmica é a teoria objetiva, prevista no artigo 927, parágrafo único do CC ou a prevista nos artigos 12 a 17 do CDC.

Já o dever de indenizar deve ser atribuído de forma solidária: i) à empresa desenvolvedor(a) do software; ii) à adquirente/usuária do programa; iii) a qualquer comerciante que participe da relação jurídica, já que todos estes auferem os lucros dessa atividade, também devendo internalizar os riscos e arcar com os eventuais prejuízos. Ademais, em razão da aplicação da LGPD, todos aqueles que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente pela reparação.

Por fim, de forma intencional, deixamos o desenvolvedor de sistemas de fora dessa análise justamente porque a responsabilidade dele é a mais simples de ser verificada. Caso este atue como empresário individual, auferindo os lucros da atividade, a responsabilidade aplicável é a teoria objetiva na posição acima descrita. Por outro lado, quando o programador atua em nome de uma empresa, na qualidade de empregado, o responsável imediato pelo dano é a própria empresa, na qualidade de empregadora. Nesse caso, a responsabilidade da empresa é que é objetiva, nos termos do artigo 932, III e 933 do Código Civil, podendo a empresa mover ação regressiva em face do programador quando este incorrer em dolo ou culpa, nos termos do artigo 934 do Código Civil.

Inicialmente, cabe destacar que os grandes nomes ligados à robótica e à IA têm prognosticado uma linha de evolução que culminará com o que vem já conhecido por pós-humanismo, época em que, como num episódio de Black Mirror, o ser humano deixará de ser biológico e poderá imergir numa realidade virtual, expandindo e projetando sua mente em ambientes digitais. Por outro lado, algumas pesquisas também apontam que muito em breve os sistemas não biológicos passarão a estar aptos para sentir emoções, como no filme Her, de Spike Jonze, que consagra a existência de um sistema operacional capaz de desenvolver sentimentos através das suas interações sociais.

Como vimos no decorrer deste trabalho, as aplicações cotidianas já concebem a existência de máquinas que desempenham funções antes apenas conferida a seres humanos. O desenvolvimento dos sistemas de machine learning tornou os algoritmos capazes de tomar decisões de forma totalmente autônoma a partir de suas próprias interações em rede, o que fez instaurar os debates acerca da possibilidade de atribuição de personalidade – e imputabilidade – à IA, robôs ou softwares como uma alternativa à responsabilização civil tradicional.

Outra alternativa viável apontada pela doutrina seria atribuir uma personalidade autônoma à tecnologia, constituindo-a como um ente ficto, tal qual as pessoas jurídicas, com destinação de patrimônio próprio e atribuição de responsabilidade de indenizar. Ou, ainda, adotar a categoria de entes despersonalizados, tal como ocorre com a massa falida ou o condomínio, o que também poderia servir de sustentáculo para atribuição da obrigação de indenizar à IA.

Nessa ordem de ideias, a adoção de um estatuto jurídico próprio à IA parece ser a tese sustentada pelo Parlamento Europeu, que através da já mencionada Resolução de 16 de fevereiro de 2017, sugeriu aos seus membros a criação de um estatuto jurídico para que ao menos os robôs autônomos mais sofisticados possam ser considerados como “pessoas eletrônicas” ou “e-persons”, responsáveis por sanar quaisquer danos que possam causar e, eventualmente, aplicar essa personalidade eletrônica a casos em que os robôs tomam decisões autônomas ou em que interagem por qualquer outro modo com terceiros de forma independente.

Sérgio Negri (2020) argumenta que a atribuição de responsabilidade civil em casos envolvendo inteligência artificial e robótica deve ser cuidadosamente considerada, evitando a simplificação excessiva de questões complexas. Ele critica a tendência de atribuir personalidade jurídica a robôs, o que pode levar à transferência indevida de responsabilidades de desenvolvedores e operadores para os próprios artefatos tecnológicos.

No mesmo caminho, também destaca a necessidade de reconhecer as particularidades dos diferentes usos de robôs e sistemas de inteligência artificial. Em vez de uma abordagem unitária e abstrata, ele propõe um modelo que leva em conta as diversas áreas de aplicação e os contextos específicos, evitando generalizações que podem resultar em injustiças e irresponsabilidades.

Imperioso informar que, o Projeto de Lei 2338/2023, também conhecido como Lei da Inteligência Artificial, que tramita no Senado Federal Brasileiro, busca o desenvolvimento regulamentar, a implementação e o uso de sistemas de IA no Brasil. A proposta tem como principais objetivos estabelecer direitos para a proteção das pessoas e criar mecanismos de governança, fiscalização e supervisão da IA com o fim de se evitar falhas e, consequentemente, a atribuição de responsabilidade ao causador do dano.

Por fim, o uso da IA deve respeitar os dados individuais das pessoas físicas e jurídicas, sem poder utilizá-los sem consentimento. A vigilância invasiva (invasive surveillance), como reconhecimento facial, biometria e monitoramento de localização deve ter emprego restrito e controlado. E, tendo em vista a vastidão de dados utilizados para alimentar a IA, deve haver mecanismos adequados de segurança contra vazamentos o (BARROSO, LR; MELLO; 2024).

3. Considerações Finais

O presente artigo buscou reflexões sobre a cultura de vigilância digital, exemplificada pelo uso de reconhecimento facial nos estádios de futebol, perpetua discriminações históricas e falha em proteger os direitos fundamentais dos indivíduos. Sendo essencial adotar uma perspectiva crítica e decolonial ao avaliar o impacto dessas tecnologias, reconhecendo seus vieses inerentes e as implicações para a população negra.

Pretende-se promover esse projeto secundário como uma solução para melhorar a segurança e proporcionar maior conforto aos torcedores. Contudo, essa tecnologia levanta preocupações sobre privacidade, direitos fundamentais e a possibilidade de ser utilizada para perseguir grupos marginalizados. Embora possa facilitar o acesso aos estádios, seu uso para segurança pública, como identificação de infratores, tem mostrado falhas significativas, como demonstrado em testes no Rio de Janeiro. Além disso, foi abordado que sistemas de reconhecimento fotográfico e facial, como o Detecta em São

Paulo, que foram desenvolvidos, exclusivamente, para fins de segurança pública, apresentaram falhas grosseiras, gerando, até mesmo, indenizações às vítimas.

Análises de Michel Foucault (2022) e Negri (2020) criticam a tendência de usar essas tecnologias como ferramentas de controle social disfarçadas de segurança, criando uma falsa sensação de eficiência. O sistema Detecta em São Paulo, um exemplo de vigilância pública com câmeras inteligentes e algoritmos, revelou inúmeras falhas operacionais e exacerbou práticas discriminatórias e segregacionais. Dados indicam que, desde sua implementação, conforme PERON e ALVAREZ (2020), houve um aumento na violência policial e no tráfico de drogas, sugerindo que tais tecnologias podem agravar desigualdades sociais e raciais.

Ainda que o Projeto de Lei 2.338/2023, que tramita no Senado Federal Brasileiro tratando a temática, que embasa a defesa da utilização dessas tecnologias nos termos da Lei Geral de Proteção de Dados (LGPD), que permite o uso de dados pessoais para segurança pública, a aplicação deve ser equilibrada com os direitos fundamentais estabelecidos na Declaração Universal dos Direitos Humanos. A implementação dessas tecnologias deve ser rigorosamente regulamentada e supervisionada para evitar abusos e proteger os direitos individuais. Portanto, é crucial reavaliar o uso de reconhecimento facial à luz das falhas observadas e das críticas sobre seus impactos sociais, assegurando que a segurança pública não comprometa a dignidade humana e os direitos fundamentais.

REFERÊNCIAS:

ALBIANI, Christine**. Responsabilidade Civil e Inteligência artificial: Quem responde pelos danos causados por robôs inteligentes?** In: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Editora Revista dos Tribunais, 2019, p.13

ALBUQUERQUER, ANA LUIZA. **Em fase de testes, reconhecimento facial no Rio falha no 2º dia**. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/07/em-fase-de-testes-reconhecimento-facial-no-rio-falha-no-2o-dia.shtml. Acesso em 12 mai. 2024.

BARATTA, Alessandro**. Nuevas Reflexiones sobre el modelo integrado da las Ciencias Penales, la Política Criminal y el Pacto Social.** Montevidéu (Uruguai), 2004.

BARBOSA, Mafalda Miranda**. Inteligência Artificial, E-persons e Direito: desafios e perpectivas.** Revista Jurídica Luso Brasileira, 2017, v.3.n.6. p.1490.

BARROS, Isabela Maria Pereira Paes de; SILVA, Isabela Inês Bernardino de Souza. **Utilização do Reconhecimento Facial Eletrônico por Empresas para identificação de suspeitos: segurança ou violação do estado democrático de direito?** In: Revista Transgressões: Ciências Criminais em debate, Recife, 2019.

BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos**. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol.** Revista Direito e Práxis, Ahead of print, Rio de Janeiro, 2024 Disponível em: link para o artigo. Acesso em 12 jun. 2024 DOI: https://doi.org/10.1590/2179-8966/2024/84479.

BATISTA, Vera Malaguti**. Introdução crítica a criminologia brasileira**. Rio de Janeiro. Revan. 2011.

_____. **Difíceis ganhos fáceis: drogas e juventude pobre no Rio de janeiro**. Rio de Janeiro: Instituto Carioca de criminologia/Revan, 2 ed., 2003.

BRAGA, Carolina. **Discriminação nas decisões por algoritmos: polícia preditiva**. In: FRAZÃO, Ana; MOLHOLLAND, Caitlin (org.). Inteligência Artificial e o Direito: ética regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019, p. 671-693, p. 687.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em 18 mai. 2024.

BRASIL. Lei 7.210 de 11 de julho de 1984**. Lei de Execução Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em 18 mai. 2024.

BRASIL. Lei 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 18 mai. 2024.

BRASIL. Lei 14.597 de 14 de junho de 2023**. Lei Geral do Esporte**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14597.htm. Acesso em 18 mai. 2024.

BRASIL. Senado Federal. **PL 2338/2023**, inciativa Senador Rodrigo Pacheco, relator atual Senador Eduardo Gomes, situação: com a relatoria. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 17 mai. 2024.

CASTRO JÚNIOR, Marco Aurélio de**. Personalidade jurídica do robô e sua efetividade no Direito.** Tese (Doutorado). Universidade Federal da Bahia, Faculdade de Direito, 2009.

Dieter, Maurício Stegemann. **Política Criminal Atuarial: A Criminologia do fim da história.** Tese de Doutorado apresentada na Faculdade de Direito da Universidade Federal do Paraná em 2012.

DONEDA, Danilo; ALMEIDA, Virgílio. **O que é a governança de algoritmos? Politics**., out. 2016. Disponível em: https://politics.org.br/edicoes/o-que-%C3%A9-governan%C3%A7a-de-algoritmos. Acesso em: 12 jun. 2024.

EUBANKS, Virginia. **Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.** New York: St. Martin's Press, 2018.

Fauré, Christiane**. Las declaraciones de los Derechos del Hombre de 1789**. México: Fondo de Cultura Ecnonómica. 1999.

Ferrajoli, Luigi. **Direito e razão : teoria do garantismo penal / Luigi Ferrajoli**. - São Paulo. Editora Revista dos Tribunais, 2002.

Foucault, Michel. **"Alternativas" à prisão: Michel Foucault: um encontro com Jean-Paul Brodeur / Seguido de entrevistas com Tony Ferri e Anthony Amicelle**. Petrópolis, RJ. Editora Vozes. 2022.

Foucault, Michel. **Vigiar e Punir: Nascimento da Prisão.** Petrópolis: Vozes. 1975.

FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Editora Revista dos Tribunais, 2019. p.388 e p.554.

Gallardo, Helio. **Direitos Humanos como movimento social.** Rio de Janeiro. Faculdade Nacional de Direito – UFRJ. 2019.

HORTA, Ricardo Lins. **Por que existem vieses cognitivos na tomada de decisão judicial? A contribuição da psicologia e das neurociências para o debate jurídico**. In: BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos**. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol.** Revista Direito e Práxis, Ahead of print, Rio de Janeiro, 2024 Disponível em: link para o artigo. Acesso em 12 jun. 2024 DOI: https://doi.org/10.1590/2179-8966/2024/84479.

HUQ, Aziz. **Constitutional Rights in the Machine Learning State.** In: BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos**. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol.** Revista Direito e Práxis, Ahead of print, Rio de Janeiro, 2024 Disponível em: link para o artigo. Acesso em 12 jun. 2024 DOI: https://doi.org/10.1590/2179-8966/2024/84479.

LARSON, Jeff et al. **How We Analyzed the Compas Recidivism Algorithm**. In: BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos**. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol.** Revista Direito e Práxis, Ahead of print, Rio de Janeiro, 2024 Disponível em: link para o artigo. Acesso em 12 jun. 2024 DOI: https://doi.org/10.1590/2179-8966/2024/84479.

LUMMERTZ, Henry. **Algoritmos, inteligência artificial e o Oráculo de Delfos**. Disponível em www.jota.info/opiniao-e-analise/artigos/algoritimos-inteligencia-artificial-e-o-oraculo-de-delfos-12102018 – Acesso em maio de 2024.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** São Paulo: Saraiva, 2021.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. **Discriminação algorítmica à luz da lei geral de proteção de dados.** In: DONEDA, Danilo et al (coord). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2020.

MORAIS DA ROSA, Alexandre**. Desejo made in machine? O fascínio da inteligência artificial.** Disponível em https://www.conjur.com.br/2018-nov-16/limite-penal-desejo-made-in-machine-fascinio-inteligencia-artificial – Acesso em 12 jun. 2024.

MULHOLLAND, Caitlin. **Responsabilidade civil e processos decisórios autônomos em sistemas de Inteligência Artificial (IA): autonomia, imputabilidade e responsabilidade**. FRAZÃO, Ana; MOLHOLLAND, Caitlin (org.). Inteligência Artificial e o Direito: ética regulação e responsabilidade. São Paulo: Editora dos Tribunais, 2019. p.335.

ONU, Assembleia Geral da**. Declaração Universal dos Direitos Humanos**. (217 [III] A). Paris. 1948. Disponível em http://www.un.org/en/universal-declaration-human-rights/. Acesso em 26 mai. 2024.

PARLAMENTO EUROPEU. **Resolução do Parlamento Europeu**. de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)).p.04.

PASQUALE, Frank. **The Black BoX Society: The Secret Algorithms That Control Money and Information.** In: BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos**. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol.** Revista Direito e Práxis, Ahead of print, Rio de Janeiro, 2024 Disponível em: link para o artigo. Acesso em 12 jun. 2024 DOI: https://doi.org/10.1590/2179-8966/2024/84479.

PERON, Alcides; ALVAREZ, Marcos César. **O sistema detecta em São Paulo e o papel do vigilantismo nas práticas de segurança da cidade.** In: BRITO CRUZ, Francisco; FRAGOSO, Nathalie (eds.). Direitos fundamentais e processo penal na era digital. São Paulo: InternetLab. 2020, v. 3. p. 160.

Negri, Sergio Marcos Carvalho Avila. **Robôs como pessoas: a personalidade eletrônica na Robótica e na inteligência artificial**. Pensar - Revista de Ciências Jurídicas. 2020.

TARTUCE, Flávio. **Teoria do risco concorrente na responsabilidade objetiva**. Tese (Doutorado). Universidade de São Paulo, São Paulo, 2010. p.335.

TEFFÉ, Chiara Spadaccini; MEDON, Filipe. **Responsabilidade civil e regulação de novas Tecnologias: questões acerca da utilização de Inteligência artificial na tomada de decisões empresariais**. Revista Estudos Institucionais, v. 6, n. 1, jan./abr. 2020. p. 301-333.

TEFFÉ, Chiara Spadaccini; MEDON, Filipe. **A utilização de inteligência artificial em decisões empresariais: notas introdutórias acerca da responsabilidade civil dos administradores**. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). Inteligência

artificial e direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais, 2019.

TEFFÉ, Chiara Spadaccini. Quem responde pelos danos causados pela IA? Jota, publicado em 24 de outubro de 2017. Disponível em https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/quem-responde-pelos-danos-causados-pela-ia-24102017. Acesso em 24.05.2024.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia**. Inteligência Artificial e elementos da responsabilidade civil**. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais, 2019.p.303.

TEPEDINO, Gustavo. **A evolução da responsabilidade civil no direito brasileiro e suas controvérsias na atividade estatal. Temas de direito civil**. Rio de Janeiro: Renovar, 2004, p.191-216.

SCHPREJER, Isabel. **UM CLOSE NO RECONHECIMENTO FOTOGRÁFICO: DADOS, PRÁTICAS E TESES.** In: BRITO CRUZ, Francisco; FRAGOSO, Nathalie (eds.). Direitos fundamentais e processo penal na era digital. São Paulo: InternetLab. 2021, v. 5. p. 206.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil: da erosão dos filtros da reparação à diluição dos danos**. 6. ed. São Paulo: Atlas, 2015. p. 29.

SILBERG, Jake; MANYIKA, James. **Notes from the AI Frontier: Tackling Bias in AI (and in Humans).** In: BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos**. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol.** Revista Direito e Práxis, Ahead of print, Rio de Janeiro, 2024 Disponível em: link para o artigo. Acesso em 12 jun. 2024 DOI: https://doi.org/10.1590/2179-8966/2024/84479.

STOLZE, Pablo; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil: Responsabilidade Civil.** 11. ed. São Paulo: Saraiva. 2013.

USTÁRROZ, Daniel. **Responsabilidade Civil por ato lícito**. São Paulo: Atlas, 2014. p. 113.

VLADECK, David C. **Machines without principals: liability rules and artificial intelligence.** Washington Law Review, v.89, n.1, mar.2014.

ZAFFARONI, Eugenio Raúl. **Criminología: aproximación desde un margen**. v.I. Bogotá: Editorial Temis, 1988. p. 244

ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito Penal Brasileiro: Teoria Geral do Direito Penal.** v. 1. 3. ed. Rio de Janeiro: Revan, 2003.