Revista: Diké Revista Jurídica

eISSN 2595-1742

Conduta típica e inteligência artificial: o desvalor objetivo da conduta nas lesões intermediadas pela *ia*

Lucas Gabriel Santos Costa[1]

Patrícia Ferreira Moreira Argôlo[2]

RESUMO: O objeto do presente estudo é o alcance da proibição penal nas lesões intermediadas pela *Inteligência Artificial*. O objetivo da pesquisa é analisar criticamente, por meio compreensão do risco permitido, o *desvalor* objetivo da conduta penalmente típica dos intervenientes nos fatos perigosos realizados por meio de *IA* nas *redes sociais*. Nesse sentido, considera as *redes sociais* como instrumento de realização da personalidade e a *IA* como ferramenta adequada ao desenvolvimento social em ambiente virtual. Um desenvolvimento que se estabelece no espaço de construção democrática que tem o direito penal como instrumento de controle e contramotivação de lesões e perigo de lesões a bens indispensáveis ao livre desenvolvimento das pessoas. O estudo será realizado por uma abordagem dedutiva, por meio de pesquisa bibliográfica e jurisprudencial, ressaltando a crítica social. Ao final, o estudo propõe que a sobreposição ao risco excessivo seja o conteúdo do desvalor objetivo da conduta nas lesões intermediadas pelo uso de *IA.*

Palavras-chave: Direito Penal; Inteligência Artificial; Redes Sociais; Conduta Típica; Imputação Objetiva.

ABSTRACT: The object of the present study is the scope of criminal prohibition in harms mediated by Artificial Intelligence. The research aims to critically analyze, through the understanding of permissible risk, the objective disvalue of the criminally typical conduct of interveners in dangerous acts carried out through *AI* on *social networks*. In this sense, it considers social networks as instruments for the realization of personality and *AI* as an appropriate tool for social development in a virtual environment. This development occurs within the framework of democratic construction, where criminal law serves as an instrument of control and counter-motivation against harm and risks of harm to assets indispensable for the free development of individuals. The study will be conducted using a deductive approach through bibliographic and case law research, emphasizing social critique. Finally, the study proposes that the excess risk overreach should constitute the objective disvalue of conduct in harms mediated by the use of *AI.*

Keywords: Criminal Law; Artificial Intelligence; Social Networks; Typical Conduct; Objective Imputation.

[1] Professor de Direito Penal e Direito Processual Penal da Universidade Estadual de Santa Cruz - UESC. Doutor em Direito pela Universidade Federal da Bahia. Mestre em Direito Público pela Universidade Federal da Bahia. Especialista em Ciências Criminais pela Fundação Faculdade de Direito da Universidade Federal da Bahia. Atualmente realiza estudos pós-doutorais no Programa de Pós-graduação em Direito da Universidade Federal da Bahia. Líder do Grupo de Pesquisa Crítica Social e Sistema Penal (CRISIS/UESC).

[2] Granduanda em Direito pela Universidade Estadual de Santa Cruz - UESC. Monitora em Direito Penal pela Universidade Estadual de Santa Cruz. Pesquisadora do Grupo de Pesquisa Crítica Social e Sistema Penal (CRISIS/UESC).

eISSN 2595-1742

1 INTRODUÇÃO

Este estudo tem como *objeto* a relação entre o direito penal, no espaço de proibição do tipo objetivo, e as novas tecnologias: especificamente, lança o olhar sobre o alcance da proibição penal nas lesões intermediadas pela *Inteligência Artificial*. O *objetivo*, nesse sentido, é analisar criticamente o *desvalor* objetivo da conduta penalmente típica dos agentes que contribuem para fatos perigosos e, eventualmente lesivos, conduzidos pela intervenção de *IA* nas *redes sociais*.

O estudo compreende que as novas ou renovadas tecnologias que se apresentam no espaço de construção social são instrumentos, para além de adequados, necessários à manutenção e ao desenvolvimento da estrutura social atual. São instrumentos que potencializam a capacidade e o alcance da ação humana em *âmbitos de competência* comuns da realização social. O uso da *IA* está presente na administração da saúde, na gestão do mercado financeiro, no comercio local e internacional, no direito, bem como na expansão das formas e do conteúdo de realização da personalidade humana por meio das *redes sociais*. É nesse espaço que o estudo encontra a sua fundamentação e *justificativa*.

É nesse contexto que este estudo tem a finalidade de analisar o alcance do Direito Penal, compreendendo o primeiro nível normativo de imputação do tipo objetivo (nível da conduta) nos fatos lesivos consequentes da interação com sistemas de *Inteligência Artificial*. A partir daí, toma-se a estrutura normativa do delito, observado a dogmática jurídico-penal e a teoria geral do crime, como ponto de partida para verificar ao nível do tipo penal, especificamente no âmbito da conduta, critérios de aferição objetiva do perigo proibido.

Nesse contexto, o estudo apresenta no segundo capítulo pontos de partida conceituais e circunstanciais do objeto de análise e do contexto social em que se desenvolvem as novas e renovadas tecnologias. No terceiro capítulo, abre espaço para a discussão sobre a regulação nos novos espaços (espaços virtualizados) de realização da personalidade. No quarto e quinto capítulos, analisa o risco criado nas redes sociais com referência nos tipos, apresentando a base normativa que serve de parâmetro para a permissividade do comportamento. Por fim, o último capítulo desenvolve a crítica sobre a reprovação objetiva do comportamento por meio da valoração do perigo juridicamente proibido criado.

O artigo se desenvolve com o *método* dedutivo, tem natureza exploratória e abordagem qualitativa. Foi construído por meio da revisão de literatura específica sobre os

eISSN 2595-1742

elementos normativos que compreendem o delito, bem como a partir da crítica legal e doutrinária sobre os parâmetros que circunstanciam as relações e, consequentemente, os riscos decorrentes da presença e do desenvolvimento das novas tecnologias, especificamente no espaço das redes sociais.

O trabalho analisa um modelo teórico de conduta arriscada sob o viés da dogmática jurídico-penal, observando o risco como um critério normativo de imputação objetiva da conduta. O estudo expõe as circunstâncias que caracterizam a permissividade social das atividades essencialmente perigosas. O intuito é compreender os parâmetros dogmáticos de imputação objetiva para determinação do comportamento proibido decorrente do uso dos sistemas de IA.

2 DESENVOLVIMENTO TECNOLÓGICO, REDES SOCIAIS E A INTELIGÊNCIA ARTIFICIAL

A sociedade digital do início do século XXI apresenta peculiaridades distintas em relação às sociedades dos séculos passados. Hoje, lidamos com uma vasta gama de dispositivos tecnológicos, dependendo diariamente de chips, smartphones, comandos à distância, computadores e do acesso à internet. São circunstâncias que caracterizam as novas formas de viver em uma sociedade.

Nos últimos anos, o conceito de redes sociais tem sido amplamente utilizado com maior intensidade e pluralidade, especialmente no contexto da análise dos agrupamentos sociais em ambientes digitais. Esse fenômeno se intensificou à medida que os rastros e interações desses grupos tornaram-se mais visíveis no espaço virtual, suscitando um renovado interesse por essa abordagem analítica. O surgimento das redes sociais, como categoria de análise, está intrinsecamente associado às mudanças estruturais ocorridas no âmbito da Sociedade da Informação, Comunicação e Conhecimento.

Conforme Castro (2007), no contexto da matemática e da física, uma rede é compreendida como um conjunto de elementos, denominados vértices ou nós, interligados por conexões, que são as arestas. No âmbito social, o conceito de rede social difere, sob esse viés Marteletto (2001) descreve uma rede social como um conjunto de participantes autônomos que se unem em torno de ideias e recursos, baseando-se em valores e interesses compartilhados. Nesse sentido, as redes sociais podem ser definidas como uma interconexão de indivíduos, grupos, organizações ou até mesmo grandes estruturas sociais, como nações, que se relacionam

eISSN 2595-1742

por meio de laços de interdependência e interação recíproca. Uma perspectiva sobre o *ciberespaço* eleva a crítica sobre o ambiente de análise neste estudo:

> O ciberespaço é para as relações sociais, nesse sentido, tão real quanto o *meatspace* (que é um termo utilizado para se referir ao espaço físico em contraste com o ciberespaço (Fielding, s.f.)). E todos os comportamentos socialmente identificáveis que não requerem um contato físico direto podem ser realizados nele da mesma forma que no espaço físico; isso se refere apenas ao aspecto qualitativo, pois, no aspecto quantitativo, o ciberespaço também potencializa a capacidade das pessoas para o contato social ao derrubar as barreiras do espaço físico. (LLINARES, 2018 P. 58-59)

Sob uma perspectiva comparativa, as redes sociais assemelham-se às redes biológicas no que tange à lógica de trocas; contudo, diferem substancialmente na natureza de seu conteúdo. Enquanto as redes biológicas se fundamentam em trocas de matéria, as redes sociais virtuais operam com a disseminação de informações, ideias e conhecimentos, constituindo-se como um espaço de circulação simbólica e intelectual.

A *Inteligência Artificial*, nesse contexto, enquanto instrumento e produto da Ciência da Computação, visa a concepção de sistemas capazes de replicar comportamentos ou processos cognitivos tipicamente associados à inteligência humana. Pode ser um instrumento voltado à execução de operações comparáveis às realizáveis pela mente humana, como por exemplo, a aprendizagem, o reconhecimento e o raciocínio lógico. No Brasil, por meio de uma perspectiva político-institucional, o Projeto de Lei 2338 de 2023 propõe uma definição de *IA* como:

> Sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real. (BRASIL, 2023, PL2338)

Trata-se de uma agência de campo de estudo de abrangência multidisciplinar, interligando-se com diversas esferas do saber, tais como psicologia, biologia, lógica matemática, linguística, engenharia e filosofia, entre outras, dado o caráter complexo e multifacetado das interações que busca simular e compreender.

Nesse sentido, por meio da denominação de Inteligência Artificial existe uma infinidade de técnicas avançadas de processamento matemático de informações. Vale destacar a gestão de grandes volumes de dados, bem como as técnicas de *Data Mnning*, que possibilita a verificação de padrões e o detalhamento de um grande volume de dados, o que facilita a tomada de decisões; a *Machine Learning*, que tem como finalidade a aprendizagem de máquina por meio da incorporação de informações atualizadas do meio.

eISSN 2595-1742

Observa-se, nesse contexto, também os *Processos de Linguagem Natural* (PLN) que tem a finalidade de potencializar as máquinas com a linguagem natural, possibilitando o reconhecimento da voz e a oferta de respostas aos comandos humanos e avança para alcançar:

> [...]Por exemplo, as emoções que uma pessoa experimenta a partir do reconhecimento facial. Desde então, os avanços das novas tecnologias têm impulsionado a evolução dessas técnicas, não tanto conceitualmente, mas na capacidade de processamento, dando origem a novas metodologias mais avançadas baseadas na ideia de automação, como o *Deep Learning* (Aprendizado Profundo) ou as Redes Neurais Artificiais. [Tradução nossa] (LLINARES, 2028 p. 91)

A *IA* busca a adaptação, o reconhecimento e a replicação de capacidades humanas. Existem dois aspectos fundamentais que vão determinar o potencial de alcance da IA "Tanto das que já existem quanto das que poderiam ser criadas virtualmente no futuro: (1) sua capacidade de executar um maior ou menor leque de instruções, e (2) o grau de autonomia com o qual as executa em relação à influência do ser humano."[3] [Tradução Nossa] (LLINARES, p. 92) Vale ressaltar, no entanto, que na atualidade é o ser humano quem determina a situação concreta do uso da IA, considerando o processo de aprendizagem de máquina.

Gimenez (2019, P.795), considerando a classificação de Stuart Russell y Peter Norvig descreve a presença de quatro tipos de sistemas de IA: i. sistemas que imitam o pensamento humano, sendo capazes de aprender, tomar decisões autônomas e resolver problemas; ii. sistemas que atuam como humanos, a partir da imitação do comportamento; iii. sistemas que buscam utilizar o pensamento lógico racional humano, com a capacidade de buscar soluções a partir de uma informação prática; e iv. IA que buscam imitar a estrutura racional do comportamento humano, são os sistemas inteligentes mais desenvolvidos.

Cozman, Plonski e Neri (2021, p. 23) descrevem que os "[...] programas representam e raciocinam sobre conhecimento e crenças, tomam decisões e aprendem, e interagem com seu ambiente, realizando todas essas atividades ou pelo menos algumas com nível alto de sofisticação." Casabona (2023) analisa que a grande revolução da IA está para chegar com o desenvolvimento dos sistemas inteligentes autônomos que, a partir da inferência da informação tomada em seu entorno, são capazes de aprender por si mesmos. Para ele, a partir dessa aprendizagem pode tomar decisões (*deep learning* y *machine learning*), realizando-se como sistemas autônomos:

> São sistemas que aprendem, se propõem a objetivos e constroem planos para alcança-los para além das funções específicas para que foram programados por seus projetistas. [...] existe de forma paralela e crescente o temos sobre o poder destrutivo

[3] "Tanto las que ya existen como las que podrían ser creadas virtualmente en el futuro: (1) su capacidad para ejecutar una mayor o menor gama de instrucciones, y (2) el grado de autonomía con el que las ejecuta en relación con la influencia del ser humano."

eISSN 2595-1742

> que esses artifícios poderiam chegar, que poderiam alcançar o seu próprio criador, o ser humano (CASABONA, 2023 p. 58).

O desenvolvimento dos sistemas informatizados produz desafios aos instrumentos de controle social e especialmente ao direito penal. Desafios que alcançam maior grau de complexidade quando a regulação penal se debruça sobre os fatos que decorrem do uso da *IA* no ciberespaço qualificado pelas redes sociais. Considerando aqui os agentes (sentido lato) que intervém no processo de construção, desenvolvimento e uso da IA, como fornecedores, "quem desenvolve um sistema de inteligência artificial, diretamente ou por encomenda, com vistas a sua colocação no mercado ou a sua aplicação em serviço por ela fornecido, sob seu próprio nome ou marca, a título oneroso ou gratuito" e/ou operador, aquele "que empregue ou utilize, em seu nome ou benefício, sistema de inteligência artificial, salvo se o referido sistema for utilizado no âmbito de uma atividade pessoal de caráter não profissional" da IA (BRASIL, 2023, PL2338).

O problema dessa pesquisa se coloca especialmente ao nível do progresso de desenvolvimento das redes sociais com a interação com a *inteligência artificial*: sendo a *IA* um instrumento para o desenvolvimento da ação humana, é necessário compreender o fundamento e a estrutura de valoração penal do comportamento das pessoas que mantém alguma forma de supervisão ou controle sobre os sistemas informatizados.

3 POLÍTICAS DE INTEGRIDADE: ABERTURA E MANUTENÇÃO DOS ESPAÇOS SOCIAIS EM REDE

O termo *Big Techs* surgiu nos Estados Unidos e não possui uma definição rígida ou única. Ele é usado para identificar as empresas de tecnologia mais influentes, com ampla participação em seus respectivos setores. Segundo Maracine, Voican e Scarlat (2020), as chamadas "Big Techs" se destacam globalmente por sua superioridade no desenvolvimento e aplicação de tecnologias digitais. Essas empresas atuam como líderes em serviços online, abrangendo redes sociais, motores de busca, e o fornecimento de plataformas tecnológicas.

Tais plataformas não apenas armazenam e processam grandes volumes de dados, mas também viabilizam a oferta de produtos e serviços por outras empresas, configurando um modelo de atuação que atende tanto ao consumidor final quanto a parceiros comerciais. Com sua posição dominante no mercado global, essas corporações oferecem serviços essenciais que moldam e sustentam a vida moderna. As *Big Techs* possuem uma relação estratégica com a *Big*

eISSN 2595-1742

Data, que pode ser entendida como o uso de grandes volumes de dados, com variações significativas, que exigem processamento rápido. Esse processo é crucial para transformar dados brutos em informações relevantes, que podem ser analisadas para oferecer maior visibilidade e apoiar decisões estratégicas (MACHADO, 2018).

Dessa forma, a *Big Data* se torna um elemento essencial nos modelos de negócios dessas empresas. Elas utilizam a coleta massiva de dados como uma ferramenta estratégica para reforçar sua liderança no mercado global, promover inovações e criar experiências personalizadas para os usuários. Por meio de plataformas como redes sociais, motores de busca e *marketplaces*, essas empresas recolhem, processam e analisam grandes quantidades de informações sobre os comportamentos e preferências dos consumidores. Essa análise detalhada de dados permite que as empresas ajustem seus produtos, identifiquem tendências e otimizem suas ofertas:

> Alguns segmentos de mercado são mais afetados que outros, especialmente no tocante à aplicação dos princípios da neutralidade, da liberdade de expressão e da privacidade dos dados dos internautas brasileiros. Entre eles temos: telecomunicações, provedores de internet, provedores de aplicações em geral (seja do internet banking ao aplicativo de táxi), portais de conteúdo, mídias sociais, empresas que fornecem serviços de *cloud computing*, empresas que fornecem serviços para monitoração da navegação do usuário e geração de métricas para marketing digital, empresas que fazem uso de Big Data para realizar enriquecimento de bases de dados (PECK, 2021, P. 58).

Além disso, empregam modelos de negócios diversificados, incluindo publicidade, assinaturas e a venda de dispositivos, visando estabilidade econômica. O constante investimento em pesquisa e desenvolvimento assegura sua liderança tecnológica, enquanto sua capacidade de expansão global permite atingir bilhões de usuários, consolidando sua relevância no cenário contemporâneo. As redes sociais também operam espaços de *marketplaces*, que, conforme descrito por Starling (2018, p. 5), podem ser entendidos como "shoppings virtuais", onde diversos lojistas se reúnem em um único ambiente online para ofertar produtos e serviços. Muitas redes sociais, como o *Instagram, Facebook e Pinterest*, agora oferecem funcionalidades de marketplace diretamente em suas plataformas. Os usuários podem ver, clicar e comprar produtos sem sair da rede social. Isso é possível por meio de anúncios, lojas virtuais integradas ou posts de compras, permitindo que os vendedores promovam seus produtos e os consumidores façam compras sem precisar deixar a plataforma. Essas plataformas conectam usuários que produzem e consomem conteúdo, além de assumirem a responsabilidade pela segurança das transações realizadas entre compradores e vendedores.

No entanto, é igualmente importante considerar o papel das redes sociais na organização e manutenção de um ambiente seguro, garantindo que conteúdos ilícitos não sejam

eISSN 2595-1742

disseminados nesses espaços digitais. A compreensão de âmbitos de organização que se revelam pertinentes neste contexto, especialmente em um ambiente caracterizado por riscos, onde a falta de controle pode ensejar danos, é essencial. Embora o Marco Civil da Internet (BRASIL, Lei nº 12.965, 2014) isente os provedores de responsabilidade pelo conteúdo gerado por terceiros, tal isenção é condicionada à efetiva remoção do conteúdo após a devida notificação judicial.

A jurisprudência tem reforçado a necessidade de vigilância ativa por parte dos gestores de redes sociais. Em decisão recente, o STJ condenou o *Facebook* por não excluir uma postagem ofensiva, mesmo após notificação extrajudicial. A decisão reafirma a responsabilidade dos provedores que, após serem notificados sobre conteúdo prejudicial, permanecem inertes. No julgamento do AREsp 1.956.838, observou-se que para fatos ocorridos antes da vigência do Marco Civil da Internet, a responsabilidade do gestor pode ser configurada mesmo sem interpelação judicial prévia, desde que tenha sido devidamente comunicado. A responsabilidade subjetiva solidária se estabelece também pela omissão.

O termo responsabilidade é utilizado em qualquer situação em que uma pessoa, natural ou jurídica, deve arcar com as consequências de um ato, fato ou negócio danoso. Sendo assim, é um conceito jurídico que permite a responsabilização daquele que, de forma ativa ou passiva, causa danos a outra pessoa. No âmbito do direito do consumidor, por exemplo, o Código de Defesa do Consumidor (CDC) adotou a Teoria do Risco como regra, o que significa que os *fornecedores* e *operadores* de produtos e serviços são responsáveis pelos danos causados aos consumidores de forma objetiva e solidária. Isso significa que o fornecedor tem o dever de indenizar o consumidor, independentemente da comprovação de intenção deliberada ou negligência, desde que estejam presentes os elementos essenciais. A teoria do risco-proveito, consagrada pelo CDC, estabelece que aquele que se beneficia de uma atividade que expõe terceiros a riscos deve, por conseguinte, arcar com as consequências de eventuais danos decorrentes dessa exposição. Tal princípio é particularmente relevante para *os fornecedores* e *operadores* de serviços, que, ao disponibilizar plataformas e ambientes virtuais, criam um espaço onde os usuários interagem e compartilham informações, frequentemente sem a devida consciência dos riscos envolvidos.

No que se refere à política de integridade, é importante destacar que as entidades responsáveis pela gestão de plataformas digitais adotem medidas rigorosas que promovam a segurança e a proteção dos dados pessoais dos usuários, em conformidade com as diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD) (Brasil, Lei nº 13.709, 2018), que

eISSN 2595-1742

impõe responsabilidade aos controladores por danos decorrentes de um tratamento inadequado de dados pessoais, exigindo que as plataformas adotem medidas para salvaguardar as informações de seus usuários.

É uma necessidade, de segurança e proteção, que se torna ainda mais premente com a crescente utilização de *inteligência artificial* nas redes sociais, em que algoritmos não apenas influenciam a disseminação de informações, mas também moldam as interações dos usuários de maneira potencialmente prejudicial.

4 IMPUTAÇÃO OBJETIVA: INTELIGÊNCIA ARTIFICIAL E CONDUTA TÍPICA

Os fatos lesivos intermediados por inteligência artificial nas redes sociais podem alcançar bens especialmente protegidos no âmbito penal por sua maior relevância no contexto de proteção ao livre desenvolvimento social da pessoa. Nas últimas décadas temos vivido a transposição de um modo de viver analógico ao digital, um despertar caracterizado por um contexto de *hiperconexão* digital, com o desenvolvimento de sociedades e comunidades virtuais que ampliam a capacidade de conexão e interação humanas (MAYA, 2017, P. 76).

Dessa consideração se observa a necessidade e a relevância de proteção de bens que compõem o núcleo de direitos constitucionalmente protegidos como, por exemplo, o patrimônio, a honra, a intimidade, a liberdade, a dignidade sexual das pessoas que se conectam ou são vinculadas às comunidades digitais: redes sociais materializadas pela internet. Nesse contexto, para Casabona (2023) é importante "revisar as características atuais da teoria do delito e adaptá-las para dar fundamento à responsabilidade penal dos sistemas e produtos da inteligência artificial.":

> Atualmente, e ainda mais à medida que o futuro avança, é previsível que estejam ocorrendo comportamentos delituosos nos ambientes mais desenvolvidos e amplos da inteligência artificial, sem repetir o que já é uma referência comum nos ciberdelitos. No contexto dos crimes financeiros e das organizações criminosas transnacionais, os dados disponíveis parecem apontar nessa direção (exemplo: lavagem de dinheiro). Consequentemente, podemos assumir que se abriu um novo cenário criminal e criminológico para os penalistas (e não apenas para nós, mas também para outros profissionais, não só do Direito). Este será o grande desafio para a humanidade nos próximos anos: como implementar essas tecnologias, evitando ao mesmo tempo que causem danos aos seres humanos e seus bens, incluindo os comportamentos delituosos. [Tradução nossa] (CASABONA, 2023, P. 59).

Neste espaço de estudo, compreende-se que a missão de aproximar o controle penal e as novas tecnologias parte, inicialmente, da construção de um fato penalmente proibido com referência à proteção subsidiária desses bens, o que influi nas formas de pensar a realização do

eISSN 2595-1742

tipo incriminador por meio da valoração do conteúdo material de cada tipo penal. Considera-se, assim, a missão político-criminal de buscar na ordem democrática constitucional a legitimação para o direito penal, o fundamento para a proibição penal e a referência para delimitação material dos tipos:

> [...] o conceito de bem jurídico, embora forjado no plano normativo (valorativo), apresenta um referencial material (ontológico), conectado à realidade existencial (material ou imaterial). O substrato empírico que serve de base ao bem jurídico não exclui a análise axiológica do sentido funcional desses elementos, dados, interesses ou relações concretas sob a perspectiva individual ou coletiva. Esse 'filtro valorativo' será responsável pela seleção dos concretos elementos, dados, interesses ou relações cujo significado social ou político, extraído à luz de um determinado momento histórico, ensejará o recurso à tutela penal (subsidiária). (CARVALHO E ÁVILA, 2015, P.138).

Assim, como a função constitucional do direito penal é a proteção subsidiária de bens jurídicos, todos os seus institutos dogmáticos devem se funcionalizar em prol dessa função (ROXIN, 2013). Considerando esse parâmetro, a teoria da imputação objetiva – que se evidencia como um conjunto de pressupostos que fazem de uma causação, uma causação objetivamente típica (GRECO, 2002) – é um limite à proibição penal, uma vez que só são objetivamente típicas as condutas que se materializam como uma lesão ou perigo de lesão ao bem jurídico-penal, pois "[...] la teoría de la imputación objetiva, que hace depender la tipicidad de la creación y realización de un riesgo no permitido." (SCHÜNEMANN, 2009, p. 13).

Trata-se de uma forma de pensar e de compreender a realização objetiva do fato criminoso para além da relação causal entre ação e resultado danoso. O que se pretende aqui é demonstrar que a valoração dos fatos lesivos deve considerar uma perspectiva dogmática capaz de – com a finalidade de ampliar os espaços sociais de liberdade individual de ação – alcançar restringir normativamente o âmbito da proibição penal, especialmente no campo do tipo objetivo[4]. Isso se faz com a inserção do *princípio do risco* como elemento normativo orientador do *desvalor* objetivo da ação e do resultado típico (GRECO, 2013, P.19-25).

A abordagem funcional, por meio da teoria da imputação possibilita um maior refinamento e adequação político-criminal para compreender a atribuição do *desvalor* da conduta nos casos de intervenção lesiva em rede social por meio de IA. A teoria da imputação pode ser entendida como um sistema normativo dotado de critérios que, com fundamento no princípio do risco material ao bem jurídico-penal, instrumentaliza procedimentos no âmbito do

[4] Vale ressaltar que a Teoria da Imputação é um instrumento limitador do tipo objetivo que tem ampliado os espaços de refinamento dogmático na doutrina e jurisprudência do Brasil, especialmente na correção das situações não alcançadas pelo uso da perspectiva causal-naturalista de compreensão do tipo.

eISSN 2595-1742

tipo objetivo para determinar, numa perspectiva valorativa e funcional a atribuição objetiva da conduta e do resultado típicos, considerando as circunstâncias que compõem um curso causal.

Para a materialização do tipo é necessário que o fato lesivo compreenda o risco que a proibição penal pretende *contramotivar*, pois "um resultado causado pelo agente só deve ser imputado como sua obra e preenche o tipo objetivo unicamente quando o comportamento do autor cria um risco não permitido para o objeto da ação, quando o risco se realiza no resultado concreto, e este resultado se encontra dentro do alcance do tipo."(ROXIN, 2002, p.01). O pensamento comum é de uma valoração normativa no âmbito do juízo de tipicidade penal que possa superar os defeitos abrigados no procedimento causal-naturalista de determinação do nexo de causalidade que vincula a ação pessoal e um resultado típico.

Os efeitos de uma decisão jurídico-penal, assim, não podem se limitar ao conteúdo de uma significação ontológica obtida com procedimentos *avalorados* que recaem sobre o fato social numa perspectiva causal, naturalística e classificatória. O pensamento é que o conteúdo da tipicidade não se completa com a ação neutra e natural, de outro modo, é preciso que o direito penal utilize métodos valorativos, típico das ciências da cultura, incorporando o conteúdo dos fins de política criminal ou da identidade social, através da proteção da norma, ao ordenamento jurídico.

É nesse espaço de compreensão que o estudo se estabelece no âmbito de alcance do risco típico, compreendido como elemento que integra a conduta, e também como um primeiro nível normativo de valoração da responsabilidade penal nos fatos intermediados por IA. O tipo objetivo, assim, pressupõe a existência de uma conduta que, normativamente, para além dos elementos subjetivos, compreende a reprovação do risco criado pelo fornecedor ou agente de IA como elemento que orienta o seu *desvalor objetivo*. Aqui que se tem a necessidade de compreender os indicadores que possam indicar o *desvalor do risco* que forma o conteúdo da tipicidade de tal conduta.

5 INTELIGÊNCIA ARTIFICIAL: DO RISCO PERMITIDO AO PERIGO PROIBIDO

O espaço desse capítulo é destinado à compreensão, através do sistema penal, do risco inerente às relações construídas pela Inteligência Artificial como um fenômeno capaz de orientar o limite material dos espaços sociais de proibição penal, considerando as vivências nas *redes sociais*. Análise que se realiza com a aferição do risco que se demonstra em atividades

eISSN 2595-1742

comuns da vida comunitária, considerado adequado e necessário ao modo de produção do sistema social.

Nas redes sociais, os algoritmos e a inteligência artificial são instrumentos que potencializam o mercado financeiro, ampliam as plataformas de diálogo que influem na estrutura da educação; da empregabilidade e na gestão de recursos humanos; na política; na conexão entre pessoas e consequentemente nas relações de afeto. Estão presentes também na administração da justiça, na gestão pública no âmbito da organização de trânsito e controle ambiental, na medicina e na farmacologia, nos serviços domésticos e até nos armamentos utilizados nos conflitos internacionais e nas ações policiais domésticas voltadas à materialização das políticas de segurança pública.

A IA se apresenta em um modelo de sociedade de riscos que, segundo Ulrich Beck (2011, p. 24) "não de apresenta exclusivamente de uma utilização econômica da natureza para libertar as pessoas de sujeições tradicionais, mas também e sobretudo de problemas decorrentes do próprio desenvolvimento técnico e econômico". Felix Herzog (250) analisa que o discurso sobre a sociedade de riscos se trata também de rupturas e destruições de conceitos tradicionais da modernidade e da pergunta acerca das novas orientações ou recuperação de ideias.

A sociedade que incorpora esse risco como fenômeno não apenas adequado, mas necessário ao atual estágio de desenvolvimento de suas estruturas. A constatação é da existência de uma comunidade apoiada numa base interacional em que as relações interpessoais intermediadas pela IA são eivadas de riscos, as pessoas voluntariamente produzem, assumem e se colocam em risco:

> A inteligência artificial (IA), a robótica e os sistemas autônomos inteligentes fazem parte do cotidiano dos seres humanos. E seu impacto está crescendo em diversos setores da atividade humana, como no diagnóstico e tratamento de doenças, na luta contra as mudanças climáticas, na melhoria e aumento da capacidade produtiva em geral e na indústria em particular, nos meios de transporte, no lazer e na antecipação de danos à cibersegurança. [Tradução nossa] (CASABONA, 2023, P. 57).

Aqui a intervenção penal alcança a necessidade de controle dos novos ou renovados riscos da sociedade pós-moderna, que afetam e colocam em perigo a existência da humanidade como um todo, expondo a perigo de lesão ou lesionando bens coletivos, de importância supraindividual. O problema se põe na análise das pretensões punitivas aos riscos evidenciados, por exemplo, através das novas relações de consumo, das relações virtuais, da intervenção no meio-ambiente com os riscos nucleares intermediados por IA.

Esse é o risco que representa um perigo supraindividual e evidencia a necessidade social de controle: gestão e limitação das consequências negativas do processo de globalização.

eISSN 2595-1742

Ulrich Beck destaca que risco, agora vinculado à sociedade de riscos pós-moderna, não decorre — exclusivamente de uma utilização econômica da natureza para libertar as pessoas de sujeições tradicionais, mas também e sobretudo de problemas decorrentes do próprio desenvolvimento técnico e econômico.

Riscos que, em uma dimensão individual, também estão contidos em atividades simples do cotidiano que são assumidas voluntariamente pelas pessoas, considerando que a valoração deles, dos riscos, é um importante critério para uma construção dogmática sobre a teoria do delito que propõem a uma legítima determinação do fato social penalmente proibido.

Para alcançar essa legitimidade, é preciso uma reinterpretação do conteúdo que o sistema penal atribui aos elementos que compõem o método inerente às construções dogmáticas. Observar os limites do risco presente nas relações normais à sociedade, os intervenientes na majoração do risco além do adequado e o modo de realização do risco num fato social perigoso ou lesivo a um bem jurídico é um critério mais apropriado para aproximar a dogmática penal e a identidade cultural assumida pelo sistema social atual.

O problema a ser enfrentando diz respeito ao estabelecimento de qual a espécie (forma) e em que nível de realização (peso) o risco permitido passa a configurar um perigo proibido capaz de conduzir a contramotivação típica.

Aqui a pretensão não é esgotar a análise da admissibilidade os fatos perigosos como forma de viver da sociedade atual, mas estabelecer como ponto de partida que a compreensão do sistema jurídico como instrumento de controle não tem a pretensão de *contramotivação* e proibição de todos os riscos e perigos enfrentados em sociedade.

Nesse sentido, as atividades arriscadas e especialmente perigosas terão relevância jurídica quando ultrapassam o limite tolerado, considerando a transposição ou não ajustamento a uma norma de cuidado. Atividades arriscadas, ainda que especialmente perigosas, realizadas no âmbito do cuidado devido não devem ser alvo de contramotivação jurídica. Santiago Mir Puig (2011, p. 15) adverte que “Não só os setores de atividade perigosa permitida, mas também o chamado risco geral da vida, representam uma classe de risco não absolutamente imprevisível, e cuja licitude decorre de uma avaliação normativa.”

Assim, a percepção e aferição dos riscos sociais não devem decorrer da mera causalidade, mas de um método valorativo que lhe atribua um significado social, que o incorpora como um dos fenômenos da sociedade moderna. A significação do risco decorre, então, do conteúdo extraído da afirmação ideológica de valores comunitários em um sistema

eISSN 2595-1742

social. Esse conteúdo demonstra o limite que a sociedade deve suportar como necessário à sua existência.

Disso, é possível afirmar que por meio de uma adequação entre liberdade e segurança se obtém parâmetros formais ao limite do comportamento arriscado. Assim, é o 21sistema social que, através dos procedimentos de composição legislativa, estabelece os limites do comportamento arriscado tolerável. Numa perspectiva funcionalista, para determinação do risco proibido como critério inicial de imputação objetiva do resultado, é preciso uma valoração, com a significação normativa, do comportamento arriscado em concreto.

Esse limite forma o conteúdo do cuidado objetivamente devido que orienta as atividades no caso concreto. São normas que compreendem os limites do perigo socialmente tolerado. No Brasil, existem normas que no sentido geral podem regular as consequências do uso da IA, como no âmbito do Direito do Consumidor, a Lei Geral de Proteção de Dados e o Marco Civil da Internet, mas permanecem espaços abertos quanto ao dever de cuidado a ser assegurado no exercício específico da gestão, do desenvolvimento e da manipulação da inteligência artificial. Nesse contexto, a valoração penal dos fatos lesivos intermediados pela inteligência artificial ainda tem como referência normas gerais de comportamento.

6 INTELIGÊNCIA ARTIFICIAL E O RISCO TÍPICO

A restrição desses espaços – considerando o limite socialmente tolerado do comportamento arriscado por meio de um juízo de ponderação entre o respeito à liberdade e a função de proteção de bens - contribuirá para uma melhor crítica sobre a conduta dos intervenientes num fato social que seja capaz de criar ou aumentar um risco, excedendo o patamar máximo de sua permissividade social com o uso de IA.

Para aferição do comportamento típico, nesse sentido, é necessária a criação de um risco juridicamente proibido. A aferição do conteúdo do desvalor objetivo da ação com a realização do risco típico, aqui, ultrapassa o nível sistêmico social: a adequação social é um primeiro filtro ao comportamento objetivamente típico que buscava observar “determinadas hipóteses *desvaloradas* do ponto de vista social, nas quais as lesões aos bens jurídicos ocorriam dentro do funcionamento normal da vida em sociedade” (CARVALHO, PRADO, 1997, P. 101). Vale ressaltar, no entanto, que nem todo comportamento socialmente inadequado é juridicamente proibido.

eISSN 2595-1742

É nesse sentido que se têm projetos de lei que dispõem sobre os princípios, bem como sobre os direitos e deveres para o uso de inteligência artificial no Brasil. Destaca-se, dentre eles, considerando a construção de critérios para a compreensão da forma e do nível de perigo presentes no desenvolvimento da inteligência artificial, o Projeto de Lei 2338 de 2023.

O projeto abre um espaço de regulamentação sobre a categorização dos riscos. Nesse sentido, "Art. 13. Previamente a sua colocação no mercado ou utilização em serviço, todo sistema de inteligência artificial passará por avaliação preliminar realizada pelo fornecedor para classificação de seu grau de risco [...]." (BRASIL, 2023, PL2338). A partir daí, o Projeto dispõe sobre modalidades de risco: i. risco excessivo; e ii. alto risco, construindo orientações para a construção de sistemas de governança do risco inerente ao uso de IA e indicadores para responsabilização civil e administrativa.

O projeto veda a utilização de sistemas de inteligência artificial na composição de fatos que possam instrumentalizar crimes nas redes sociais digitais, como fraudes em jogos digitais, investimentos fraudulentos e violações à privacidade e à dignidade sexual. Nesse sentido, veda-se a utilização de sistemas de IA que "empreguem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança" (BRASIL, 2023, PL2338).

Proíbe também aqueles que "explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como as associadas a sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma prejudicial a sua saúde ou segurança."

O projeto considera de alto risco, demandando estratégias especiais de governança e manutenção da integridade, por exemplo, o desenvolvimento de sistemas de IA que instrumentalize "veículos autônomos, quando seu uso puder gerar riscos à integridade física de pessoas", e os sistemas aplicados "na área da saúde, inclusive as destinadas a auxiliar diagnósticos e procedimentos médicos" (BRASIL, 2023, PL2338).

O projeto prevê que "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 terceiros, assim como de caso fortuito externo." (BRASIL, 2023, PL2338).

É importante ressaltar que a realização do risco que caracteriza a violação do cuidado devido não se esgota o conteúdo necessário para a atribuição do tipo, mas é um marcador adequado para delimitar o limite do risco permitido. A questão é que: considerando

eISSN 2595-1742

o direito penal como instrumento de controle social em subsidiário e fragmentário, a violação à norma de determinação capaz de ensejar a caracterização do injusto deve ser mais qualificada que a violação de normas cíveis ou administrativas. “A essência do perigo é a proximidade do dano que pode ou não se concretizar. A essência do risco, não mais a decantada fortuna, é a inerência e a permanência de escolhas humanas.” (MARQUES, 2008, P.34)

Se no âmbito formal da proibição, a eleição do direito penal como instrumento de proteção se estabelece de modo subsidiário, como última forma de proteção; no âmbito do material, ou seja, da violação da proibição, a compreensão do comportamento juridicamente arriscado não se esgota na contraposição de normas de proteção *prima ratio*, como aquelas destinadas ao direito administrativo, mas requer a valoração em face da matéria que o direito penal quer proibir.

É necessário valorar, por exemplo, o risco que se manifestam como ofensas à dignidade e ao decoro das pessoas, que se constituem como matéria proibitiva dos crimes contra a honra; o perigo que produz as lesões à integridade física e à vida, que orientam a finalidade da proibição penal dos tipos de lesão e de homicídio; assim como o *desvalor* do comportamento fraudulento, que se manifesta como conteúdo ou modo de realização de tipos que buscam a proteção ao patrimônio.

7 CONSIDERAÇÕES FINAIS

Os novos e renovados riscos que decorrem do desenvolvimento tecnológico contemporâneo amplia a complexidade da relação entre a sociedade e as suas estruturas de controle, especialmente as de controle formal como o direito penal. A criação e a ampliação das redes sociais digitais e dos sistemas de inteligência artificial constroem novos espaços sociais de realização da humanidade.

Os riscos do desenvolvimento da *inteligência artificial* são toleráveis no limite adequado e necessário ao desenvolvimento humano. A criação e o aumento do risco que decorre da uso da *IA* pode ser intermediado pela ação de agentes e desenvolvedores, que podem não ter o controle sobre o resultado decorrente da colocação do sistema em rede.

Nesse sentido, para a valoração da responsabilidade penal em face dos fatos lesivos intermediados pela *IA*, tem-se como adequado um método dogmático axiológico, referido a valores, com a capacidade de compreender o risco do desenvolvimento do sistema como critério

eISSN 2595-1742

de imputação. Neste trabalho, por meio da teoria da imputação objetiva, observa-se o critério da *conduta típica* como o primeiro nível dogmático necessário para a determinação da responsabilidade penal.

Projetos de Lei pretendem orientar o limite do cuidado devido para a realização de riscos inerentes ao uso dos sistemas de *inteligência artificial* em âmbito administrativo. A partir deles, observa-se um horizonte de expectativa mais refinado para compreender o *desvalor objetivo* da conduta penalmente típica, alcançado pela realização de um perigo proibido e, consequentemente, socialmente insuportável.

REFERÊNCIAS

BECK, Ulrich. **Sociedade de Risco:** Rumo a uma outra modernidade. Tradução: Sebastião Nascimento. Rio de Janeiro: Editora 34, 2011.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm>. Acesso em: 26 set. 2024.

BRASIL. Projeto de **Lei nº 2338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Disponível em: < https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1732829643926&disposition=inline >. Acesso em: 29 nov. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 26 set. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da República Federativa do Brasil], Poder Legislativo, Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 29 março 2023.

CARVALHO, Érika Mendes de. ÁVILA, Gustavo Noronha de. **Falsos bens jurídicos e política criminal de drogas: uma aproximação crítica**. Direito Penal, Criminologia e Segurança Pública [Recurso eletrônico on-line] organização CONPEDI/Madrid-Espanha; Coordenadores: Romuldo RehmoPalitot Braga, Amparo Martínez Guerra– Madrid: CONPEDI, 2015.

CASABONA, Carlos Romeo. Inteligencia artificial y responsabilidad penal. **Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial**. Volumen II. Comares: Granada, 2023.

eISSN 2595-1742

CASTRO, P. A. **Rede complexa e criticalidade auto-organizada:** modelos e aplicações. 2007. Tese (Doutorado em Física) - Instituto de Física de São Carlos, Universidade de São Paulo, 2007.

COZMAN, Fabio G.; PLONSKI, Guilherme Ary; NERI, Hugo (orgs.). **Inteligência Artificial: Avanços e Tendências**. São Paulo: Instituto de Estudos Avançados, 2021. Disponível em: https://doi.org/10.11606/9786587773131. Acesso em: 30 set de 2024.

GIMENEZ, María Hernández.. Inteligencia Artificial Y Derecho Penal. **Actualidad Jurídica Iberoamericana** Nº 10 bis, junio 2019, pp. 792-843

GRECO, Luís. A Teoria da Imputação Objetiva: uma introdução. In: ROXIN, Claus. **Funcionalismo e Imputação Objetiva no Direito Penal**. São Paulo: Renovar, 2002.

_____. **Introdução à Dogmática Funcionalista do Delito**. Texto do trabalho apresentado (com algumas modificações) no I Congresso de Direito Penal e Criminologia, ocorrido da UFBA, nos dias 13-15 de abril de 2000, no painel sobre o "Funcionalismono Direito Penal".

_____. **Um Panorama da Teoria da Imputação Objetiva**. São Paulo: Revista dos Tribunais, 2013.

HERZOG, Felix. **Sociedad del Riesgo, Derecho Penal del Riesgo, Regulación del Riesgo:** Perspectivas más allá del Derecho Penal. IN: ZAPATERO, Luis Alberto Arroyo. MARTÍN, Adán Nieto. NEUMANN, Ulfrid. Crítica y justificación del derecho penal en el cambio de siglo: el análisis crítico de la Escuela de Frankfurt. Universidad de Castilla-La Mancha, 2003.

LLINARES, Fernando Miró. Inteligencia Artificial Y Justicia Penal: Más Allá De Los Resultados Lesivos Causados Por Robots. **Revista De Derecho Penal Y Criminología**, 3.ª Época, n.º 20 (julio de 2018), págs. 87-130.

MAYA, Ricardo Posada. El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual **Nuevo Foro Penal**. Vol. 13, Nº. 88, 2017, págs. 72-112
PRADO, Luiz Régis. CARVALHO, Érika Mendes de. CARVALHO, Gisele Mendes de. *Curso de Direito Penal*. São Paulo: Revista dos Tribunais, 2014.

MARACINE, Virginia; VOICAN, Oona; SCARLAT, Emil**. The digital transformation and disruption in business models of the banks under the Impact of FinTech and BigTech**. In: INTERNATIONAL CONFERENCE ON BUSINESS EXCELLENCE, 14., 2020, Bucareste. Proceedings […]. Bucareste: The Bucharest University of Economic Studies, 2020. p. 294-305. Disponível em: https://sciendo.com/article/10.2478/picbe-2020-0028. Acesso em: 11 ago. 2024.

PECK PINHEIRO, Patrícia**. *Direito digital*. 7**. ed. rev., ampl. e atual. São Paulo: Saraiva Jur, 2021.

eISSN 2595-1742

ROXIN, Claus **Funcionalismo e Imputação Objetiva no Direito Penal**. Rio de Janeiro: Renovar, 2002. p. 354.

_____. **Política Criminal e Sistema Jurídico-Penal**. Tradução: Luís Greco. Rio de Janeiro: Renovar, 2000.

_____. **A proteção de Bens Jurídicos como função do Direito Penal**. Organização e Tradução de André Luís Callegari e Nereu José Giacomolli. 2ª Ed. Porto Alegre: Livraria do Advogado, 2013.

_____. **A teoria da imputação objetiva**. IN: Estudos de direito penal. Tradução: Luís Greco. São Paulo: Renovar, 2006.

_____. **Funcionalismo e Imputação Objetiva no Direito Penal**. Tradução Luís Greco. Rio de Janeiro: Renovar, 2002.

MACHADO, Felipe Nery Rodrigues**. Big Data: o futuro dos dados e aplicações**. São Paulo: Érica, 2018.

MARTELETO, R. M**. Análise de redes sociais:** aplicação nos estudos de transferência de informação. *Ciência da Informação*, Brasília, v. 30, 2001.

MIR PUIG, Santiago. **Direito Penal**. Fundamentos e Teoria do Delito. São Paulo: Revista dos Tribunais, 2007.

_____. **Bases Constitucionales del Derecho Penal**. Madrid: Iustel, 2011.

SCHUNEMANN, Bernd. **A Crítica ao Paternalismo Jurídico-Penal**: Um trabalho de Sísifo? IN: SCHÜNEMANN, Bernd. Estudos de Direito Penal, Direito Processual Penal e Filosofia do Direito. Coordenador: Luís Greco. São Paulo: Marcial Pons, 2013.

_____. **El propio sistema de la teoría del delito**. Barcelona: Indret. 2009.

STARLING, Ana P**. Marketplace e os pequenos negócios**: Pesquisa aplicada ao ambiente do ELO7. 2018. p.26. Trabalho de conclusão de curso -Centro Universitario de Brasília, Brasília, 2018. Disponível em: < https://repositorio.uniceub.br/jspui/bitstream/235/12303/1/51500841.pdf> . Acesso em: 01. Nov.2014.