UNIVERSIDADE NOVE DE JULHO

Mariana Fleming Soares Ortiz

INTELIGÊNCIA ARTIFICIAL E RESPONSABILIDADE PENAL

São Paulo, 2023

Mariana Fleming Soares Ortiz

INTELIGÊNCIA ARTIFICIAL E RESPONSABILIDADE PENAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Nove de Julho para obtenção do título de Mestre em Direito.

Área de concentração: Regulação e Empresa Transnacional.

Orientador: Prof. Dr. Rogerio Schietti Machado Cruz

São Paulo, 2023

Nome: Mariana Fleming Soares Ortiz

Título: Inteligência artificial e responsabilidade penal

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Nove de Julho para obtenção do título de Mestra em Direito.

Aprovado em: 17/08/2023

Banca Examinadora

Orientador: Prof. Dr. Rogerio Schietti Cruz

Instituição: UNINOVE Assinatura: _____

Prof. Dr. Marcelo Costenaro Cavalli

Instituição: UNINOVE Julgamento:_____

Prof. Dra. Danyelle Galvão

Instituição: USP Julgamento:_____

RESUMO

A inteligência artificial nunca esteve tão perto da ficção científica. Com o avanço das tecnologias o Direito – enquanto regulador das relações humanas – tem se deparado com diversos desafios e questionamentos para responder às demandas da sociedade, especialmente em âmbito criminal. O presente trabalho se desenvolveu a partir do estudo de doutrina, principalmente internacional, na busca por entender a recente situação da relação entre inteligência artificial e direito penal, perpassando pela análise de casos concretos de violações à bens jurídicos por máquinas, os quais vêm ocorrendo em âmbito mundial, bem como, pela análise das regulamentações atuais sobre o tema “inteligência artificial”. Por fim, o foco é enfrentar o tema sob a ótica da teoria do delito, no aspecto da tipicidade, como sugestão de enfrentamento do problema. Em resumo, o objetivo desse trabalho é discutir se, e como, alguém pode ser responsabilizado no Brasil pelas violações de bens jurídicos causadas por máquinas dotadas de sistemas autônomos e máquinas dotadas de autoaprendizagem.

PALAVRAS-CHAVE: Inteligência artificial. Sistemas autônomos. Autoaprendizagem. Direito Penal. Responsabilização.

ABSTRACT

Artificial intelligence has never been closer to science fiction. With the advancement of technology, Law – as a regulator of human relations – has faced several challenges and questions in order to respond to the demands of society, especially in the criminal sphere. The present dissertation was developed from the study of doctrine, mainly international, in the search to understand the recent situation of the relationship between artificial intelligence and criminal law, passing through the analysis of concrete cases of violations of legal interests by machines, which have been occurring in world scope, as well as, by the analysis of the current regulations on the subject “artificial intelligence”. Finally, the focus is on tackling the issue from the perspective of the theory of crime, in terms of typicality, as a suggestion for tackling the problem. In summary, the objective of this dissertation is to discuss whether and how someone can be held responsible in Brazil for violations of legal interests caused by machines with autonomous systems and machines with self-learning.

KEYWORDS: Artificial intelligence. Autonomous systems. Self-learning. Criminal Law. Accountability.

Sumário

Introdução

O Direito como regulador das relações sociais e humanas vem sendo impactado pelo fenômeno da *digitalização* em suas mais diferentes áreas e é ocasionalmente acionado para impor limites e criar regulamentações aos avanços tecnológicos. A digitalização revoluciona toda a vida em sociedade, e assim, também, o campo de aplicação do Direito.

Por evidente que o presente trabalho não tem a pretensão de esgotar a matéria acerca da relação entre inteligência artificial e direito que, em verdade, parece ser infinita, porque a tendência mundial da tecnologia não é retroceder e, sim, expandir. A previsão em âmbito global é que a quantidade de produtos dotados inteligência artificial aumente cada vez mais, porquanto a tecnologia avançada tem potencial para evoluir a vida em sociedade nas mais diversas áreas e ambientes (medicina, direito, engenharia, transportes, fábricas etc), e isso ocorre principalmente porque as máquinas, por meio de algoritmos, têm capacidade de processar dados com precisão e velocidade que são humanamente impossíveis.[1]

Merece atenção o fato de que atualmente produtos tecnológicos com inteligência artificial podem ser compostos de “machine learning”, os chamados sistemas autônomos com autoaprendizagem, que são capazes de se autoalimentar de dados que lhe são fornecidos (por pessoas e pelo ambiente) para alcançar e aprimorar resultados pré-estabelecidos e, portanto, serem capazes de, por si, tomar decisões.

Esse estado da tecnologia alcança o direito penal em variados temas abertos à discussão, especialmente porque bens jurídicos já tutelados em âmbito nacional e internacional passaram a ser violados por máquinas, como por

[1] A descrição é de 2020 e do Parlamento Europeu. Disponível em: https://www.europarl.europa.eu/news/de/headlines/society/20200206STO72030/kunstliche-intelligenz-verbraucher-vor-risiken-schutzen Acesso em: 23 de dezembro de 2022.

exemplo a integridade física e a vida. Ocasionalmente, essa revolução tecnológica pode vir, também, a gerar novas formas de criminalidade digital, inclusive para além das já conhecidas violações a bens jurídicos ocorridas por meio de computação *stricto sensu* (fraudes eletrônicas, hackeamento de informações, compartilhamento de fotos/vídeos íntimos etc.).

Diversos são os exemplos de possíveis crimes a partir da ampliação da digitalização, tal como a divulgação maciça e coordenada de mensagens de ódio e desinformação no âmbito das redes sociais a partir de *fake news*, as ofensas provenientes de algoritmos tendenciosos, racistas e sexistas em *sites,* aplicativos e redes sociais, ofensas à intimidade e privacidade por vazamento de dados pessoais, violações a consumidores por meio de algoritmos pré-condicionados, erros decorrentes de medicina robótica, discussão sobre crimes cibernéticos no metaverso e, até mesmo, a discussão acerca da possibilidade (ou não) de cometimento de crimes comuns por meio de avatares em ambiente de realidade aumentada[2]. Hoje, o exemplo mais comum é a violação à integridade física por danos causados a partir de acidentes automobilísticos envolvendo veículos autônomos, tal como os carros “full selfdriving capabillity” Tesla[3], que são coordenados e guiados a partir de avançada tecnologia.

A partir da interconexão ubíqua na “internet das coisas”, quando tudo estiver conectado e a vida for operada majoritariamente por meio – ou através de – máquinas e robôs, outras violações a bens jurídicos são previsíveis.

Isso traz potencial dificuldade ao direito penal, ao menos aparente, de atribuição de responsabilidade quando for causado resultado típico por produto dotado de inteligência artificial, especialmente de sistema autônomo com autoaprendizagem, haja vista que a teoria do delito é calçada no conceito de conduta como ação humana e a imputação de responsabilidade aos robôs ainda fica limitada à ficção científica.

---

[2] https://www.uol.com.br/universa/noticias/redacao/2022/06/03/estupro-no-metaverso-o-aconteceu-comigo-foi-real.htm

[3] A descrição do produto está no *site* da Tesla. Disponível em: <https://www.tesla.com/support/autopilot> Acesso em 12 de janeiro de 2023

O que se avalia nessa oportunidade é a atribuição de responsabilidade penal, em âmbito empresarial, a partir de violações a bens jurídicos já conhecidos e tutelados, praticados por produtos dotados de inteligência artificial, e por aqueles que detêm sistemas autônomos com autoaprendizagem.

A criação, implementação, circulação e uso de produtos dotados de inteligência artificial envolve uma grande gama de pessoas desde a fabricação, passando pela manutenção, controle/acompanhamento do desenvolvimento, venda e distribuição, como a propriedade e a própria utilização pelo usuário final e sua relação com a sociedade.

Esta longa cadeia, que vai desde a criação até a distribuição e uso de produto de inteligência artificial pode contar com a participação de diversos personagens como: criador, desenvolvedor, fabricante, sócios e gerentes da empresa/fábrica, programador e até mesmo o vendedor e o usuário final, o que faz com que as condutas realizadas neste processo sejam cada vez menos pessoalizadas.

Problema parecido já se percebe nas relações estabelecidas dentro de ambientes empresariais que têm divisão de tarefas e, é, na maior parte das vezes, hierarquizado.[4]

Pensa-se nessa oportunidade sobre essa equação, mas sob a ótica de um diferente elemento, pois pretende-se verificar, quem - e de que modo – pode ser responsabilizado penalmente a partir de conduta típica praticada por produto com inteligência artificial e capaz de autoaprendizagem, dentro deste contexto empresarial e das relações traçadas. Ou seja, quem pode ser responsável por uma conduta violadora de bem jurídico praticada por uma máquina?

---

[4] Para saber mais, ver: ESTELLITA, Heloísa. Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros de empresa – 1. ed. – São Paulo: Marcial Pons, 2017.

Ao final, busca-se entender se o direito penal brasileiro tem condições imediatas de responder adequadamente a estas novidades tecnológicas e suas implicações, e quais aparentam ser os caminhos viáveis.

1. DIGITALIZAÇÃO

O fenômeno da *digitalização* é o processo de transformar o que é físico em digital, de tal maneira que o que é material pode ser submetido a uma linguagem de zeros e uns. (GLEIZER, 2020)

Tudo que existe e está no mundo real pode ser transportado para o mundo digital e, com isso, virar informação. Um exemplo são carros em uma via pública, cuja situação real é captada via satélite e se transforma em informação de tráfego para GPS.

Qualquer informação digitalizada tem suas multifaces, ou seja, pode ser transformada em vídeo, foto, áudio, arquivo de texto etc. Inclusive em mais de um formato concomitantemente (HILGENDORF, 2020). Um mesmo arquivo pode ser a um só tempo um arquivo de imagem e de vídeo. Um exemplo disso seria um livro, que digitalmente pode ser um e-book, que é um arquivo de texto, mas poder ser também um arquivo de áudio livro. Isso se define como *grau de plasticidade das informações*:

> Variados dados da realidade analógica, como alguém sentado em um banco de uma praça com um livro na mão, podem ser transformados em uma linguagem simples de apenas dois dígitos (0 e 1). Essa linguagem pode ser lida por máquinas de leitura digital (computadores) e submetida a diversos algoritmos, que, com base nestes dados, poderão, por exemplo, recriar em uma tela a imagem que se vê de alguém sentado em um banco de uma praça com um livro na mão, traduzi-la para um formato de áudio que a descreva para usuários com problemas visuais ou em um vídeo no qual ela se mova, ou ainda em um comando informativo para o sistema de condução autônoma de veículo, que indicará que naquela direção há uma pessoa sentada no banco da praça, ou, possivelmente, em um alerta para o sistema de busca de foragidos, de que a sequencia numérica formada a partir da identificação fácil daquele individuo é semelhante àquela resultante da identificação facial de um terrorista procurado. (GLEIZER, 2020, p. 19 e 20)

Atualmente os computadores têm elevado potencial de captação, armazenamento, edição e compartilhamento dessas informações, principalmente pelo alto grau de desenvolvimento da internet que garante que qualquer dado, em um período de milésimos de segundos, alcance todo o

planeta. Todas as informações digitais são recebidas, processadas, armazenas e compartilhadas mundialmente e de maneira imediata (HILGENDORF, 2020)

Além desse flagrante desenvolvimento gerado pela conexão do mundo todo a partir da internet, existem fenômenos que devem ser analisados para se caracterizar o cenário mundial da digitalização. Exemplos são: computação e internet ubíquas, indústria 4.0, internet das coisas (IoT), *smart city*, *smart home* etc.

1.1. FENÔMENOS DA DIGITALIZAÇÃO

Dentro da área de Interação Humano-Computador foi criado o conceito de computação ubíqua para descrever a computação onipresente no dia a dia da vida das pessoas (RODOVALHO; MORAES, 2017).

Por muito tempo os desenvolvedores de tecnologia focaram em criar design de computadores para torná-los mais atrativos para que as pessoas não mais quisessem parar de usá-los (RODOVALHO; MORAES, 2017). Entretanto, ao menos desde 1988, tornar atrativo não era mais suficiente, sendo então criada a ideia da computação ubíqua por Mark Weiser (1991) no artigo "The Computer for the 21st Century".

Na concepção de Mark Weiser (1991) seria necessário que a computação se tornasse algo invisível aos olhos, mas tão profundo na realidade humana que as pessoas interagissem com ela a todo momento sem sequer perceber.

> Tal desaparecimento é uma consequência fundamental não da tecnologia, mas da psicologia humana. Sempre que as pessoas aprendem algo suficientemente bem, elas deixam de ter consciência disso. Quando você olha para uma placa de rua, por exemplo, você absorve suas informações sem realizar o ato de leitura de forma consciente. (WEISER, 1991)[5]

[5] Tradução livre. Texto no original: “Such a disappearance is a fundamental consequence not of technology but of human psychology. Whenever people learn something sufficiently well, they

De acordo com essa ideia de Mark Weiser (1991), que seria pautada em conceitos anteriores e bem construídos, inclusive por Heidegger, quando os objetos somem é que estão integrados na vida humana, permitindo, assim, que o foco de atenção seja em outros objetos e coisas.

> A ideia de integrar os computadores perfeitamente ao mundo em geral vai contra uma série de tendências atuais. "Computação ubíqua" neste contexto não significa apenas computadores que podem ser levados para a praia, selva ou aeroporto. Mesmo o notebook mais poderoso, com acesso a uma rede mundial de informações, ainda concentra a atenção em uma única caixa. Por analogia com a escrita, carregar um superlaptop é como possuir apenas um livro muito importante. Personalizar este livro, mesmo escrevendo milhões de outros livros, não começa a captar o real poder da alfabetização.[6]

De acordo com este entendimento as pessoas seriam cercadas por tecnologia e a computação teria um sistema inteligente integrado e conectado entre si, com trocas de informações a todo tempo (RODOVALHO; MORAES, 2017).

> A Computação Ubíqua trata do desenvolvimento de soluções, na área de tecnologia da informação, que visam interagir com o usuário por meio de dispositivos que podem ser distribuídos no ambiente e que estão presentes no dia a dia das pessoas. Este paradigma computacional se contrapõe a ambientes restritos e controlados, como domicílios, escritórios e empresas, em que a conexão a redes de computadores se dá por meio de cabos ou conexões sem fio de curta distância. No contexto ubíquo, o usuário tem maior flexibilidade para se deslocar por longas distâncias, permanecendo o tempo todo conectado a redes de computadores (KUMAR, 2009). Já que o indivíduo encontra-se constantemente imerso em ambientes que entrelaçam o real e o virtual e dada a onipresença computacional, a expectativa é que os dispositivos físicos e suas interfaces estejam diluídos, imperceptíveis e invisíveis de tão próximos que estão do cotidiano humano (WEISER, 1999). Embora a visão de Weiser tenha sido fortemente baseada em computadores, ele mesmo já sinalizava para o surgimento de dispositivos vestíveis - ou wearable devices, em inglês. (PIRES; OLIVEIRA NETO, 2021)

---

cease to be aware of it. When you look at a street sign, for example, you absorb its information without conseiously performing the act of reading.

[6] Tradução livre. Texto no original: “The idea of integrating computers seamlessly into the world at large runs counter to a number of present-day trends. "Ubiquitous computing" in this context does not mean just computers that can be carried to the beach, jungle or airport. Even the most powerful notebook computer, with access to a world- wide information network, still focuses attention on a single box. By analogy with writing, carrying a super-lap-top is like owning just one very important book. Customizing this book, even writing millions of other books, does not begin to capture the real power of literacy.””

Ainda atualmente, para alcance desse objetivo, o conceito inspira o surgimento quase constante de tecnologias e essa evolução já afeta todas as áreas da “vida social, econômica, política, cultural e contemporânea do mundo” (SARLET, 2021)

No que diz respeito à conexão à internet, as inovações permitiram a humanidade, por exemplo, caminhar em poucos anos de uma internet discada para sem fio, incluindo nisso ambientes externos, o que faz com que as pessoas possam estar quase 100% do tempo conectadas, como ocorre com cidades mundo afora que fornecem acesso gratuito à internet à população, o que inclusive vem sendo ampliado no Brasil.[7]

Para além dessas conexões sem fio, os avanços são constantes também em termos de acesso a aparelhos de comunicação móveis – os chamados smartphones, que hoje podem ser desbloqueados sem que seja necessário ao usuário sequer preencher uma senha ou conferir sua digital. Apenas os olhos são suficientes[8], ou como divulga a *Apple* “Basta um olhar, e o Face ID desbloqueia o iPhone ou iPad Pro com segurança”[9]

O mesmo ocorre em relação aos sistemas de armazenamento de arquivos e informações em nuvem, que podem ser acessados de praticamente qualquer lugar do mundo, inclusive com arquivos que podem ser simultaneamente alterados por pessoas que estejam a quilômetros de distância uma da outra. A mesma lógica é aplicável ao compartilhamento imediato e em massa de informações em âmbito global.

---

[7] Recentemente foi divulgado que a cidade de Aparecida do Norte, estado de São Paulo começa a levar internet gratuita para os cidadãos. Disponível em: <https://www.aparecida.go.gov.br/prefeitura-de-aparecida-comeca-a-levar-internet-gratuita-a-200-cantos-da-cidade/> Acesso em 25 de janeiro de 2023.

[8] Depois da propagação da pandemia COVID-19 que impôs à população o uso de máscaras, a *Apple*, como divulga em seu site, aumentou a tecnologia do Face ID para que o reconhecimento se dê inclusive com o uso de máscara. Disponível em: https://support.apple.com/pt-br/HT213062 Acesso em 25 de janeiro de 2023

[9] Disponível em: https://support.apple.com/pt-br/HT208108#:~:text=Para%20come%C3%A7ar%20a%20usar%20o,lo%20usando%20o%20Face%20ID. Acesso em: 25 de janeiro de 2023

Isso tende a se intensificar com o aumento progressivo do acesso à internet móvel. Nos últimos anos foi amplamente divulgada a disputa[10] entre China x Estados Unidos pelo domínio da tecnologia 5G, que torna possível, em tese, a consolidação da sociedade como hiperconectada. Essa tecnologia ainda não foi amplamente implementada no Brasil, sequer em suas principais capitais.

De toda forma, a tecnologia 6G já está prevista para ocorrer mundialmente em 2030[11] e pretende ser 100 vezes mais rápida[12] que a atual. Com isso surgirão muitas oportunidades de criação e desenvolvimento de outras tecnologias.

Desde já os exemplos de inovação decorrentes desse conceito de onipresença da tecnologia são diversos. Cada vez mais diminui o espaço-tempo necessário para que os itens sejam conectados entre si (O'NEIL, 2020). É o que vemos com *smart speakers* e *smart homes* onde basta um comando de voz para que toda a casa se ilumine, se refrigere e diversas outras formas de interação ocorram. Até mesmo itens perdidos e animais de estimação podem ser facilmente encontrados através de seu smartphone, via conexão *bluetooth* e um *itag.*

Isso se expande do aspecto residencial para o social com o conceito de *smart city* que "utiliza a tecnologia para prestar de forma mais eficiente os serviços urbanos, melhorar a qualidade de vida das pessoas e transformar a relação entre entidades locais, empresas e cidadãos proporcionando uma nova forma de viver na cidade.*"*(CUNHA, et al, 2016).

Nesse contexto, dentro das mais diversas subáreas, como meio ambiente, mobilidade, saúde etc as tecnologias são desenvolvidas e aplicadas para melhorar a vida em sociedade, na busca ideal de fazer com que os serviços

---

[10] Disponível em: https://g1.globo.com/tecnologia/noticia/2021/11/05/5g-entenda-a-briga-entre-estados-unidos-e-china.ghtml Acesso em 28 de janeiro de 2023

[11] Disponível em: https://www.correiobraziliense.com.br/ciencia-e-saude/2022/10/5045335-6g-pesquisador-brasileiro-explica-tecnologia-que-substituira-o-5g-em-2030.html Acesso em 28 de janeiro de 2023

[12] Disponível em: <https://www.techtudo.com.br/noticias/2022/06/internet-6g-chega-em-2030-e-sera-100-vezes-mais-rapida-que-o-5g.ghtml> Acesso em 28 de janeiro de 2023

à disposição da população sejam substancialmente integrados e cada vez mais eficientes.

Além disso, a partir deste conceito que pretende tornar a tecnologia onipresente, se percebe que o trabalho humano fica menos exposto. As pessoas trabalham muito mais atrás dos computadores, dentro das empresas ou até suas próprias casas, principalmente depois dos efeitos da pandemia covd-19. Como exemplo, há alguns anos grandes marcas como a *Amazon* já se utilizam de drones e robôs para fazer entregas de compras nos Estados Unidos da América[13], assim como recentemente outras marcas famosas, como *Uber Eats,* lançaram naquele mesmo país os robôs delivery[14] de comidas e bebidas.

Também se constata a mesma situação para os veículos autônomos que já estão em uso e logo não necessitarão sequer da atenção do passageiro para tráfego viário. A UBER já vem anunciando a pretensão de utilização em massa destes veículos para fornecimento de táxi nos Estados Unidos.[15]

A tendência é que esse cenário cresça e a tecnologia se torne cada vez mais relacionada e composta ao ambiente que vivemos e, assim, imperceptível: “the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it”[16] (Madakam; Ramaswamy; Tripath, 2015).

Também como exemplo existem os jogos e interações de realidade aumentada, que replicam o mundo e as pessoas, por meio de avatares.

Recentemente houve um bombardeamento de informações sobre o *metaverso*, sistema que mistura a realidade aumentada com ambiente virtual do

---

[13] Isso é o que a Forbes vem divulgando. Disponível em: https://forbes.com.br/forbes-tech/2022/01/conheca-5-empresas-que-ja-utilizam-drones-e-robos-para-entregas/ Acesso aos 25 de janeiro de 2023

[14] O mesmo na CNN. Disponível em: <https://www.cnnbrasil.com.br/business/uber-eats-dos-eua-lanca-servico-de-entrega-feito-por-robos/> Acesso aos 25 de janeiro de 2023

[15] Disponível em: https://autopapo.uol.com.br/curta/uber-comeca-a-utilizar-carros-autonomos-a-partir-de-2022/ Acesso aos 25 de janeiro de 2023

[16] Tradução livre: “...as tecnologias mais profundas são aquelas que desaparecem. Elas se entrelaçam no tecido da vida cotidiana até que sejam indistinguíveis dele”.

grupo META[17], do *facebook.* Tal como se define: “assim como a internet, o metaverso vai ajudar você a se conectar com as pessoas quando não estiverem fisicamente no mesmo lugar, nos aproximando ainda mais da sensação de estar juntos pessoalmente.”[18]

Esse sistema recentemente começou a ser utilizado e propõe uma interação humana ampla, mas virtual. Inclui a possibilidade de reuniões[19] em um *workspace*, com toda organização do encontro via digital e, principalmente, a própria participação na reunião virtual, por meio de avatares e através da utilização de óculos de realidade aumentada, com uma experiência imersiva.

Para além desse aspecto individual, hoje já conhecemos o conceito indústria 4.0 (ou quarta revolução industrial) que é utilizado para descrever a automação industrial e a integração da tecnologia no âmbito da indústria, que inclui uso de avançada robótica, com maquinário dotado de inteligência artificial, utilização de armazenamento de dados via nuvem, big data e internet das coisas, visando o aumento de eficiência, produtividade e melhora do desenvolvimento da atividade em si.

> A quarta Revolução Industrial, também conhecida como Indústria 4.0, tem trazido mudanças para as organizações contemporâneas. A principal transformação é a produção massiva de dados e informações disseminadas por objetos, pessoas e elementos biológicos (SCHWAB, 2016). Esse novo contexto foi reconhecido a partir de 2013 na Alemanha e desde então vem influenciando pesquisas científicas e a indústria manufatureira em diversos países. As empresas sofrerão mudanças significativas em sua estrutura e nos modos de produção, modificando, inclusive, a vida em sociedade. A Indústria 4.0 (I4.0) traz novas oportunidades de negócios e novas formas de compreensão a respeito da qualidade de vida da população. A Industria 4.0 possui várias tecnologias que a complementam, dentre elas estão os recursos de *Big Data.* (OTTONICAR; ATAYDE; SANTA-EULALIA, 2019)

[17] A empresa META divulga como seu sistema funciona. Disponível em: https://about.meta.com/company-info/ Acesso em 28 de janeiro de 2023

[18] Disponível em: <https://about.meta.com/br/what-is-the-metaverse/> Acesso em: 28 de janeiro de 2023

[19] Disponível em: https://www.meta.com/work/workrooms/ Acesso em: 28 de janeiro de 2023

Big Data é o processamento e armazenamento ampliado de dados[20] pelas máquinas, o que é humanamente impossível, porque o número dessas informações pode ser infinito, assim como a velocidade desse processamento. “Os Big Data podem ser entendidos como o armazenamento de dados provenientes de sistemas e da web a fim de que possam ser utilizados no futuro.” (OTTONICAR; ATAYDE; SANTA-EULALIA, 2019)

> ...o *Big Data,* que nada mais é do que um conjunto gigantesco de informações que, devido a sua quantidade e velocidade de geração, ao poderiam ser examinados por um único indivíduo. Assim, atrelando-se o sistema de inteligência artificial à capacidade de aprendizado das máquinas, as possibilidades de aplicações úteis aos seres humanos são enormes. (SIQUEIRA NETO; LANNES; BARBOSA DE MIRANDA, 2020)

Por sua vez, a internet das coisas (IoT – Internet of Things) “descreve a rede de objetos físicos incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet”[21].

A acepção de internet das coisas é variável perante os sujeitos da área, havendo diferentes definições em âmbito acadêmico e profissional, apesar de seu uso e definição serem atribuídos ao expert Kevin Ashton. Todas elas indicam que a internet antes conhecida tratava sobre dados desenvolvidos por pessoas, já a nova sobre dados desenvolvidos por coisas (Madakam; Ramaswamy; Tripath, 2015).

> A melhor definição para Internet das Coisas seria: “Uma rede aberta e abrangente de objetos inteligentes que possuem a capacidade de se auto-organizar, compartilhar informações, dados e recursos, reagindo e agindo diante de situações e mudanças no ambiente (Madakam; Ramaswamy; Tripath, 2015).[22]

---

[20] Para mais informações, ler: VERONESE, Alexandre. Os Direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. in Lei Geral de PROTEÇÃO DE DADOS PESSOAIS e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019.

[21] Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/ Acesso em: 28 de janeiro de 2023

[22] Tradução livre. Texto original: “The best definition for the Internet of Things would be: “An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment”

A internet das coisas é a rede que pretende vincular objetos, que podem ser domésticos ou industriais, por meio de sistemas e softwares, tornando-os integrados e com capacidade de processamento e compartilhamento de dados e autoaprendizado. A internet das coisas vem evoluindo: “com mais de 7 bilhões de dispositivos IoT conectados hoje, os especialistas esperam que esse número cresça para 10 bilhões em 2020 e 22 bilhões em 2025.” [23]

> Essa etapa da evolução da internet também possibilita, mais uma vez, novos modelos de negócios. A fábrica conectada (Industria 4.0), a cidade inteligente (“smart city”), os carros autônomos em rede, e as diversas variantes de computação em nuvem operadas comercialmente são palavras-chave. Mesmo autonomamente, na forma de “smart home”, com o mundo exterior: a geladeira reconhece, por conta própria, que o suprimento de leite está chegando ao fim e encomenda, no supermercado da esquina, um refil. Um modelo desses só funciona, naturalmente, caso as sacolas de leite equipadas com chips RFID possam se comunicar com a geladeira e essa, por sua vez, com o supermercado. Com dimensão completamente nova. Para conceiturar a internet das coisas, pode-se falar em “allnet” ou simplesmente “net” (HILGENDORF, 2020, p. 171)

A internet tal como se conhece hoje será logo esquecida e substituída pela chamada “allnet”, que é a internet onipresente, capaz de conectar tudo ao seu redor.

> Já em futuro próximo, a “internet das coisas” irá substituir a internet atual. Hoje, já não são apenas os computadores de mesa que se comunicam entre si. Há muito tempo, a internet se tornou móvel com os notebooks, tablets e smartphones. Em seguida, por meio da miniaturização de máquinas (p. ex. RFID-Chips), cada vez mais itens do nosso cotidiano (p. ex. peças de roupas), irão armazenar, enviar e receber dados. Carros semiautônomos receberão, em tempo real, dados e softwares necessários a partir da internet, e também trocarão dados entre si. Nas fábricas do futuro, máquinas semiautônomas estarão funcionando conectadas entre si via internet. As máquinas em rede tornar-se-ão, por assim dizer, os olhos, ouvidos e mãos da internet. Essa nova internet, onipresente na vida profissional e no cotidiano, é melhor descrita pelo termo “allnet” (HILGENDORF, 2019)

[23] Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/ Acesso em 28 de janeiro de 2022

1.2. INTELIGÊNCIA ARTIFICIAL: AGENTES INTELIGÊNTES E SISTEMAS AUTÔNOMOS COM AUTOAPRENDIZAGEM

Todo esse fenômeno da digitalização deságua nos agentes inteligentes que são os sistemas que processam informações de forma autônoma diante de regras e softwares previamente instalados por desenvolvedores.

> Agentes inteligentes – em suas diversas formas – são utilizados ali onde o processamento rápido de grande quantidade de informações demanda combinações precisas e uma reação rápida, ou também ali onde o uso de forma física, que supera as possibilidades humanas, é necessário. Há, hoje, agentes inteligentes em diversos setores da vida: eles determinam – na forma simples de um agente de software, por exemplo, as máquinas de busca na internet -, nosso acesso à informação e, com isso, em certa medida, nossa percepção da realidade: “agentes de software de leitura” em corretores de bolsa de valores online tomam decisões autônomas de compra e venda de valores mobiliários a partir de determinadas informações. Sistemas complexos como “bisturis inteligentes” e “robôs de corte” (fäsroboter) realizam operações cirúrgicas e equipamentos de voo inteligentes (drones) são usados não só para fins militares, mas também para vigilância e segurança em âmbitos civis sensíveis e, talvez em futuro breve, para entrega de mercadorias. (GLESS, WEIGEND, 2019, p. 38)

Conforme define a União Europeia, a inteligência artificial (ou mundialmente conhecida como AI) é uma “família de tecnologias em rápida evolução capaz de oferecer um vasto conjunto de benefícios económicos e sociais a todo o leque de indústrias e atividades sociais”[24].

> Ao melhorar as previsões, otimizar as operações e a afetação de recursos e personalizar o fornecimento dos serviços, a utilização da inteligência artificial pode contribuir para resultados benéficos para a sociedade e o ambiente e conceder vantagens competitivas às empresas e à economia europeia. Essa ação torna-se especialmente necessária em setores de elevado impacto, incluindo os domínios das alterações climáticas, do ambiente e da saúde, do setor público, das finanças, da mobilidade, dos assuntos internos e da agricultura. Contudo, os mesmos elementos e técnicas que produzem os benefícios socioeconómicos da IA também podem trazer novos riscos ou consequências negativas para os cidadãos e a sociedade. (Regulamento Inteligência Artificial, 2021).

[24] Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligencia Artificial). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN Acesso 06 de fevereiro de 2023.

O conceito de agentes inteligentes pode ser subdividido em três grandes categorias, sendo a primeira “sistemas de simples processamento de dados”, a segunda “sistemas abertos” e a terceira “sistemas inteligentes” (GLESS, WEIGEND, 2019, p. 38).

Na primeira estariam contidos aqueles sistemas de baixa complexidade em que o desenvolvedor já estabelece a forma completa da captação dos dados do mundo exterior, assim como se dará seu tratamento. Na segunda categoria estariam contidos aqueles que são submetidos a alguma interferência dos dados externos e são capazes de, autonomamente, perceber o ambiente, como um robô aspirador de pó, por exemplo. Já na terceira categoria estariam contidos todos aqueles que captam dados externos, os armazenam e podem vir a utilizá-los para tomada de decisão. Essa última categoria engloba desde sistemas mais simples, como um buscador de pesquisa na internet até mais complexos, como os veículos autônomos (GLESS, WEIGEND, 2019).

O que interessa principalmente ao presente estudo é a terceira categoria, mas em sua modalidade mais complexa. Ou seja, quando a máquina detém inteligência artificial que lhe outorga a capacidade de agir sem um comando humano direto. Nessa oportunidade preferiu intitulá-las “sistemas autônomos”, que são as “máquinas que tomam decisões em situações concretas sem comando humano imediato” (HILGENDORF, 2020).

Esses referidos sistemas autônomos são possíveis a partir determinadas configurações de software e podem ainda, em caráter mais avançado, possuir o que se convencionou chamar de “autoaprendizagem das máquinas” ou “machine learning”, que é uma autonomia decisória diante de informações captadas de terceiros e de ambientes e processadas pelas próprias máquinas. São aquelas desenvolvidas para, diante de uma programação pré-estabelecida, aprender diante de dados externos e se comportar adequadamente independente de outras ações humanas (HILGENDORF, 2020).

Essa autonomia decorre de softwares pré-instalados que preparam a máquina para deliberar sobre o que fazer a partir dos algoritmos previamente inseridos em seus sistemas, somados a dados captados no ambiente físico ou digital, que são combinados.

Os softwares que detêm “machine learning” já são encontrados nos veículos autônomos. Outro exemplo é o robô *Rover Perseversance* da NASA que foi enviado à Marte, desenvolvido para responder à adversidades, habilitado para enfrentar problemas e programado para decidir por si mesmo o que fazer. O robô foi equipado com um software - Autonomous Exploration for Gathering Increased Science, ou AEGIS - que autoriza que ele próprio escolha as rochas de marte que serão submetidas à análise, sem necessidade de qualquer intervenção humana.[25] Nesse caso, o humano poderia se tornar um verdadeiro espectador da atividade do robô.

Há também um amplo debate sobre o uso de armas autônomas nesse formato de “machine learning”, isto é, que usam inteligência artificial para identificar, escolher e matar humanos procurados sem necessidade de intervenção humana direta e a partir de dados externos por elas obtidos.

Ao menos desde 2014, discute-se em âmbito internacional a possibilidade de utilização das chamadas lethal autonomous weapon systems – LAWS - ou, informalmente, *killer robots*, na Convenção das Nações Unidas sobre Certas Armas Convencionais (UN CCW). Estas discussões formaram o “Grupo de Especialistas Governamentais” (GGE) que debatem a (im)possibilidade de implementação e suas formas (o grupo tem como função examinar suas dimensões tecnológica, militar, ética e legal)[26].

---

[25] Conforme noticiado pela NASA. Disponível em: https://mars.nasa.gov/mars2020/mission/status/383/perseverance-now-selects-its-own-targets-to-zap/ Acesso em: 13 de janeiro de 2023

[26] Convention of Certain Conventional Weapons. Disponível em: <https://meetings.unoda.org/ccw-mhcp/convention-certain-conventional-weapons-meeting-high-contracting-parties-2022> Acesso em: 05 de fevereiro de 2023.

O serviço de pesquisa do Congresso Americano divulgou em novembro de 2022[27] a atual situação das LAWS no que se refere aos Estados Unidos da América, definindo-as como uma classe especial de sistemas de armas que se utilizam de sensores e algortimos para identificar o alvo e operar sem atuação humana manual, ou seja, de forma independente.[28]

Como está disposto no informativo, não há uma definição concreta do que seriam as LAWS em contexto internacional, motivo por que os EUA a partir de seu Departamento de Defesa criou uma diretiva própria:

> "...sistemas de armas que, uma vez ativados, podem selecionar e engajar alvos sem intervenção adicional de um operador humano". Esse conceito de autonomia também é conhecido como "humano fora do circuito" ou "autonomia total". A diretiva contrasta o LAWS com sistemas de armas autônomos supervisionados por humanos, ou "humanos no circuito", nos quais os operadores têm a capacidade de monitorar e interromper o engajamento de uma arma. Outra categoria são os sistemas de armas semi-autônomos, ou "humanos no circuito", que "enfrentam apenas alvos individuais ou grupos-alvo específicos que foram selecionados por um operador humano". As armas semiautônomas incluem as chamadas armas "dispare e esqueça", como certos tipos de mísseis guiados, que produzem efeitos em alvos identificados por humanos usando funções autônomas […][29]

---

[27] U.S. Policy on Lethal Autonomous Weapon Systems. Disponível em: https://www.google.com/search?q=Defense+Primer%3A+U.S.+Policy+on+Lethal+Autonomous+Weapon+Systems&oq=Defense+Primer%3A+U.S.+Policy+on+Lethal+Autonomous+Weapon+Systems&aqs=chrome..69i57.278j0j7&sourceid=chrome&ie=UTF-8#:~:text=Resultados%20da%20pesquisa-,U.S.%20Policy%20on%20Lethal%20Autonomous%20Weapon%20Systems,https%3A//crsreports.congress.gov%20%E2%80%BA%20product%20%E2%80%BA%20pdf,-PDF Acesso em: 05 de fevereiro de 2023.

[28] Lethal autonomous weapon systems (LAWS) are a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system. Although these systems are not yet in widespread development, it is believed they would enable military operations in communications-degraded or -denied environments in which traditional systems may not be able to operate

[29] DODD 3000.09 defines LAWS as "weapon system[s] that, once activated, can select and engage targets without further intervention by a human operator." This concept of autonomy is also known as "human out of the loop" or "full autonomy." The directive contrasts LAWS with human supervised, or "human on the loop," autonomous weapon systems, in which operators have the ability to monitor and halt a weapon's target engagement. Another category is semi-autonomous, or "human in the loop," weapon systems that "only engage individual targets or specific target groups that have been selected by a human operator." Semiautonomous weapons include so-called "fire and forget" weapons, such as certain types of guided missiles, that deliver effects to human-identified targets using autonomous functions.

A diretiva faz um direcionamento para a necessidade da intervenção humana, em maior ou menor nível e aponta para a necessidade do software ser testado e constantemente avaliado para garantir o adequado funcionamento, inclusive nos sistemas com autoaprendizagem:

> O DODD 3000.09 exige que o software e o hardware de todos os sistemas, incluindo armas autônomas letais, sejam testados e avaliados para garantir que funcionem conforme previsto em ambientes operacionais realistas contra adversários adaptativos; concluir os engajamentos em um prazo consistente com as intenções do comandante e do operador e, se não puder fazê-lo, encerrar os engajamentos ou buscar informações adicionais do operador humano antes de continuar o engajamento; e são suficientemente robustos para minimizar falhas que podem levar a engajamentos não intencionais ou à perda de controle do sistema para partes não autorizadas. Quaisquer alterações no estado operacional do sistema, por exemplo, devido ao aprendizado de máquina, exigiriam que o sistema passasse por testes e avaliações novamente para garantir que manteve seus recursos de segurança e capacidade de operar conforme pretendido.[30]

Desde novembro de 2022 tem chamado atenção mundial uma ferramenta gratuita online chamada Chat GPT (Generative Pre-Training Transformer)[31], criada pela OpenAI, que é uma tecnologia dotada de inteligência artificial para construção de diálogos e textos completos. Trata-se de um *chatbot*, tal como um robô de atendimento ao cliente de grandes marcas, mas muito mais robusto, podendo ser considerado um sistema autônomo. Pode esse *chatbot* criar literatura, gerar relatórios, escrever currículos, e-mails corporativos e até textos acadêmicos. Nos testes, o sistema foi aprovado no exame da ordem e no exame de licenciamento médico dos Estados Unidos[32].

---

[30] DODD 3000.09 requires that the software and hardware of all systems, including lethal autonomous weapons, be tested and evaluated to ensure they Function as anticipated in realistic operational environments against adaptive adversaries; complete engagements in a timeframe consistent with commander and operator intentions and, if unable to do so, terminate engagements or seek additional human operator input before continuing the engagement; and are sufficiently robust to minimize failures that could lead to unintended engagements or to loss of control of the system to unauthorized parties. Any changes to the system's operating state—for example, due to machine learning—would require the system to go through testing and evaluation again to ensure that it has retained its safety features and ability to operate as intended"

[31] Disponível em: https://chat.apps.openai.com/auth/login Acesso em: 10 de fevereiro de 2023.

[32] Notícia disponível em: https://www.terra.com.br/byte/chatgpt-passa-em-prova-de-mba-oab-dos-eua-e-de-capacitacao-medica,9b884393b116e0c0bc5bf35b5e066d63wj7tf4rv.html Acesso em 12 de fevereiro de 2023.

Em consulta, o ChatGPT se descreveu da seguinte forma (a partir da pergunta “o que é o ChatGPT?”):

> ChatGPT é um modelo de linguagem de grande porte criado pela OpenAI. Ele foi treinado usando uma grande quantidade de textos da internet para gerar texto de forma autônoma com base em um prompt ou tópico dado. Isso significa que, quando você fornece uma pergunta ou tópico ao ChatGPT, ele poderá responder com uma resposta coerente e natural. O ChatGPT é amplamente utilizado para conversação humana, perguntas e respostas, geração de texto e outras aplicações de processamento de linguagem natural.[33]

O Tribunal de Justiça de Minas Gerais tem estudado utilizar a plataforma Sistema Assistente Virtual de Inteligência Artificial (SAVIA), que é baseada no ChatGPT, para assistência dos magistrados e servidores, como também dos prestadores de serviços da área administrativa para a confecção de documentos.[34]

O ChatGPT é mais um sistema autônomo dotado de autoaprendizagem, que a partir de cada informação buscada e fornecida aprende, armazena dados e se aprimora. Um ótimo exemplar do que seria o sistema autônomo para fins do presente desenvolvimento.

1.3. DIRTY DATA

Dirty data, em tradução literal para o português seria dados sujos. A melhor tradução para “dirty data”, a fim de entender seu impacto negativo no desenvolvimento da inteligência artificial seria “dados não coesos” ou “dados incompletos” (ORTIZ; SAYEG, 2020)

Os dados são a fonte de todo o desenvolvimento da inteligência artificial. São todas as informações inseridas nos sistemas e softwares. Em outros termos,

---

[33] Disponível em: https://chat.openai.com/chat Acesso em: 12 de fevereiro de 2023

[34] Disponível em: https://www.jota.info/justica/chat-gpt-tjmg-estuda-uso-de-ferramenta-de-inteligencia-artificial-08022023 Acesso em: 12 de fevereiro de 2023

a máquina precisa operar a partir de algo e esse “algo” são as informações obtidas a partir de dados inseridos nos softwares ou captados pela máquina a partir do ambiente externo, operadores e usuários etc.

Sendo estes dados equivocados, mentirosos, falsos ou até mesmo racistas e misóginos, podem prejudicar ou até corromper integralmente o resultado alcançado pela inteligência artificial.

Todos os dados não coesos podem ser considerados “*dirty data”,* independentemente se foram implantados deliberadamente para corromper o sistema ou se apenas correspondam a um reflexo das relações sociais (SIQUEIRA NETO; LANNES; BARBOSA DE MIRANDA, 2020)

Nos casos em que a máquina se trata de sistema autônomo que detém software de autoaprendizagem a evitação de *dirty data* é de ainda maior relevância, pois a base de seu aprendizado - a partir do qual tomará decisões no futuro - são, para além dos dados inseridos inicialmente quando da criação do sistema, os demais dados e informações obtidos a partir do ambiente e/ou fornecidos por terceiros no curso do desenvolvimento da própria atividade da máquina.

Isso precisa ser considerado pelos desenvolvedores para fins de criar mecanismos de proteção aos dados que serão efetivamente absorvidos pelos sistemas autônomos.

2. IMPACTOS À SOCIEDADE

Diversas são as áreas onde há uma estreita relação das pessoas com sistemas autônomos com autoaprendizagem. Por isso que cada vez mais se vê notícias, em âmbito mundial, de violações a bens jurídicos causados por máquinas.

2.1. CASOS CONCRETOS MIDIÁTICOS

O jornal Deseret News, em 09 de dezembro de 1981, já anunciava[35] o falecimento de Kenji Urada, onde citava tratar-se do primeiro acidente dessa natureza no Japão, país que detinha, ao tempo do ocorrido, o maior polo mundial de robôs.[36] Kenji era empregado de uma Industria da Kawasaki em Akashi e, ao sofrer acidente, morreu esmagado por braço robô.

Conforme as notícias, o acidente ocorreu quando Kenji tentou verificar um mau funcionamento da máquina. Teria o funcionário a ligado de forma acidental depois de retirar de maneira inadequada uma proteção que fazia com que o robô ficasse desligado enquanto estava sendo reparado.

Essa notícia demonstra que não é de hoje que o aprofundamento da relação humano-máquina pode gerar riscos e efetivos danos à sociedade e às pessoas. O Guinnes World Records aponta que o primeiro caso de morte causada por robô teria acontecido ainda antes disso, em 25 de janeiro de 1979, quando o Sr. Robert Williams, nos Estados Unidos, teve a cabeça presa e foi morto também por um braço de robô na fábrica da FORD Motor Company em Michigan.[37]

---

[35] Disponível em: <https://news.google.com/newspapers?id=1t00AAAAIBAJ&sjid=xoMDAAAAIBAJ&pg=6313,2597702&dq=kenji+urada&hl=en> Acesso em 22 de fevereiro de 2022

[36] Disponível em: <https://www.theguardian.com/theguardian/2014/dec/09/robot-kills-factory-worker> Acesso em 22 de fevereiro de 2022

[37] Disponível em: <https://www.guinnessworldrecords.com/world-records/first-human-to-be-killed-by-a-robot> Acesso em 10 de outubro de 2022

Casos dessa natureza não saíram da mídia desde então, apenas se agravaram na medida em que a tecnologia avança. Em 2012 houve o primeiro acidente decorrente de veículo semiautônomo, que ocorreu em Aschaffenburg, na Alemanha.

2.1.1. Caso Aschaffenburg

Em Aschaffenburg, 2012, um condutor de um veículo de aproximadamente 60 anos sofreu um derrame cerebral e perdeu a consciência, quando involuntariamente virou o volante para a direita em direção à arbustos (HILGENDORF, 2020).

O carro, que possuía tecnologia de assistente de manutenção de faixa de rolagem reconduziu o carro de volta para a via e prosseguiu em alta velocidade em direção à cidade de Alzenau, matando uma mulher e uma criança e ferindo um homem que sobreviveu.[38]

Aschaffenburg foi o primeiro caso que um sistema autônomo (na verdade, semiautônomo) machucou seres humanos (HILGENDORF, 2020). Apesar de ter sido pouco divulgado mundialmente, abriu amplo debate na Alemanha sobre essas ferramentas automatizadas em veículos, porquanto a partir dele foi possível verificar diversas problemáticas possíveis ao se admitir um comando “automático” pela própria máquina.

Como ponta HILGENDORF (2020, p. 49 a 51 e 67/68), para o direito civil Alemão o caso não apresentou grandes mistérios, porquanto existe responsabilidade pelo risco (§7 StVG) ao titular do veículo, que deveria arcar com a indenização. Mas, de fato, trouxe problema para o campo penal, que na Alemanha, assim como no Brasil, não admite responsabilidade objetiva, como também porque o condutor, aparentemente, foi tão vítima quanto os demais humanos afetados. Assim, o raciocínio deveria seguir pela responsabilidade do

[38] Disponível em: https://www.youtube.com/watch?v=RDCbsn_5On4 Acesso em 10 de fevereiro de 2023

fabricante, mas essa precisa ser pensada de forma que não torne o desenvolvimento da tecnologia inviável (HILGENDORF, 2020).

2.1.2. Caso Baunatal

Alcançou os principais jornais do mundo[39] a manchete que ficou conhecida como caso Baunatal[40] - porque ocorreu na cidade de Baunatal - na Alemanha, em 2015, com um empregado de 22 anos, que dentro da fábrica da Volkswagem foi agarrado e esmagado por um braço de robô que não estava protegido e, em decorrência disso, veio a falecer. Ao que consta, o robô foi ligado por outro funcionário antes do momento previsto (HILGENDORF, 2020).

As manchetes dos jornais afirmavam que o caso parecia ser o primeiro de morte causada por robô na Alemanha e que as autoridades estavam a investigar se era possível responsabilizar alguém pela morte do funcionário.

O porta-voz da Volkswagem, Heiko Hillwig, afirmou que as conclusões iniciais indicavam para erro humano e não problema com o funcionamento do robô, que é usado para diversas tarefas no processo de montagem de veículos e opera em área restrita transportando peças.[41] A matéria vinculada no The Guardian[42] apontou que a DPA - The German Press Agency informava que os promotores consideravam apresentar acusações contra o funcionário que ligou indevidamente a máquina, pois ao que parecia, tratava-se de erro humano.

Este foi o primeiro caso amplamente divulgado de um robô autônomo (ou semiautônomo) que matou um humano na Alemanha. A tendência já era crescente naquela época e assim permanece, porque crescente também é a participação das máquinas dotadas de sistemas autônomos na vida em

---

[39] Disponível em: <https://www.washingtonpost.com/news/morning-mix/wp/2015/07/02/robot-grabs-man-kills-him-in-german-car-factory/> Acesso em: 10 de outubro de 2022
[40] Disponível em: <https://g1.globo.com/mundo/noticia/2015/07/robo-agarra-e-mata-trabalhador-dentro-de-fabrica-da-volkswagen.html> Acesso em: 10 de outubro de 2022
[41] Disponível em: <https://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany> Acesso em: 10 de outubro de 2022
[42] Disponível em: <https://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany> Acesso em: 10 de outubro de 2022

sociedade, não se limitando mais a ambientes restritos como indústrias. O contato dessas máquinas com seres humanos está cada vez maior e mais imperceptível (HILGENDORF, 2020).

2.1.3. Caso Tay

Tay foi um *chatbot* criado pela *Microsoft* em 2016 para operar nas principais redes sociais e no *twitter* pela conta @*tayandyou* como um experimento destinado a adolescentes. Ao que consta, Tay era um chatbot dotado de inteligência artificial, criado para conversar por *posts* a partir de sua interação com os efetivos usuários humanos.[43]

A *Microsoft* explicou que a Tay operava por meio de algoritmos. Fazia buscas reiteradas de conversas de adolescentes e cada vez que os usuários interagiam com o perfil ele captava as informações e se aprimorava. Ou seja, a partir de inteligência artificial, aprendia com as informações fornecidas pelos usuários (SIQUEIRA NETO; LANNES; BARBOSA DE MIRANDA, 2020).

Ocorre que em 24 horas do lançamento o perfil precisou ser desabilitado pela empresa *Microsoft* porque o conteúdo das postagens era ofensivo e criminoso, fazia apologia ao nazismo e referências ao holocausto; bem como continha misoginia, entre outros conteúdos reprováveis e/ou criminosos[44]:

> Em março de 2016, a Microsoft lançou um avatar de comunicação (sprachavatar) online, que deveria conversar com pessoas e aprender a partir de suas reações. Um comunicador artificial como esse poderia ser empregado, por exemplo, em lojas, museus, em hospitais, em asilos ou na educação de crianças. No entanto, manipuladores tiveram a ideia de, em algumas horas, “alimentar” Tay de respostas que fizeram o sistema se tornar racista e misógino. Por fim, as respostas da Tay eram tão radicais que a

[43] Disponível em: <https://twitter.com/geraldmellor/status/712880710328139776?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E712880710328139776%7Ctwgr%5Ed762487f856bcbdb1c7acb833dd9faa1140d9e51%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fwww.theverge.com%2F2016%2F3%2F24%2F11297050%2Ftay-microsoft-chatbot-racist> Acesso em: 22 de dezembro de 2022

[44] Notícia disponível em: https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech> Acesso em: 22 de dezembro de 2022

> Microsoft precisou desligar o sistema. Tay respondeu “errado” (com pessoas erradas”) (HILGENDORF, 2020, p. 120)

É possível deduzir, pelo que foi amplamente divulgado, que isso se deu porque o software implementado na Tay foi criado para absorver as informações e alimentar o sistema com os referidos dados indiscriminadamente, sendo um exemplo claro de problema decorrente de *dirty data*.

2.1.4. Caso UBER

Em 2018, Elaine Herzberg, 49, foi atropelada e morta por um veículo autônomo Volvo XC90 da UBER (Uber self-driving car) enquanto atravessava uma rodovia com sua bicicleta em Tempe, Arizona, Estados Unidos da América.[45]

Pelo que foi divulgado pela mídia, a apuração policial baseada em vídeo que estava sendo gravado no momento do acidente indicou que a motorista Rafaela Vasquez estava assistindo um episódio do programa de televisão *The Voice* em seu celular e, em tese, não viu o alerta emitido pelo carro para frear a tempo de evitar o acidente fatal.

Em 27 de agosto de 2020, o Maricopa County Grand Jury acusou Rafaela Vasquez de homicídio culposo (negligent homicide) pela morte de Elaine. O procurador do condado Allister Adel deu declaração de que “Dirigir distraído é questão de grande importância em nossa comunidade” e que “quando um motorista se senta ao volante de um carro, ele tem a responsabilidade de controlar e operar o veículo com segurança e de acordo com a lei.” [46] (traduções livres).

> RAFAEL STUART VASQUEZ, on or about March 18, 2018, with criminal negligence, did cause the death of ELAINE MARIE HERZBERG in violation

[45] Notícia divulgada pela BBC. Disponível em: <https://www.bbc.com/news/technology-54175359> Acesso em: 10 de fevereiro de 2023.
[46] Disponível em: <https://www.maricopacountyattorney.org/CivicAlerts.aspx?AID=751> Acesso em: 10 de fevereiro de 2023

> of A.R.S. §§ 13-1101, 131102, 28-3001, 28-3004, 28-3005, 28-3315, 13-701, 13-702, and 13-801. The State further alleges that the offense charged in this count is a dangerous felony because the offense involved the discharge, use, or threatening exhibition of a motor vehicle, a deadly weapon or dangerous instrument and knowing infliction of serious physical injury upon \ or the intentional or ELAINE MARIE HERZBER of A.R.S. §§ 13105 and 13704. G , in violation ("A True Bill") ALLISTER ADEL MARICOPA COUNTY ATTORNEY Date: August 27, 2020 Tiffany Brady Deputy County Attorney sk FOREPERSON OF THE GRAND JURY[47]

Perante o Maricopa County Superior Court, em 15 de setembro de 2020, Rafaela se declarou inocente e foi liberada com monitoramento por tornozeleira.

Até o presente momento o caso não foi julgado, mas detém grande repercussão já que a motorista afirma ser apenas a operadora da máquina[48] e, portanto, ser a UBER responsável pelo acidente. Sua defesa também alega que ela não estava assistindo ao programa de televisão. Em requerimento formulado pelos defensores de Rafaela em 13 de junho de 2022, em tradução livre:

> Em 18 de março de 2018, Elaine Herzberg, drogada por metanfetamina e vestida com roupas escuras, começou a atravessar um trecho escuro da Mill Avenue, no meio da quadra, enquanto empurrava uma bicicleta que não tinha refletores adequados e farol dianteiro, quando foi atingida por um veículo de teste automatizado da Uber. Seu escritório obteve uma acusação apresentando testemunho de que a colisão ocorreu porque a Sra. Vasquez, operadora do veículo automatizado Uber, estava assistindo a um programa de televisão em seu telefone, em vez de observar a estrada. O Grande Júri considerou a causa provável para homicídio culposo porque os promotores apresentaram evidências de que a Sra. Vasquez era uma motorista distraída que, durante momentos críticos de sua viagem, assistia ao The Voice em um telefone celular colocado em uma área entre a parte inferior do painel e o console central perto do joelho direito e sem prestar atenção na estrada. Mas, se o agente do caso, o detetive do Departamento de Polícia de Tempe, Marsland ("Marsland") se preocupasse em fazer uma revisão completa das evidências, incluindo simplesmente olhar para os telefones, ele saberia que sua premissa era falsa. Se os próprios promotores tivessem analisado minuciosamente as evidências antes de apresentar este assunto ao Grande Júri, ou tivessem revisado tudo por conta própria, eles poderiam ter optado por não prosseguir com este caso. Para ser claro, essa era uma evidência

[47] Tradução livre: RAFAEL STUART VASQUEZ, em ou por volta de 18 de março de 2018, com negligência criminal, causou a morte de ELAINE MARIE HERZBERG em violação da A.R.S. §§ 13-1101, 131102, 28-3001, 28-3004, 28-3005, 28-3315, 13-701, 13-702 e 13-801. O Estado alega ainda que o delito imputado nesta acusação é um crime perigoso porque o delito envolveu a descarga, uso ou exposição ameaçadora de um veículo motorizado, uma arma mortal ou instrumento perigoso e inflição consciente de lesão física grave sobre \ou o intencional ou ELAINE MARIE HERZBER de A.R.S. §§ 13105 e 13704. G, em violação ("A True Bill") ALLISTER ADEL MARICOPA COUNTY ADVOGADO Data: 27 de agosto de 2020 Tiffany Brady Vice-Procurador do Condado sk PRESIDENTE DO GRANDE JÚRI

[48] Notícia disponível em: https://www.wired.com/story/uber-self-driving-car-fatal-crash/ Acesso em 10 de fevereiro de 2023

> que estava disponível para eles desde 2018 - dois anos antes de seu escritório decidir cobrar de nosso cliente. A falha em revisar as evidências e simplesmente confiar no que foi dito, fez de toda a apresentação ao grande júri um exercício de ocultação de evidências claramente ilibatórias. Embora existam várias outras questões controversas neste caso sobre as quais as partes discordam, isso não pode ser um deles. Aqui, a evidência é clara. A Sra. Vasquez não estava assistindo The Voice, ou qualquer outro programa, no celular durante qualquer parte da rota do SUV naquela noite. Na verdade, ela estava apenas ouvindo o programa no Bluetooth do veículo por meio de seu telefone pessoal - uma atividade que o Uber autorizou seus motoristas a fazer. Isso foi facilmente verificável se Marsland ou os promotores tivessem se dado ao trabalho de revisar adequadamente as evidências. [49]

De toda forma, ao que interessa ao presente trabalho, constatou-se que a Uber, nem nenhum dos engenheiros do veículo foram não foi acusada criminalmente. Os Promotores encarregados do caso entenderam que não haveria base para a companhia ter responsabilidade penal ("no basis for criminal liability for the Uber Corporation"), ou algum de seus engenheiros.

O acidente foi o primeiro gravado envolvendo um veículo autônomo e causou o encerramento dos testes dessa tecnologia pela UBER no Arizona.

---

[49] "On March 18, 2018, Elaine Herzberg, impaired by methamphetamine and dressed in dark clothing, started across a darkened section of Mill Avenue, mid-block, while pushing a bicycle that lacked proper reflectors and a front headlight, when she was struck by an Uber automated test vehicle. Your office obtained an indictment by presenting testimony that the collision occurred because Ms. Vasquez, the operator of the Uber automated vehicle, was watching a television program on her phone, rather than watching the road. The Grand Jury found probable cause for negligent homicide because the prosecutors presented evidence that Ms. Vasquez was a distracted driver who, during critical moments of her trip, was watching The Voice on a cell phone placed in an area between the bottom of the dashboard and the center console near her right knee and not paying attention to the roadway. But, had the case agent, Tempe Police Department Detective Marsland ("Marsland´) bothered to do a thorough review of the evidence, including simply looking at the phones, he would have known that his premise was false. Had the prosecutors thoroughly reviewed the evidence themselves prior to presenting this matter to the Grand Jury, or reviewed it in toto on their own, they might have elected not to go forward with this case. 2 To be clear, this was evidence that had been available to them since 2018 - two years before your office decided to charge our client. Failure to review the evidence and simply relying upon what they were told, made the entire presentation to the grand jury an exercise in concealing clearly exculpatory evidence.3 While there are numerous other disputed issues in this case that the parties disagree about, this cannot be one of them. Here, the evidence is clear. Ms. Vasquez was not watching The Voice, or any other program, on cell phone during any part of the SUV's route that night. In fact, she was merely listening to the show on the vehicle's Bluetooth through her personal phone - an activity Uber had authorized its drivers to do. This was easily verifiable had Marsland or the prosecutors taken the time to properly review the evidence"

Pouco tempo depois a UBER viria a vender sua divisão de pesquisa e criação de veículos autônomos para a concorrência, uma empresa *startup* chamada Aurora.[50]

Mas, em 2022, a UBER voltou ao negócio dos veículos autônomos como "táxis". A empresa assinou um acordo de 10 anos com uma joint venture (Motional) entre a Hyundai e a Aptiv, para implantar veículos autônomos em suas plataformas de carona e entrega.

2.1.5. Casos Tesla

A Tesla Inc. tem como um de seus pontos altos de divulgação comercial os veículos autônomos. A empresa tem hoje disponível três sistemas em seus carros: "autopilot", "enhanced autopilot" e "full self-driving capability". De acordo as informações do próprio site esses sistemas estão em desenvolvimento, mas, a forma como são comercializados hoje não faz com que os veículos sejam efetivamente autônomos (atuantes sem a necessidade de um motorista atento):

> Autopilot and Full Self-Driving Capability
> Autopilot is an advanced driver assistance system that enhances safety and convenience behind the wheel. When used properly, Autopilot reduces your overall workload as a driver. Each new Tesla vehicle is equipped with eight external cameras and powerful vision processing to provide an additional layer of safety. All vehicles built for the North American market now use our camera-based Tesla Vision to deliver Autopilot features, rather than radar.
>
> Autopilot comes standard on every new Tesla. For owners who took delivery of their cars without Autopilot, there are multiple packages available for purchase, depending on when your car was built: Autopilot, Enhanced Autopilot and Full Self-Driving Capability.
>
> Autopilot, Enhanced Autopilot and Full Self-Driving Capability are intended for use with a fully attentive driver, who has their hands on the wheel and is prepared to take over at any moment. While these features are designed to become more capable over time, the currently enabled features do not make the vehicle autonomous.[51]

---

[50] Notícia disponível em: https://www.npr.org/2020/12/08/944337751/uber-sells-its-autonomous-vehicle-research-division#:~:text=Uber%20Sells%20Its%20Autonomous%20Vehicle%20Research%20Division%20%3A%20NPR&text=Uber%20Sells%20Its%20Autonomous%20Vehicle%20Research%20Division%20Uber%20has%20sold,core%20investment%20for%20its%20future. Acesso em 10 de fevereiro de 2022

[51] Tradução livre: "Piloto automático e capacidade total de direção autônoma. O piloto automático é um sistema avançado de assistência ao motorista que aumenta a segurança e a conveniência

O veículo com software full self-driving capability é o mais aprimorado da linha e inclui as funcionalidades do autopilot e do enhanced autopilot, além de identificar sinais de paradas e semáforos, desacelerar sozinho em caso de aviso de interferência etc. A promessa da marca é que conforme os softwares forem se desenvolvendo o veículo constantemente se atualizará sem fio. O futuro é a direção autônoma do carro.

Esse sistema está sendo oferecido desde 2015[52] e consta da informação oficial da marca que o sistema opera como uma assistência ao motorista e demanda um piloto totalmente atento, que deve manter suas duas mãos ao volante e preparado para assumir o controle a qualquer momento. Mas, seu CEO, Elon Musk, vem anualmente fazendo previsões de quando os carros terão capacidade plena de dirigir por si mesmos, sozinhos.[53]

Ocorre que os veículos Tesla estão constantemente envolvidos em acidentes graves, alguns fatais.

Em 2016 ocorreu um acidente que ficou conhecido como caso Emmentaler, que ocorreu na Suíça. Um jovem dirigia um tesla com piloto automático em uma autoestrada. Uma faixa da estrada estava em obras e o veículo não desviou, colidindo com a sinalização e um trator. O Tribunal Suíço,

---

ao volante. Quando usado corretamente, o piloto automático reduz sua carga de trabalho geral como motorista. Cada novo veículo Tesla é equipado com oito câmeras externas e um poderoso processamento de visão para fornecer uma camada adicional de segurança. Todos os veículos construídos para o mercado norte-americano agora usam nosso Tesla Vision baseado em câmera para fornecer recursos de piloto automático, em vez de radar. O piloto automático é padrão em todos os novos Tesla. Para os proprietários que receberam seus carros sem piloto automático, há vários pacotes disponíveis para compra, dependendo de quando seu carro foi construído: piloto automático, piloto automático aprimorado e capacidade total de direção autônoma. O piloto automático, o piloto automático aprimorado e a capacidade total de autocondução destinam-se a um motorista totalmente atento, que está com as mãos no volante e está preparado para assumir o comando a qualquer momento. Embora esses recursos sejam projetados para se tornarem mais capazes com o tempo, os recursos atualmente ativados não tornam o veículo autônomo”

[52] Disponível em: https://www.usatoday.com/story/tech/news/2016/10/19/tesla-announces-fully-self-driving-fleet/92430638/ Acesso em 10 de fevereiro de 2023.

[53] Disponível em: https://futurism.com/video-elon-musk-promising-self-driving-cars Acesso em 10 de fevereiro de 2023.

em julgamento de 30 de maio de 2018 entendeu pela responsabilidade do condutor no que tange ao dano. (HILGENDORF, 2020)

> Um motorista deve controlar constantemente seu veículo, de modo a poder cumprir seus deveres de cuidado. Isso só e possível caso ele esteja atento e focado na estrada e no trânsito [...]. No presente caso, é óbvio que o acusado estava desatento no momento decisivo – isso, sem dúvida, no momento do acidente, mas, também, pelo menos nos 20 segundos anteriores. De acordo com a clara posição do tribunal, é absolutamente impensável que ele tivesse colidido, sem frear (!), com um obstáculo na estrada nitidamente visível à distância, grande e chamativo [...], caso ele [...] tivesse prestado pelo menos um pouco de atenção à estrada [...]. (decisão da Corte Regional de Emmental-Oberaargau, p. 15)[54]

Em 2022 um veículo Tesla model S que estava em modo self-driving capability causou um grande acidente envolvendo outros 8 carros em San Francisco, na San Francisco Bay Brigde[55].

O acidente ocorreu no dia de Ação de Graças, 24.11.2022, e as câmeras da rodovia mostram o veículo Tesla freando de forma repentina injustificadamente, causando um acidente que envolveu outros oito veículos. Nove pessoas ficaram feridas.[56] O vídeo do ocorrido, em diferentes ângulos de imagem, está disponível em: *https://theintercept.com/2023/01/10/tesla-crash-footage-autopilot/* .

Ocorre que apenas algumas horas antes do acidente, no mesmo dia 24.11.2022, Elon Musk, CEO da Tesla, havia anunciado em sua conta no twitter (@elonmusk) que o Tesla “Full Self-Driving” estava disponível para todos os consumidores da América do Norte: “Tesla Full Self-Driving Beta is now available to anyone in North America who requests it from the car screen, assuming you have bought this option. Congrats to Tesla Autopilot/AI team on achieving a major milestone!”57 Em tradução livre: “O Tesla Full Self-Driving Beta agora está

---

[54] Decisão da Corte Regional de Emmental-Oberaargau apud HILGENDORF, Eric. Digitalização e direito; org. e trad. Orlandino Gleizer – São Paulo, SP: Marcial Pons, 2020.
[55] Disponível em: https://www.theguardian.com/technology/2022/dec/22/tesla-crash-full-self-driving-mode-san-francisco Acesso em 10 de fevereiro de 2023
[56] Disponível em: https://theintercept.com/2023/01/10/tesla-crash-footage-autopilot/ Acesso em 10 de fevereiro de 2023
[57]Disponível em: https://twitter.com/elonmusk/status/1595682322707267584?ref_src=twsrc%5Etfw%7Ctwcamp

disponível para qualquer pessoa na América do Norte que o solicitar na tela do carro, desde que você tenha comprado esta opção. Parabéns à equipe Tesla Autopilot/AI por alcançar um marco importante!”

Ao que foi divulgado, o motorista do carro afirmou que estava usando justamente o sistema Full Self Driving. Esse caso se somou a outros investigados pela National Highway Traffic Safety Administration (NHTSA), que ao total investiga ao menos 41 acidentes envolvendo veículos da Tesla com esses recursos de sistema de assistência ao motorista.[58]

A Tesla vem respondendo a processos judiciais de consumidores (class action complaint), caso 3:22-cv-05240[59], perante o Distrito da Califórnia, sob as seguintes acusações:

> 1. VIOLATION OF THE MAGNUSON MOSS WARRANTY ACT 2. BREACH OF EXPRESS WRITTEN WARRANTY 3. BREACH OF IMPLIED WARRANTY OF MERCHANTABILITY 4. VIOLATION OF THE CALIFORNIA FALSE ADVERTISING LAW 5. VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT 6. VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW 7. FRAUD AND DECEIT 8. NEGLIGENT MISREPRESENTATION 9. UNJUST ENRICHMENT 10. NEGLIGENCE[60]

Há uma grande questão de marketing envolvendo a Tesla, seu CEO e os veículos autônomos, porquanto ao que consta do processo judicial, não poderia a empresa divulgar a tecnologia tal como está sendo vendida, com nome de “self-driving”, porque isso causa uma falsa impressão, especialmente nos operadores, de que o carro dirige sozinho quando na verdade o motorista deve manter sua atenção e mãos no volante a todo tempo.

%5Etweetembed%7Ctwterm%5E1595682322707267584%7Ctwgr%5Ed2c6a0139310859c89fd4180579f01906908c1e2%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Ftheintercept.com%2F2023%2F01%2F10%2Ftesla-crash-footage-autopilot%2F Acesso em 10 de fevereiro de 2023

[58] Disponível em: https://www.cnbc.com/2022/12/22/nhtsa-initiates-two-more-tesla-crash-investigations.html Acesso em 10 de fevereiro de 2023

[59] Peça processual - case 3:22-cv-05240

[60] Peça processual - case 3:22-cv-05240. Tradução livre: 1. VIOLAÇÃO DA LEI MAGNUSON MOSS WARRANRTY. 2. QUEBRA DA GARANTIA EXPRESSA POR ESCRITO 3. QUEBRA DA GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO 4. VIOLAÇÃO DA LEI DE PROPAGANDA FALSA DA CALIFÓRNIA 5. VIOLAÇÃO DA LEI DE RECURSOS LEGAIS DO CONSUMIDOR DA CALIFÓRNIA 6. VIOLAÇÃO DA LEI DE CONCORRÊNCIA DESLEAL DA CALIFÓRNIA 7. FRAUDE E ENGANAÇÃO 8. DECLARAÇÃO FALSA NEGLIGENTE 9. ENRIQUECIMENTO INJUSTO 10. NEGLIGÊNCIA

De acordo com o processo judicial existe uma classificação pela SAE International (Society of Automotive Engineers) de automação dos veículos em seis níveis, que vai de 0 a 5. A Tesla está classificada no número 2[61], enquanto a Mercedes-benz, mais avançada, vende veículos de classificação 3[62]. A direção autônoma somente seria encontrada no nível 5.

> A SAE Internacional, anteriormente conhecida como Society of Automotive Engineers, é uma associação profissional com sede nos Estados Unidos e uma organização de desenvolvimento de normas fundada no início do século XX. Em 2014, a SAE Internacional assumiu um papel de liderança no desenvolvimento de padrões de tecnologia de veículos autônomos ao publicar a versão inicial da Prática Recomendada SAE J3016: Taxonomia e Definições de Termos Relacionados a Sistemas de Automação de Direção para Veículos Motorizados On-Road, comumente referido como o Níveis SAE de Automação de Condução ("Níveis SAE"). Em seguida, a SAE Internacional publicou versões revisadas dos Níveis SAE em 2016, 2018 e 2021.7 26. Os Níveis SAE fornecem uma taxonomia de sistemas de automação de direção de veículos com definições detalhadas para seis níveis de automação de direção, variando de nenhuma automação de direção (Nível SAE 0) para automação de direção completa (SAE nível 5). Os níveis SAE podem ser resumidos da seguinte forma: Nível 0: Sem Automação de Direção. O motorista humano executa todas as tarefas de direção (direção, aceleração, frenagem, etc.), embora os veículos possam ter recursos de segurança como frenagem automática de emergência e aviso de colisão frontal. Nível 1: Assistência ao Condutor. O veículo possui recursos que fornecem um pequeno grau de automação na aceleração, frenagem ou direção do veículo (por exemplo, controle de cruzeiro adaptativo, assistência para manter a faixa). Nível 2: Automação de direção parcial. O veículo pode executar várias tarefas de direção (por exemplo, aceleração, direção), mas permanece sob supervisão, responsabilidade e controle constantes do motorista humano. Nível 3: Automação Condicional de Condução. O veículo pode assumir o controle total de certas tarefas de direção, de modo que o motorista humano não precise permanecer constantemente alerta, mas esteja pronto para intervir a pedido do veículo. Nível 4: Alta Automação de Condução. O veículo pode executar todas as tarefas de direção em locais ou ambientes específicos, mas a intervenção humana ainda é uma opção. Nível 5: Automação de condução completa. O veículo pode executar todas as tarefas de direção em todas as condições, sem necessidade de atenção humana ou interação.[63]

---

[61] Disponível em: <https://www.forbes.com/sites/jamesmorris/2021/03/13/why-is-teslas-full-self-driving-only-level-2-autonomous/> Acesso em 10 de fevereiro de 2023

[62] Disponível em: <https://europe.autonews.com/automakers/mercedes-opens-sales-level-3-self-driving-system-s-class-eqs> Acesso em 10 de fevereiro de 2023

[63] SAE International, formerly the Society of Automotive Engineers, is a U.S.-based professional association and standards development organization founded in the early 20th century. In 2014, SAE International took a leading role in the development of autonomous vehicle technology standards by publishing the initial version of SAE J3016 Recommended Practice: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, commonly referred to as the SAE Levels of Driving Automation ("SAE Levels"). Following this, SAE International published revised versions of the SAE Levels in 2016, 2018, and 2021.7 26. The SAE Levels provide a taxonomy of vehicle driving automation systems with detailed

A classificação pela SAE é amplamente aceita nos padrões interacionais e foi adotada pelas agências americanas de regulação. A NHTSA, em maio de 2022 divulgou gráfico resumindo os níveis:

definitions for six levels for driving automation, ranging from no driving automation (SAE Level 0) to full driving automation (SAE Level 5). The SAE Levels can be summarized as follows: Level 0: No Driving Automation. The human driver performs all driving tasks (steering, acceleration, braking, etc.), although vehicles may have safety features like automatic emergency braking and forward collision warning. Level 1: Driver Assistance. The vehicle has features that provide a small degree of automation over the vehicle's acceleration, braking, or steering (e.g., adaptive cruise control, lane-keeping assistance). Level 2: Partial Driving Automation. The vehicle can perform multiple driving tasks (e.g., acceleration, steering) but remains under the human driver's constant supervision, responsibility, and control. Level 3: Conditional Driving Automation. The vehicle can take full control of certain driving tasks such that the human driver need not remain constantly alert but must be ready to intervene upon request from the vehicle. Level 4: High Driving Automation. The vehicle can perform all driving tasks in specific locations or environments, but human override is still an option. Level 5: Full Driving Automation. The vehicle can perform all driving tasks under all conditions, with zero human attention or interaction required

Por isso o termo “Full Self-Driving” está sendo amplamente criticado por fabricantes e grupos da indústria como enganoso e perigoso, exatamente por passar a falsa impressão de que o veículo dirige sozinho, quando está muito longe de alcançar isso.

A Tesla também está no foco de investigação pelo Departamento de Justiça dos EUA em razão dos veículos autônomos que têm causado graves acidentes em diversos estados daquele país.[64] O Departamento de Justiça dos EUA divulgou que está investigando criminalmente a Tesla após inúmeras falhas relacionadas ao sistema oferecido pela empresa. Especificamente, está examinando se a Tesla engana consumidores, reguladores e investidores no lançamento da tecnologia semiautônoma. Esta investigação do DOJ se soma a uma rede existente de investigações e ações judiciais enfrentadas pela Tesla, incluindo a investigação da National Highway Transportation Safety Administration sobre acidentes fatais envolvendo o Autopilot. Mas o Departamento de Veículos Motorizados da Califórnia também acusou a Tesla de anunciar falsamente suas capacidades de veículos semiautônomos como totalmente autônomos.

2.1.6. Outros casos

Os veículos autônomos foram os que receberam especial atenção nos últimos anos dentre os sistemas que utilizam de inteligência artificial avançada, especialmente na Alemanha, o que pode estar relacionado à relevância social e econômica de veículos naquele país, ou ainda porque sua indústria automobilística tem posição de destaque mundial (HILGENDORF, 2020). Mas não há dúvida que esse debate se expande e alcança outros sistemas autônomos.

---

[64] Disponível em: https://www.reuters.com/legal/exclusive-tesla-faces-us-criminal-probe-over-self-driving-claims-sources-2022-10-26/ Acesso em 10 de fevereiro de 2023

Há poucos anos a plataforma Google, por exemplo, foi alvo de acusações de discriminação decorrente de algoritmos sexistas por sua função autocompletar (autocomplete function).[65] Houve ainda acusações de que o sistema seria racista ao divulgar predominantemente imagens de pessoas brancas em pesquisas como “mulher” em sua barra de pesquisa (Google’s image Search).

Não foi a primeira vez que o Google disponibilizou amplamente ao público ferramenta de tecnologia racista. Em 2015 um caso ficou conhecido porque uma foto de um casal de pessoas negras foi identificado pela plataforma como “gorilas”.[66]

Em outro caso, a Amazon, em 2019, abandonou um projeto de recrutamento de serviço a partir de inteligência artificial por ser sexista (ORTIZ, SAYEG, 2020):

> Recentemente a Amazon abandonou um projeto de uma ferramenta de Inteligência Artificial. Tratava-se de um algoritmo que estava a ser testado e funcionava como ferramenta de recrutamento, mas estava enviesada porque era sexista. O sistema de inteligência artificial foi treinado em dados referentes a recrutamentos de um período de dez anos, muitos dos quais referiam-se a homens. Entretanto, os desenvolvedores da ferramenta perceberam que o sistema havia aprendido que candidatos do sexo masculino eram preferíveis. O sistema avaliava e atribuía aos candidatos uma pontuação que variava de uma a cinco estrelas. O intuito era que o sistema recebesse os currículos e, automaticamente, indicasse os melhores para serem contratados. O preconceito, aprendido com os dados estava claro: o sistema não estava avaliando candidatos de maneira neutra em termos de sexo, porque foi construído com base em dados de currículos, principalmente, de homens. Assim, o algoritmo penalizava currículos que incluíam a palavra “mulher” o que inviabilizava o seu uso de uma forma neutra e confiável (PEDREIRA, 2019).

Para além dessas plataformas online, recentemente, na Guerra entre Rússia e Ucrânia foi identificado um *killer drone* Russo, que seria o drone com capacidade de identificar alvos e detonar explosivos a partir de inteligência

[65] Disponível em: https://theconversation.com/googles-algorithms-discriminate-against-women-and-people-of-colour-112516 Acesso em: 11 de janeiro de 2023
[66] Disponível em: https://www.bbc.com/news/technology-33347866 Acesso em: 11 de janeiro de 2023

artificial, autorizado a matar e ferir pessoas sem necessidade de comando humano.[67]

Diversos são os casos que já ocorreram ofensas a bens jurídicos tutelados[68] mundialmente e muitas são as possibilidades futuras das máquinas afetarem a vida humana.

Hoje o exemplo mais comum são as ofensas aos bens jurídicos vida e integridade física por danos causados a partir dos acidentes automobilísticos envolvendo veículos autônomos ou semiautônomos, mas isso se estende a outras máquinas dotadas de inteligência artificial capazes de autoaprendizagem.

Para além da integridade física, já estão ocorrendo também crimes de racismo e injúria racial praticados a partir de inteligência artificial dotada de autoaprendizagem. Como os já citados, praticados pelo software Tay e algoritmos Google, o que podem vir a se repetir em sistemas como o mencionado ChatGPT.

É possível visualizar também a ocorrência de crimes contra o estado democrático de direito praticado a partir de desinformação massiva e *fake news* com uso de inteligência artificial, como também eventuais ofensas à intimidade e privacidade por vazamento de dados pessoais diante de atuação de inteligência artificial.

Há ainda um vasto campo para ofensa a bens jurídicos de consumidores a partir de inteligência artificial que aprende mediante algoritmos com os gostos e tendências pessoais dos consumidores. Basta alguns algoritmos equivocadamente pré-condicionados ou indevidamente direcionados e uma compra pode ser realizada contra a legítima vontade do consumidor. Não é necessário fantasiar. Atualmente muitas compras de supermercado são feitas

---

[67] Disponível em: https://cacm.acm.org/news/259529-russias-killer-drone-in-ukraine-raises-fears-about-ai-in-warfare/fulltext acesso em 10 de fevereiro de 2023

[68] Para uma apropriada conceituação de bem jurídico: TAVARES, Juarez. Teoria do injusto penal. 4 ed - São Paulo: Tirant lo Blanch, 2019, p. 199 e ss.

por aplicativos de aquisição recorrente e as sugestões de marca, por exemplo, são feitas com base no próprio histórico do consumidor. Suponhamos que por um erro de algoritmo, ou por condicionamento prévio para benefício de uma companhia, o aplicativo sugira sempre a marca X invés da Y, mais barata. Daqui alguns anos, com a implementação da IoT, a geladeira comum será capaz de adquirir o produto que está em falta e poderá escolher a marca X mesmo sem a prévia aprovação do consumidor.

A mesma ideia se aplica às questões da medicina envolvendo robótica. O Hospital Albert Einstein em São Paulo tem a honra de se anunciar como pioneiro na América Latina na técnica robô assistida, que desde 2011 vem atuando na realização de cirurgias não invasivas.[69] Num futuro próximo as máquinas de cirurgia serão automatizadas e necessitarão de pouca ou nenhuma intervenção médica, tudo a partir de inteligência artificial. Um erro de informação ou algoritmo equivocado e será ao custo da saúde e de vidas humanas.

Avançando a discussão, há a possibilidade de pensar crimes cibernéticos no metaverso e a possibilidade - ou não - de cometimento de crimes comuns por meio de avatares em ambiente de realidade aumentada.

Tudo isso pode parecer retirado diretamente de um filme de ficção científica, mas a tecnologia dotada de inteligência artificial fica cada dia mais sofisticada nos principais países do mundo. No Brasil, enquanto país em desenvolvimento, o tema da regulação da inteligência artificial e dos sistemas autônomos ainda está em debate no Congresso Nacional e demanda atenção da sociedade porque inevitavelmente será uma realidade.

---

[69] Disponível em: https://www.einstein.br/especialidades/cirurgia/programa/cirurgia-robotica#:~:text=Da%20Vinci%20Surgical%20System,-A%20aquisi%C3%A7%C3%A3o%20do&text=Os%20profissionais%20de%20cirurgia%20rob%C3%B3tica,de%20forma%20sistem%C3%A1tica%20e%20peri%C3%B3dica. Acesso em 11 de fevereiro de 2023.

3. INTELIGÊNCIA ARTIFICIAL: REGULAÇÃO NO CENÁRIO MUNDIAL

A nível mundial, a evolução da Inteligência Artificial tem sido acompanhada de perto pelas nações desenvolvidas, que vêm travando profundas discussões sobre a necessidade de regulação jurídica para, a um só tempo, garantir a proteção aos direitos humanos, trazer segurança jurídica aos desenvolvedores e usuários e permitir o desenvolvimento das tecnologias, com incentivos dos mais diversos, porquanto tem sido reconhecido que a AI é o futuro para todos: Estado, indivíduos, empresas etc. (MINISTÉRIO DA CIÊNCIA, TECNOLGIA E INOVAÇÃO, 2021)

Já existem exemplos internacionais esparsos de normas jurídicas que regulam diferentes inteligências artificiais, como por exemplo, os veículos autônomos, sobre o quê a Alemanha foi pioneira com a Lei de Regulação da Condução Automatizada, de 16 de junho de 2017 – BGBI. 1648 (HILGENDORF, 2020).

As nações têm debatido a construção de textos que estabeleçam quais são os "princípios gerais e parâmetros éticos a serem adotados por atores públicos e privados quanto ao tema AI, por meio de códigos de conduta, manuais de boas práticas e diretrizes de alto nível".[70]

Em 2018 um grupo de ativistas com parceria de empresas de tecnologia publicou, no Canadá, um manifesto que ficou conhecido como The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems[71] que buscava evitar que o avanço das máquinas dotadas de autoaprendizado (machine learning) afetasse sobremaneira direitos humanos. Em tradução livre:

---

[70] Cartilha da Estratégia Brasileira de Inteligência Artificial, disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial#:~:text=Estrat%C3%A9gia%20Brasileira%20de%20Intelig%C3%AAncia%20Artificial%20%2D%20EBIA Acesso em 11 de fevereiro de 2023

[71] The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems. Disponível em: <https://mail.intgovforum.org/multilingual/sites/default/files/webform/toronto-declaration-final.pdf> Acesso em 11 de fevereiro de 2023

> Esta Declaração foca nos direitos à igualdade e à não discriminação, princípios fundamentais que sustentam todos os direitos humanos. 12. A discriminação é definida pela lei internacional como "qualquer distinção, exclusão, restrição ou preferência baseada em qualquer motivo, como raça, cor, sexo, idioma, religião, opinião política ou de outra natureza, origem nacional ou social, propriedade, nascimento ou outra condição, e que tenha por objeto ou efeito anular ou prejudicar o reconhecimento, gozo ou exercício por todas as pessoas, em pé de igualdade, de todos os direitos e liberdades". Esta lista não é exaustiva, pois o 3º Alto Comissariado das Nações Unidas para os Direitos Humanos reconheceu a necessidade de prevenir a discriminação contra classes adicionais.[72]

A OCDE (Organização para a Cooperação e Desenvolvimento Econômico), organização econômica intergovernamental com 38 países membros, dentre eles o Brasil, emitiu em 2019 uma cartilha consolidada (Recommendation of the Council on Artificial Intelligence) no que tange à inteligência artificial e sua regulamentação perante os respectivos países.[73]

Ao que interessa ao presente trabalho essa Recomendação contém dois pontos essenciais, sobre a centralização e respeito ao ser humano e *accountability.* A saber, em tradução livre:

> 1.2. Valores centrados no ser humano e justiça
> a) Os atores da IA devem respeitar o estado de direito, os direitos humanos e os valores democráticos, durante todo o ciclo de vida do sistema de IA. Estes incluem liberdade, dignidade e autonomia, privacidade e proteção de dados, não discriminação e igualdade, diversidade, equidade, justiça social e direitos trabalhistas reconhecidos internacionalmente.
> b) Para tal, os atores da IA devem implementar mecanismos e salvaguardas, como a capacidade de determinação humana, que sejam adequados ao contexto e consistentes com o estado da arte. [...]
> 1.5 Responsabilidade

---

[72] This Declaration focuses on the rights to equality and non-discrimination, critical principles underpinning all human rights. 12. Discrimination is defined under international law as "any distinction, exclusion, restriction or preference which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms." This list is non-exhaustive as the 3 United Nations High Commissioner for Human Rights has recognized the necessity of preventing discrimination against additional classes

[73] Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 Acesso em 11 de fevereiro de 2023

> Os atores da IA devem ser responsáveis pelo bom funcionamento dos sistemas de IA e pelo respeito aos princípios acima, com base em suas funções, no contexto e de acordo com o estado da arte.[74]

Em reunião do G20, aos 05.08.2021, em Trieste, na Itália, Ministros que compõem o grupo assinaram declaração conjunta sobre 12 ações para acelerar a transformação digital da economia e governos[75]. Em resumo:

> Os 12 princípios destacam temas como a transformação digital para o crescimento sustentável; uso da inteligência artificial para promoção de startups; medição, prática e impactos da economia digital; conscientização e proteção do consumidores; proteção e empoderamento de crianças no ambiente digital; apoio a inovação para cidades inteligentes; conectividade e inclusão social; livre fluxo de dados entre os países; digitalização de serviços públicos; identidade digital; regulamentação ágil; e transformação da Força Tarefa para Transformação Digital do G20 em um Grupo de Trabalho para esse fim.[76]

O Parlamento Europeu e o Conselho da Comissão Europeia consolidaram, também em 2021, proposta de regulamento que estabelece regras em matéria de inteligência artificial (Regulamento inteligência Artificial) e tal se deu para:

> melhorar as previsões, otimizar as operações e a afetação de recursos e personalizar o fornecimento dos serviços, a utilização da inteligência artificial pode contribuir para resultados benéficos para a sociedade e o ambiente", sob a motivação de atender às necessidades dos setores de elevado impacto como "os domínios das alterações climáticas, do ambiente e da saúde, do setor público, das finanças, da mobilidade, dos assuntos internos e da agricultura.

---

[74] 1.2.Human-centred values and fairness
a)AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labour rights.
b)To this end, AI actors should implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context and consistent with the state of art. [...]
1.5 Accountability
AI actors should be accountable for the proper functioning of AI systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of art

[75] Declaração disponível em: https://www.g20.org/wp-content/uploads/2021/08/DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdf Acesso em 11 de fevereiro de 2023

[76] Informações obtidas pelo site do Governo. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2021/08/declaracao-de-ministros-do-g20-identifica-12-acoes-para-acelerar-a-transformacao-digital Acesso em 11 de fevereiro de 2023

O documento justifica sua necessidade porque reconhece que a inteligência artificial (IA) também pode trazer novos riscos ou consequências negativas para os cidadãos e a sociedade:

> À luz da velocidade da evolução tecnológica e dos possíveis desafios, a UE está empenhada em alcançar uma abordagem equilibrada. É do interesse da União preservar a liderança tecnológica da UE e assegurar que novas tecnologias, desenvolvidas e exploradas respeitando os valores, os direitos fundamentais e os princípios da União, estejam ao serviço dos cidadãos europeus. A presente proposta honra o compromisso político assumido pela presidente Ursula von der Leyen, que anunciou nas suas orientações políticas para 2019-2024, intituladas «Uma União mais ambiciosa» 1 , que a Comissão apresentaria uma proposta legislativa relativa a uma abordagem europeia coordenada às implicações humanas e éticas da inteligência artificial. [...] A presente proposta visa dar execução ao segundo objetivo, desenvolvendo um ecossistema de confiança mediante a proposta de um quadro jurídico para uma IA de confiança. A proposta tem como base os valores e os direitos fundamentais da UE e pretende dar às pessoas e a outros utilizadores a confiança necessária para adotarem soluções baseadas em IA, ao mesmo tempo que incentiva as empresas para que as desenvolvam. A inteligência artificial deve ser uma ferramenta ao serviço das pessoas e uma força positiva para a sociedade com o objetivo final de aumentar o bem-estar dos seres humanos. As regras aplicáveis às tecnologias de inteligência artificial disponibilizadas no mercado da União ou que afetam as pessoas da União devem, por isso, centrar-se no ser humano, de modo que as pessoas possam confiar que a tecnologia é utilizada de uma forma segura e em cumprimento da lei, incluindo em matéria de respeito dos direitos fundamentais. [...] As Conclusões, mais recentes, de 21 de outubro de 2020 reforçaram a importância de dar resposta a desafios como a opacidade, a complexidade, os preconceitos [ou enviesamentos], um certo grau de imprevisibilidade e comportamentos parcialmente autónomos de determinados sistemas de IA, a fim de garantir a compatibilidade destes sistemas com os direitos fundamentais e facilitar a aplicação das normas jurídicas.

Trata-se tal regulamento de arquivo extenso que traz diversas definições, regulamentações e consequências, algumas das quais, por serem relevantes ao desenvolvimento desta pesquisa, serão mencionadas. Já nos “considerandos” é possível notar a preocupação com a responsabilização pelos produtos de inteligência artificial (AI):

> É apropriado que uma pessoa singular ou coletiva específica, identificada como «fornecedor», assuma a responsabilidade pela colocação no mercado ou pela colocação em serviço de um sistema de IA de risco elevado, independentemente de ser ou não a pessoa que concebeu ou desenvolveu o sistema. [...]

> Dada a natureza dos sistemas de IA e os riscos para a segurança e os direitos fundamentais possivelmente associados à sua utilização, nomeadamente no que respeita à necessidade de assegurar um controlo adequado do desempenho de um sistema de IA num cenário real, é apropriado determinar responsabilidades específicas para os utilizadores. Em particular, os utilizadores devem utilizar os sistemas de IA de risco elevado de acordo com as instruções de utilização e devem ser equacionadas outras obrigações relativas ao controlo do funcionamento dos sistemas de IA e à manutenção de registos, se for caso disso.

Por exemplo, em seu artigo 14, há a previsão de uma necessária supervisão humana para os sistemas de IA de risco elevado. Em seus termos:

> Artigo 14.º - Supervisão humana
> 1.Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de tal modo, incluindo com ferramentas de interface homem-máquina apropriadas, que possam ser eficazmente supervisionados por pessoas singulares durante o período de utilização do sistema de IA.
> 2.A supervisão humana deve procurar prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de IA de risco elevado é usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, em especial quando esses riscos persistem apesar da aplicação de outros requisitos estabelecidos neste capítulo.
> 3.A supervisão humana deve ser assegurada por meio de um ou de todos os seguintes tipos de medidas:
> a)Medidas identificadas e integradas, quando tecnicamente viável, pelo fornecedor no sistema de IA de risco elevado antes de este ser colocado no mercado ou colocado em serviço;
> b)Medidas identificadas pelo fornecedor antes de o sistema de IA de risco elevado ser colocado no mercado ou colocado em serviço e que sejam adequadas para implantação por parte do utilizador.
> 4.As medidas a que se refere o n.º 3 devem permitir que as pessoas responsáveis pela supervisão humana façam o seguinte, em função das circunstâncias:
> a)Compreendam completamente as capacidades e limitações do sistema de IA de risco elevado e sejam capazes de controlar devidamente o seu funcionamento, de modo que os sinais de anomalias, disfuncionalidades e desempenho inesperado possam ser deletados e resolvidos o mais rapidamente possível;
> b)Estejam conscientes da possível tendência para confiar automaticamente ou confiar excessivamente no resultado produzido pelo sistema de IA de risco elevado («enviesamento da automatização»), em especial relativamente aos sistemas de IA de risco elevado usados para fornecer informações ou recomendações com vista à tomada de decisões por pessoas singulares;
> c)Sejam capazes de interpretar corretamente o resultado do sistema de IA de risco elevado, tendo em conta, nomeadamente, as características do sistema e as ferramentas e os métodos de interpretação disponíveis;
> d)Sejam capazes de decidir, em qualquer situação específica, não usar o sistema de IA de risco elevado ou ignorar, anular ou reverter o resultado do sistema de IA de risco elevado;

> e)Serem capazes de intervir no funcionamento do sistema de IA de risco elevado ou interromper o sistema por meio de um botão de «paragem» ou procedimento similar.
> 5.Em relação aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 1, alínea a), as medidas referidas no n.º 3 devem, além disso, permitir assegurar que nenhuma ação ou decisão seja tomada pelo utilizador com base na identificação resultante do sistema, salvo se a mesma tiver sido verificada e confirmada por, pelo menos, duas pessoas singulares.

Já o artigo 16 prevê as obrigações dos fornecedores de sistemas de inteligência artificial de risco elevado, enquanto o artigo 24 prevê as obrigações dos fabricantes. São eles:

> Artigo 16.º - Obrigações dos fornecedores de sistemas de inteligência artificial de risco elevado
> Os fornecedores de sistemas de IA de risco elevado devem:
> a)Assegurar que os seus sistemas de IA de risco elevado cumprem os requisitos estabelecidos no capítulo 2 do presente título;
> b)Dispor de um sistema de gestão da qualidade que cumpra o disposto no artigo 17.º;
> c)Elaborar a documentação técnica do sistema de IA de risco elevado;
> d)Quando tal esteja sob o seu controlo, manter os registos gerados automaticamente pelos sistemas de IA de risco elevado que fornecem;
> e)Assegurar que o sistema de IA de risco elevado seja sujeito ao procedimento de avaliação da conformidade aplicável, antes da colocação no mercado ou da colocação em serviço;
> f)Respeitar as obrigações de registo a que se refere o artigo 51.º;
> g)Adotar as medidas corretivas necessárias, se o sistema de IA de risco elevado não estiver em conformidade com os requisitos estabelecidos no capítulo 2 do presente título;
> h)Informar as autoridades nacionais competentes dos Estados-Membros nos quais disponibilizaram o sistema de IA ou o colocaram em serviço e, se for caso disso, o organismo notificado sobre a não conformidade e quaisquer medidas corretivas tomadas;
> i)Apor a marcação CE nos sistemas de IA de risco elevado para indicar a conformidade com o presente regulamento de acordo com o artigo 49.º;
> j)Mediante pedido de uma autoridade nacional competente, demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título.

> Artigo 24.º - Obrigações dos fabricantes de produtos
> Se um sistema de IA de risco elevado relacionado com produtos aos quais são aplicáveis os atos jurídicos enumerados no anexo II, secção A, for colocado no mercado ou colocado em serviço juntamente com o produto fabricado em conformidade com esses atos jurídicos e sob o nome do fabricante do produto, este último fica incumbido de garantir a conformidade do sistema de IA com o presente regulamento e, no que diz respeito ao sistema de IA, tem as mesmas obrigações impostas ao fornecedor pelo presente regulamento.

Estão ainda previstas nos artigos subsequentes as obrigações dos distribuidores, importadores, utilizadores e outros terceiros. A União Europeia criou uma normativa recheada, abarcando, dentre outras disposições, as obrigações e responsabilidades de todos os participantes da cadeia de desenvolvimento da IA.

Em março de 2022[77], a China também aprovou regulamento[78] de inteligência artificial que tem como objetivo regular serviços de informação no âmbito da internet e atividade de algoritmos de recomendação, em seus termos, a fim de perpetuar os valores socialistas e, também, preservar a segurança nacional e o interesse público da sociedade, como ainda, proteger os direitos e interesses legais das pessoas físicas e jurídicas e outras organizações, bem como, preservar o desenvolvimento dos serviços de internet. Em suma, ao que interessa, o Capítulo 5 prevê as responsabilidades legais administrativas e estabelece o que seria infração à segurança pública. Pontua que onde um crime for praticado, a responsabilidade criminal deve ser perseguida de acordo com a lei daquele país.

Por fim, dentre os quais são relevantes ao presente estudo, o Reino Unido, também reconhecendo a relevância da AI e, de outro lado, seus riscos, em dezembro de 2022, elaborou um plano para tornar a Grã-Bretanha uma superpotência mundial de inteligência artificial[79], o qual foi desenvolvido a partir de 3 pilares. São eles: (i) investir nas necessidades de longo prazo do ecossistema de IA; (ii) garantir que a IA beneficie todos os setores e regiões e (iii) governar a IA de forma eficaz. Eis seus termos, em tradução livre:

> Há uma conscientização crescente na indústria e pelos cidadãos dos riscos e danos potenciais associados às tecnologias de IA. Isso inclui preocupações

[77] Informação disponível em: https://www.scmp.com/tech/policy/article/3168816/chinas-algorithm-law-takes-effect-curb-big-techs-sway-public-opinion Acesso em 12 de fevereiro de 2023

[78] Regulamento disponível em: http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm Acesso em 12 de fevereiro de 2023

[79] Disponível em: https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version#our-ten-year-plan-to-make-britain-a-global-ai-superpower Acesso em 12 de fevereiro de 2023

> sobre justiça, viés e responsabilidade dos sistemas de IA. Por exemplo, o relatório da Comissão sobre Disparidades Raciais e Étnicas levantou preocupações sobre o potencial de novas formas de viés a serem introduzidas por meio da IA. Outras preocupações incluem a capacidade da IA de minar a privacidade e a agência humana; e danos físicos, econômicos e financeiros sendo permitidos ou exacerbados por tecnologias de IA. Por exemplo, a segurança cibernética deve ser considerada no início do desenvolvimento e implantação de sistemas de IA para evitar que tais danos surjam, adotando uma abordagem "segura por design" para mitigar a segurança cibernética que se torna uma reflexão tardia.".[80]

3.1. CENÁRIO NACIONAL

Especialmente diante desse cenário mundial, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) da União emitiu a Portaria 1.122/2020 que define as prioridades, no âmbito do Ministério, no que se refere a projetos de pesquisa, desenvolvimento de tecnologias e inovações para o período entre os anos de 2020 e 2023. A portaria estabelece como prioritários os projetos de pesquisa, desenvolvimento e inovações voltados para, dentre outras, a área de "tecnologias habilitadoras", definindo que ela contempla os setores de inteligência artificial e internet das coisas.

Também foi criada a Estratégia Brasileira de Inteligência Artificial – EBIA[81], a partir da Portaria MCTI nº 4.617/21[82] alterada pela Portaria MCTI nº 4.979/21[83], que é uma espécie de cartilha que tem o "papel de nortear as ações do Estado brasileiro em prol do desenvolvimento das ações, em suas várias

---

[80] Idem. Tradução livre: There is growing awareness in industry and by citizens of the potential risks and harms associated with AI technologies. These include concerns around fairness, bias and accountability of AI systems. For example, the report from the Commission on Race and Ethnic Disparities raised concerns around the potential for novel ways for bias to be introduced through AI. Other concerns include the ability of AI to undermine privacy and human agency; and physical, economic and financial harms being enabled or exacerbated by AI technologies. For example, cyber security should be considered early in the development and deployment of AI systems to prevent such harms from arising, by adopting a 'secure by design' approach to mitigate against cyber security becoming an afterthought

[81] Cartilha da Estratégia Brasileira de Inteligência Artificial, disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial#:~:text=Estrat%C3%A9gia%20Brasileira%20de%20Intelig%C3%AAncia%20Artificial%20%2D%20EBIA Acesso em 11 de fevereiro de 2023.

[82] Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gm-n-4.617-de-6-de-abril-de-2021-*-313212172 Acesso em 12 de fevereiro de 2023

[83] Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-4.979-de-13-de-julho-de-2021-332164912 Acesso em 12 de fevereiro de 2023

vertentes, que estimulem a pesquisa, inovação e desenvolvimento de soluções em Inteligência Artificial...”[84]. Porque, segundo suas disposições:

> É preciso entender a conexão da Inteligência Artificial com várias tecnologias e deixar claro os limites e pontos de conexão e de conceitos como: machine learning, big data, analytics, sistemas especialistas, automação, reconhecimento de voz e imagens, etc

A EBIA foi alinhada às mencionadas diretrizes da OCDE apoiadas pelo Brasil, e tem como princípios aqueles definidos pela Organização para uma gestão responsável dos sistemas de inteligência artificial. (MINISTÉRIO DA CIÊNCIA, TECNOLGIA E INOVAÇÃO, 2021)

> [...] quais sejam: (i) crescimento inclusivo, o desenvolvimento sustentável e o bem-estar; (ii) valores centrados no ser humano e na equidade; (iii) transparência e explicabilidade; (iv) robustez, segurança e proteção e; (v) a responsabilização ou a prestação de contas (accountability).
> A EBIA tem como objetivos:
>
> • Contribuir para a elaboração de princípios éticos para o desenvolvimento e uso de IA responsáveis.
> • Promover investimentos sustentados em pesquisa e desenvolvimento em IA.
> • Remover barreiras à inovação em IA.
> • Capacitar e formar profissionais para o ecossistema da IA.
> • Estimular a inovação e o desenvolvimento da IA brasileira em ambiente internacional.
> • Promover ambiente de cooperação entre os entes públicos e privados, a indústria e os centros de pesquisas para o desenvolvimento da Inteligência Artificial. Para tanto, a Estratégia estabelece nove eixos temáticos, caracterizados como os pilares do documento; apresenta um diagnóstico da situação atual da IA no mundo e no Brasil; destaca os desafios a serem enfrentados; oferece uma visão de futuro; e apresenta um conjunto de ações estratégicas que nos aproximam dessa visão.

Ao mesmo tempo tramita no Congresso Nacional projetos de lei para regulamentar a inteligência artificial, sendo o principal o PL 21/2020, que propõe modelo diverso daquele da Proposta de Regulamentação de Inteligência Artificial

---

[84] Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial Acesso em 12 de fevereiro de 2023

pela Comissão Europeia (regulamentação de 2021), que é a mais completa e debatida até o momento (pela União Europeia).[85]

Em razão disso foi instalada em março de 2022 uma Comissão de Juristas, presidida pelo Ministro Ricardo Villas Bôas Cueva do Superior Tribunal de Justiça, para debater os temas propostos e subsidiar a elaboração da minuta do substitutivo a partir dos projetos de lei (PLs).

O Relatório Final da Comissão apresentou sugestão de texto com pouco mais de 40 artigos, o qual foi entregue em 06 de dezembro de 2022[86]:

> Instalada em março de 2022, a comissão de 18 juristas promoveu reuniões, seminários e audiências públicas divididas por eixos temáticos, com a participação de especialistas e representantes nacionais e internacionais para aprofundar o tema. Foram promovidos 12 painéis temáticos pela comissão, que recebeu 102 manifestações de entidades da sociedade civil organizada, consolidadas no relatório pelos juristas. Também foram criados cinco subgrupos temáticos e promovido um seminário internacional, que discutiu as experiências de inteligência artificial em vigor no mundo. Durante a apresentação do relatório, os membros da comissão foram unânimes em homenagear em suas exposições o jurista Danilo Cesar Maganhoto Doneda, que integrou o colegiado e faleceu em 4 de dezembro, por motivo de saúde.— Contamos com a participação dele ao longo de todo o processo, sempre muito ativo e atuante. A memória dele vai continuar viva em todos nós e certamente se materializou nesse projeto aqui — afirmou o presidente da comissão, Ricardo Villas Bôas Cueva. Cueva destacou ainda que o substitutivo entregue ao Senado constitui "um embrião da regulação" da inteligência artificial no Brasil. Ele também destacou o trabalho desenvolvido pelos juristas. — Foi amplo e profundo ao mesmo tempo, implicou ouvir todos os segmentos da economia e da sociedade civil, especialistas do mundo todo. Todo esse conhecimento foi compendiado ao longo dos meses. Temos hoje um mapa muito completo do que se pensa no mundo sobre o tema no mundo e no Brasil. O trabalho é um espelho do que se espera da regulação da inteligência artificial, todos esperamos não termos errado, nem para mais nem para menos. As escolhas políticas e técnicas que foram feitas estão todos explicitadas no relatório — afirmou. Relatora da comissão e professora da Universidade de Brasília (UnB) e do Instituto Brasiliense de Direito Público (IDP), Laura Schertel Ferreira Mendes disse que a unanimidade dos juristas em torno do substitutivo foi obtida a partir de um trabalho árduo e a liderança de Ricardo Villas Bôas Cueva, também destacada pela advogada e professora da Universidade Federal do Rio Grande do Sul, Cláudia Lima Marques. Advogado e professor de proteção de dados, Fabrício de Mota Alves disse que o substitutivo produzido pela comissão conta com legitimação superior àquela que veio da Câmara, na medida em que o

[85] Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-regulacao-da-inteligencia-artificial-no-brasil-21052022 Acesso em 11 de fevereiro de 2023

[86] Relatório final disponível em: https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relato%CC%81rio%20final%20CJSUBIA.pdf Acesso em 11 de fevereiro de 2023

> colegiado ouviu uma pluralidade de acadêmicos e representantes de diversos setores da sociedade civil. Especialista em proteção de dados, o professor Bruno Ricardo Bioni disse que o substitutivo "é meritório não só no seu conteúdo, mas na forma como o texto foi articulado, uma verdadeira biblioteca sobre temas de inteligência artificial, que reúne visões locais e globais". Advogado e professor da UnB, Thiago Luís Sombra destacou que o substitutivo "é um ponto de partida muito relevante, mas que fatalmente contemplou algumas escolhas, foi fruto de muita composição e, ao final, é um texto completo que reflete diversidade". — O texto precisará passar por novas discussões e alterações, mas entregamos um trabalho amadurecido e refletido — afirmou. Ao término da reunião, o advogado e professor Filipe Medon destacou a iniciativa do Senado em ouvir a sociedade sobre a regulamentação da atividade de inteligência artificial.— O Brasil poderá ser tornar um grande marco. Cabe ao Parlamento o aprofundamento das questões suscitadas ao longo do trabalho da comissão — concluiu. (AGÊNCIA SENADO)[87]

Em suma, o Relatório detém mais de 900 páginas e apresenta um apanhado do que foi realizado e as constatações alcançadas. Entendeu-se não ser possível definir inteligência artificial como conceito pacífico, mas depois de muito debate foi possível estabelecer – para fins do relatório – "*tipos diferentes de IA: fraca e forte, supervisionada e independente, que substituem comportamentos humanos e que apenas emitem recomendações",* mas o objetivo foi alcançado: apresentou-se minuta de substitutivo aos projetos de leis existentes com a finalidade de estabelecer quais são os princípios, regramentos e fundamentos *"para regular o desenvolvimento e aplicação da inteligência artificial no Brasil".* Essa proposta teve uma dupla perspectiva, de proteger a pessoa natural impactada por esses sistemas de inteligência artificial e, também, garantir segurança para o incentivo e desenvolvimento tecnológico.

No que interessa ao presente trabalho, ou seja, no que se refere à responsabilização a partir das condutas praticadas por inteligência artificial, houve sugestões da Comissão, no referida Relatório, no que tange aos danos causados por máquinas autônomas, tanto no âmbito cível, quanto penal. No aspecto cível, eis em suma a discussão travada:

> Preliminarmente, deve-se destacar que alguns expositores apontaram não ser adequado tratar questões de responsabilidade civil no projeto,

[87] Disponível em: https://www12.senado.leg.br/noticias/materias/2022/12/06/comissao-conclui-texto-sobre-regulacao-da-inteligencia-artificial-no-brasil Acesso em 12 de fevereiro de 2023

particularmente durante o Painel 10, que abordava exatamente os “Regimes de responsabilidade civil”. De modo geral, apontou-se a complexidade da questão, incompatível com o caráter geral do projeto, e o fato de as regras relativas à responsabilidade civil já se encontrarem previstas em diversos instrumentos legais. Superada essa preliminar, a forma como a responsabilidade civil foi tratada no PL nº 21, de 2020, foi amplamente criticada. De acordo com ANDERSON SCHREIBER, a opção pela responsabilidade civil subjetiva “não faz sentido”, pois a doutrina, a jurisprudência, o Código Civil e a legislação consumerista adotam o regime de responsabilidade objetiva. Além disso, apontou que estabelecer, em lei ordinária, uma simples “preferência por um certo regime de responsabilidade civil” seria desnecessário, por exigir uma outra norma para especificar a questão. Destacou ainda que “eleger um regime único para todos os usos de IA é um equívoco”, tendo em vista a variedade de situações possíveis. Por fim, ressaltou que “as normas gerais de responsabilidade civil já encontradas no nosso sistema jurídico dão conta, a princípio, de novos usos que começam a ser introduzidos” com a IA, ainda que a questão possa ser um pouco mais detalhada em norma específica. CAITLIN MULHOLLAND afirmou que ela tem “uma visão muito semelhante no que diz respeito à responsabilidade civil e IA”. Ressaltou que, para se reconhecer o regime de responsabilização a ser aplicado, é necessário identificar que tipo de IA está envolvida e que tipos de danos foram provocados83 e que, em geral, a responsabilidade seria objetiva, enfatizando a dificuldade de se comprovar a conduta culposa do desenvolvedor da IA. Corroborou ainda a crítica ao uso do termo “preferencial”, reiterando a necessidade de se estabelecerem regras mais claras para prever o regime aplicável e adicionou que o posicionamento mais adequado seria utilizar as regras de responsabilidade civil já identificadas no ordenamento jurídico. GISELA SAMPAIO DA CRUZ GUEDES Para ANDRÉ LUCAS FERNANDES, o PL nº 21, de 2020, “traz uma anacrônica responsabilidade subjetiva de analítica dogmática frágil”. NELSON ROSELVALD destacou que o projeto, “quando traz a responsabilidade subjetiva para os agentes que atuam nessa cadeia, infelizmente trouxe uma grande simplificação que contradiz a própria complexidade do que se quer regular (…)” e destacou a existência de diversos outros regimes possíveis. RAQUEL LIMA SARAIVA afirmou que o projeto propõe “um modelo de responsabilidade civil que se mostra (…) no mínimo temerário”. DORA KAUFFMAN ressaltou que a “discussão sobre responsabilidades objetiva e subjetiva tem que levar em conta a lógica da IA”. SERGIO PAULO GALLINDO propôs a adoção da responsabilidade subjetiva imprópria, nos termos observados na Lei Geral de Proteção de Dados Pessoais (LGPD). CRISLEINE YEMAJI corroborou a adoção do citado modelo. IVAR HARTMANN indicou que “a responsabilidade objetiva sozinha, nesse cenário, é o pior caminho”, propondo que “o legislador faça de obrigações de meio, e não de obrigações de resultado”. Dessa maneira, as empresas estariam isentas da responsabilidade objetiva se comprovassem adotar boas práticas. DORA KAUFFMAN sugeriu que fossem qualificadas e separadas “as responsabilidades do provedor entre desenvolvedores e fornecedores e entre usuário intermediário e usuário final”, posição elogiada por PAULO RENÁ. EDSON PRESTES ponderou que “não somente os desenvolvedores ou a companhia que desenvolveu o sistema são responsáveis, porque existe toda uma cadeia de produção”. Na mesma linha, GUSTAVO CAMARGO defendeu a “ideia de divisão das responsabilidades pelos atores na cadeia de valor da IA”, considerando que “a proporção de responsabilidade de um player é muito diferente da de outro”. EDSON PRESTES enfatizou que “a atribuição de responsabilidade tem que ser dada ao ser humano, ou seja, a atribuição final de responsabilidade sobre falhas tem que ser dada ao ser humano, nunca a uma máquina”. DORA KAUFFMAN destacou que a regulamentação poderia exigir que as decisões da IA fossem sempre avaliadas por seres humanos, evitando “a substituição da decisão pura e simples”. A seu turno, PAULO RENÁ defendeu que “não faz nenhum sentido

> impor a responsabilidade à máquina, à artificialidade", e que "é uma questão importante que haja a definição da responsabilidade das empresas, a responsabilidade das pessoas jurídicas, das instituições e não efetivamente dos indivíduos". [...] IG BITTENCOURT defendeu que a cadeia de responsabilização seja avaliada depois dos eventos envolvendo a máquina.96 Por outro lado, IVAR HARTMANN argumentou que "uma aposta num sistema unicamente de responsabilização posterior, no caso do Brasil (…) não (…) parece ser uma boa opção", e que "essa lei precisa também lidar com regulação ex ante", complementando que, "em alguns setores (…), nós talvez precisemos de obrigações de licenciamento prévio." GUSTAVO CAMARGO defendeu também que as regras de responsabilidade civil adotassem uma perspectiva baseada em riscos, citando exemplo do Parlamento Europeu. Para SAMANTA OLIVEIRA, "quando a quando a IA for de baixo risco (…), a responsabilidade dos seus desenvolvedores deve se encerrar na medida em que demonstrar de forma clara a compreensão e observando os seus segredos comerciais". Acerca da proposta de vincular o regime de responsabilidade ao risco, CAITLIN MULHOLLAND afirmou que seria precipitada98 e GISELA SAMPAIO DA CRUZ GUEDES classificou a ideia de "inteligente e interessante", mas ponderou que "infelizmente, estamos num estágio muito menos avançado do que os europeus" e que "a gente não tem muita maturidade ainda para tratar disso, de estabelecer essa graduação de risco, essas tipologias". Para NELSON ROSENVALD, "a melhor forma de regular a responsabilidade civil na IA é trabalhando com (…) camadas adicionais de responsabilidade, que são a accountability e a answerability". Destaca ainda que, ao avaliar a responsabilidade, "o magistrado tem que apartar quem é o agente cauteloso daquele que nada faz. Tem que haver um incentivo a comportamentos estratégicos em termos de segurança. E aí que surge a função promocional da responsabilidade civil (…)." SERGIO PAULO GALLINDO relembrou que "a LGPD também valorizou boas práticas, governança e códigos de conduta", pontuando que "isso também deveria ser objeto do corpo da lei". Para MARCELA MATTIUZZO, é necessário incluir no projeto "um mecanismo de *enforcement* efetivo"; posição compartilhada por RAQUEL LIMA SARAIVA, para quem o "PL nº 21, de 2020, da forma como está redigido, não traz qualquer consequência ou sanção". Na mesma linha, PALOMA MENDES apontou a necessidade de um poder sancionador além do Poder Judiciário. De modo divergente, RONY VAINZOF defendeu "seguir as sanções já previstas setorialmente, além, obviamente, do Poder Judiciário em relação à responsabilidade civil". CAITLIN MULHOLLAND sugeriu, como alternativas à responsabilidade civil, mecanismos de "seguro obrigatório, fundo de compensação e um eventual patrimônio de afetação". Apontou que o "seguro obrigatório é uma solução já aventada na proposta de regulação europeia" que ela considera bastante adequada. GISELA SAMPAIO DA CRUZ GUEDES afirmou que todos reconhecem que o caminho é o seguro obrigatório, mas destacou alguns aspectos práticos que precisariam ser solucionados. Na mesma direção, ANDERSON SCHREIBER ressaltou que tem defendido há anos os seguros e fundos de responsabilidade civil, mas pontuou a necessidade de amadurecimento com relação aos detalhes operacionais, que poderiam não ser tratados no projeto. NELSON ROSENVALD corroborou as ideias de sistemas de seguro e de fundos coletivos.

Sob o aspecto penal, a Prof. Dra. Heloisa Estellita participou da Comissão e levantou apontamentos sobre perspectivas criminais, já que os próprios sistemas de inteligência artificial não podem ser responsabilizados penalmente, fazendo com que a responsabilização seja direcionada a uma das

pessoas envolvidas na sua cadeia de confecção, como o fabricante, programador e até usuário, também porque no Brasil apenas há a responsabilização da pessoa jurídica para os crimes ambientais.[88] Pelas dificuldades para verificar dolo em casos desse tipo - e havendo poucas figuras culposas - propõe a referida Professora que ainda não haja a introdução desses sistemas IA no mercado, a saber:

> Para HELOISA ESTELLITA, ainda não é possível responsabilizar penalmente sistemas de IA (como carros autônomos), sendo necessário buscar as pessoas envolvidas: fabricante, programador, proprietário, usuário, etc. Diante das dificuldades para se caracterizar o dolo em casos envolvendo IA, e considerando haver poucas figuras culposas, sugere que "a medida mais correta seria a não introdução desses mecanismos ou dessas máquinas com IA no mercado
>
> Eu não tenho uma [maneira de] responsabilizar o carro ainda por um homicídio no trânsito. Então, eu vou começar a procurar as pessoas que estão por detrás. Eu posso chegar até o fabricante. Eu tenho fabricante, tenho programadora, eu tenho a vendedora e eu tenho o proprietário do veículo ou aquele que vai utilizar. Todas essas pessoas, desde que tenham colocado uma causa para esse acidente fatal, podem, eventualmente, ser responsabilizadas penalmente." 95 "No âmbito de uma responsabilidade por ação dolosa (…), o Direito Penal atual não tem muito problema para responder. Todas as contribuições são puníveis, todos que conheciam que aquilo ia causar dano e puseram isso em ação são puníveis também; eles sabiam que iam causar danos ou contavam com a possibilidade ou com a alta probabilidade de causação de danos (…). Só que essa não é a regra, porque, normalmente, justamente a inserção de uma instância de decisão autônoma ou semiautônoma corta justamente esse controle, pelo menos no nível do conhecimento, de causação de um dano (…). Então, esse é o grande problema da introdução da IA para que o Direito Penal consiga dar uma resposta. E isso é grave, porque a gente pode gerar lacunas de punibilidade em âmbitos de bens jurídicos de altíssima relevância (…). (…) além de eu ter uma dificuldade de praticamente eliminar o dolo quando ponho IA, eu tenho poucas figuras culposas e, ainda assim, vou ter dificuldade, eventualmente, de comprovar a culpa, se de fato o algoritmo tornar a conduta imprevisível ou incontrolável. Nesses casos, a medida mais correta seria a não introdução desses mecanismos ou dessas máquinas com IA no mercado.(NOTAS DE RODA PÉ)

Após a apresentação do Relatório, até o presente momento, em agosto de 2023, os projetos de lei permanecem aguardando trânsito no Senado Federal.

[88] Art. 125, §3º da Constituição da República.

4. ASPECTOS DO DIREITO PENAL: FOCO A PARTIR DA TEORIA DO BEM JURÍDICO

Em razão da crescente relação humanos-máquinas o direito penal também tem sido – mundialmente – acionado para responsabilização a partir das violações a bens jurídicos que vêm sendo afetados.

Para o que interessa ao presente trabalho, o foco é responder a pergunta se é ou não possível responsabilizar alguém, no Brasil, quando uma máquina dotada de sistema autônomo violar bem jurídico já protegido pelo sistema vigente, mas sem abordar, nessa oportunidade, a criação de novos tipos penais e/ou expansão da concepção de bens jurídicos, tão somente utilizando-se o tipos penais previstos na legislação brasileira, a título de exemplo: homicídio, lesão corporal, injúria, racismo etc.

Dessa maneira, no que se refere ao direito penal afetado pela inteligência artificial não se pretende analisar a efetividade do sistema penal enquanto poder/dever de intervenção do Estado, sob a ótica de polícia criminal, mas tão somente verificar se a teoria do delito - apoiada na teoria do bem jurídico - é capaz de responder adequadamente às demandas que já estão postas dentro do sistema penal instituído.

> Desde que o Estado assumiu a constituição de Estado Democrático de Direito, cabe ao direito penal, como espécie de saber, orientar suas discussões para delimitar o poder de punir, condicionando-o, rigidamente, às regras da estrutura do injusto (tipo e antijuridicidade) e da culpabilidade. Dada a importância desses elementos, convém tratá-los, separadamente, de modo mais aprofundado. Cada um deles, assim, comporta uma definição e elementos próprios. A argumentação em torno desses elementos, suas características, extensão e significado constituem o cerne da teoria do delito. (TAVARES, 2018a)

Também não se pretende, nesse trabalho, analisar historicamente a teoria do bem jurídico[89], mas diante do movimento histórico de expansão do

[89] Para saber mais, ver: TAVARES, Juarez. Teoria do injusto penal – 4ª ed. – São Paulo: Tirant lo branch, 2019, p.199 a 237 e LOBO DA COSTA, Regina Helena. Considerações sobre o estado atual da teoria do bem jurídico à luz do harm principle. In: Direito penal como crítica da pena.

direito penal (SANCHEZ, 2013), que se caracteriza por aumentos de penas, maior rigidez na execução, criação de novos âmbitos de criminalização e, ainda, diminuição ou supressão de garantias individuais, o conceito de bem jurídico vem sofrendo intensos impactos, especialmente quanto à capacidade de limitar o âmbito de aplicação do direito penal.

> O direito penal é um instrumento qualificado de proteção de bens jurídicos especialmente importantes. Fixado este ponto, parece obrigatório levar em conta a possibilidade de que sua expansão obedeça, ao menos em parte, já à aparição de novos bens jurídicos – de novos interesses ou de novas valorações de interesses preexistentes – já ao aumento de valor experimentado por alguns dos que existiam anteriormente, que poderia legitimar sua proteção por meio do Direito Penal. As causas da provável existência de novos bens jurídico-penais são, seguramente, distintas. Por um lado, cabe considerar a conformação ou generalização de novas realidades que antes não existiam – ou com a mesma incidência -, e em cujo contexto há de viver o indivíduo, que se vê influenciado por uma alteração daquelas. (SANCHEZ, 2013)

O tema ora abordado pode se caracterizar sobremaneira como exemplo da expansão do direito penal e, assim, demonstrar a dificuldade à teoria do bem jurídico: “a criminalidade, associada aos meios informáticos e à internet (chamada ciberdeliquência) é, seguramente, o maior exemplo de tal evolução.” (SANCHEZ, 2013)

O debate acerca da teoria do bem jurídico é extenso. ROXIN adota “o conceito de bem jurídico como limitação importante e fundamental ao Estado e ao legislador” (LOBO DA COSTA, 2012).

> ...para mim o objeto de proteção do Direito Penal é o bem jurídico, e não a validade da norma. Assim, conceituo bens jurídicos como dados imprescindíveis para a livre e pacífica convivência dos seres humanos sob a garantia de todos OS direitos assegurados pela Constituição. São bens jurídicos, por exemplo, a vida humana, a integridade física, a autodeterminação sexual, a propriedade e patrimônio, e também os chamados bens jurídicos da coletividade, como a moeda e a administração da justiça. Afinal, sem uma moeda intacta e uma administração da justiça que funcione não e possível uma livre e pacífica convivência na sociedade moderna. Teoria do Direito Penal é a proteção de bens jurídicos apenas quando essa proteção não possa ser alcançada por meio de outras medidas sociopolíticas menos gravosas (como o Direito Civil, o Direito Público ou o

---

Estudos em homenagem a Juarez Tavares por seu 70º Aniversário em 2 de setembro de 2012. Ed. Marcial Pons: Madrid, 2012, p. 134 a 140.

> Direito de contraordenações), pois o princípio da proporcionalidade exige que o Estado se de por satisfeito com a intervenção menos intensa possível. Em breves palavras, isso significa: tarefa do Direito Penal é a proteção subsidiária de bens jurídicos. Injusto é todo comportamento a que deve ser cominada uma pena por razões ligadas à proteção de bens jurídicos. De início, um conceito de injusto desses moldes diferencia-se da versão que compreende o injusto como violação da validade da norma em dois pontos centrais. Ao contrário da lesão à validade da norma, que representa uma atribuição abstrata e possui uma existência puramente ideal, a violação do bem jurídico é algo real. Não é necessário que sempre se esteja diante de uma realidade física como no homicídio. Basta uma realidade social, como ocorre nos crimes contra a honra, ou ainda uma violação psíquica, como ocorre no constrangimento ilegal (Nötigung, § 240 StGB). Além disso, esse conceito de injusto não se compatibiliza com normas de conteúdo qualquer, senão que toma como fundamento valorativo nossa Constituição: a discriminação de minorias étnicas ou o tolhimento do direito de exercício de crença são violações de bens jurídicos, corretamente cominadas com pena (§$ 130, 166 SIGB). E está correto, pois tais comportamentos não são compatíveis com uma livre e pacífica convivência humana sob o domínio da Lei Fundamental. De fato, o ponto de partida da concepção aqui desenvolvida de injusto é normativo, na medida em que é reconduzido ao fim do Direito Penal como proteção subsidiária de bens jurídicos. Ocorre, no entanto, que esse padrão normativo se materializa na plenitude das manifestações da vida, e, por levar em conta essa realidade, é saturado de dados empíricos. (ROXIN, 2014b)

HASSEMER (ROXIN, 2014a) defende uma concepção crítica do sistema, a qual entende que a limitação proposta por ROXIN deve ser somada ao atendimento de outros princípios (subsidiariedade, danosidade social, tolerância, entre outros) e, ainda, que os bens jurídicos precisam ser tangíveis, como também, que os direitos coletivos e difusos devem ter como objeto e direcionamento o ser humano (LOBO DA COSTA, 2012).

JUAREZ TAVARES, no caminho de HASSEMER, adota um conceito de bem jurídico pautado na pessoa humana, também com o objetivo final de limitar a atividade do Estado.

> Se o objetivo do direito penal, porém, não é o de simplesmente proteger bens jurídicos, mas o de traçar, nitidamente, os contornos das zonas do lícito e do ilícito, do proibido e do permitido, no sentido de só justificar a intervenção do Estado sobre a liberdade da pessoa humana, em casos de extrema e demonstrada necessidade, a primeira condição de seu implemento é a de descartar, desde logo, a essa classificação, entre bens individuais e coletivos e trabalhar com a noção de bem jurídico, como bem jurídico pessoal. (TAVARES, 2019)

O problema atual é que muitas vezes a teoria do bem jurídico é utilizada "equivocadamente como razão para a criminalização, em vez de limitação ao

espaço de criminalização" (LOBO DA COSTA, 2012), motivo por que nessa oportunidade o conceito é utilizado como "objeto de referência necessário à incriminação" (TAVARES, 2019), ou seja, afasta-se a ideia de que bem jurídico é o que justifica as incriminações porquanto isso apenas fortaleceria o poder punitivo em vez de limitar seu alcance.

Diante dessa concepção, passa-se a análise das possíveis dificuldades à teoria do delito, no que tange à tipicidade, para responsabilização a partir de condutas violadoras de bem jurídicos praticadas por sistemas autônomos, pois, um bem jurídico, ainda que protegido por uma norma incriminadora, só poderá ser "considerado violado se esta violação se der na zona do ilícito" (TAVARES, 2019).

> Como a norma penal é fundamentalmente uma norma de conduta, porque se destina a demarcar as zonas do lícito e do ilícito em relação aos sujeitos e a delimitar o poder de intervenção do Estado, a ação ou omissão típica violadora de bem jurídico ou que produza uma lesão de direito subjetivo é sempre representada por um verbo dotado de certo sentido. A representação da ação através de um verbo demonstra, por seu turno, o sentido dinâmico da conduta típica, que passa a ser operada por um sujeito determinado. A vinculação do sujeito à execução da ação põe de manifesto que o tipo deve estar amparado também por critérios de imputação, de modo que seja atribuído a alguém com base na causalidade de sua produção e ainda pelos princípios de orientação na ordem jurídica, com vistas aos propósitos garantistas. Os critérios de imputação é que irão determinar, por seu turno, a divisão entre delitos dolosos e culposos e bem assim fundamentar os delitos omissivos, tanto próprios como impróprios. (TAVARES, 2018b)

5. DIFICULDADES PARA RESPONSABILIZAÇÃO PENAL: UM PANORAMA GERAL

Visualizando os casos concretos que vêm ocorrendo mundo afora e, considerando os bens jurídicos já tutelados pelo direito penal brasileiro, é necessário abordar as dificuldades para a responsabilização penal de condutas que, ao menos a primeira impressão, parecem terem sido praticadas por máquinas e/ou robôs.

O primeiro ponto que demanda enfrentamento é que o direito penal clássico é construído a partir do conceito de conduta praticada por um sujeito humano.

> O direito penal clássico baseia-se na ideia de uma clara atribuição de responsabilidade: o autor do delito, pensado como pessoa individual (e natural), tem que ter praticado o delito de forma típica, antijurídica e culpável. Ele só pode ser apenado caso tenha agido de forma pessoalmente reprovável. (HILGENDORF, 2020, p. 110)

Em um Estado Democrático de Direito o direito penal tem como função principal a delimitação do poder estatal de punição. Cabe ao direito penal, portanto, condicionar sua incidência às regras da teoria do injusto (e da culpabilidade). (TAVARES, 2018a)

> O injusto penal se caracteriza pela realização de uma ação violadora de uma norma proibitiva ou mandamental e também contrária à ordem jurídica em sua totalidade. Essa ação é atribuída a um sujeito com as qualidades de pessoa deliberativa e produz uma alteração sensível da realidade, expressa na lesão ou perigo concreto de lesão de um bem jurídico. (TAVARES, 2018a)

Sob o fundamento principal na dignidade da pessoa humana (art. 1º, III, da Constituição da República) “a estrutura normativa da reponsabilidade penal tem por referência um indivíduo que pratica um comportamento proibido por uma norma penal e cuja prática poderia evitar”. (ESTELLITA, 2017)

Mas o injusto não é apenas o que resulta da lei incriminadora. É o conjunto de elementos que visa delimitar a incidência do direito penal enquanto intervenção no campo individual da pessoa. (TAVARES, 2019)

> A delimitação dessa intervenção deve passar, necessariamente, sob o crivo de dois conceitos básicos, que de certa forma integram o injusto, mas que podem já constituir, na verdade, seus pressupostos indeclináveis. O primeiro diz respeito ao conceito de sujeito. O segundo envolve a questão da conduta. (TAVARES, 2019, p. 191)

São, o sujeito e a conduta, os dois conceitos principais que formam o injusto. “O conceito jurídico de conduta pressupõe um sujeito capaz de atuar de acordo com o contexto e ajustado a uma norma proibitiva ou mandamental, bem como a um processo democrático de comunicação” (TAVARES, 2018a). Em relação ao sujeito:

> A discussão em torno do sujeito constitui, hoje, uma condição essencial para o aprofundamento das questões penais. Isso se deve à necessidade de se discutir o poder de punir e a própria legitimidade da criminalização. Na verdade, a doutrina penal tem buscado sempre uma justificativa para as normas incriminadoras. Pode-se dizer que o discurso penal tem sido um discurso legitimador. Raramente se presencia no discurso penal uma discussão mais ampla sobre a relação entre o sujeito e o poder punitivo. Parece que, diante do Estado, o sujeito não existe, daí, inclusive, ser tratado pelos funcionalistas mais radicais como mero subsistema do sistema jurídico. O sujeito só é visto de modo secundário, ou como vítima dos delitos pessoais ou patrimoniais (homicídio, lesões, sequestro, furto, roubo, extorsão etc.) ou como autor individual, no momento da individualização da pena. Nada mais do que isso. Todavia, o conceito de sujeito é relevante, especialmente como pressuposto indeclinável de um conceito de ação. (TAVARES, 2018a).

Há quem discuta, entretanto, a possibilidade de uma responsabilização dos próprios robôs a partir de uma personalidade jurídica criada para esse fim (E-Person), que seria um sujeito autônomo de responsabilidade (HILGENDORF, 2019), o qual se viabilizaria mediante o registro oficial dos robôs, criação de fundos para arcar com eventuais danos (ESTELITTA, LEITE, 2019) e até mesmo possibilidade de destruição completa das máquinas incorrigíveis. (GLESS; WEIGEND, 2019)

Como abordam Sabine Gless e Thomas Weigend (2019, p. 44 a 53) nem sempre o ser humano deteve o “monopólio da culpabilidade”, apesar da teoria do delito ser construída e direcionada a humanos, excluindo, assim, outros seres dessa capacidade (humana). Tal ideia já foi flexibilizada, por exemplo, quando se passou a admitir a responsabilidade penal de pessoas jurídicas[90]:

> Mas mesmo estas sanções (predominantemente financeiras) devem, em última instância, atingir não a entidade abstrata "pessoa jurídica", mas as pessoas naturais que estão economicamente por trás da pessoa jurídica - como acionistas ou como sócias. A possibilidade da "punição" de um agente inteligente que correspondesse ao sentido e à finalidade de uma pena aplicada a humanos é muito difícil de se imaginar atualmente. Dado que os agentes inteligentes não têm um patrimônio próprio (de qualquer maneira, não pode ele compreender que tem um patrimônio, ainda que civilmente, de alguma forma, seja-lhe assignado um patrimônio)," uma pena de multa a ele eventualmente aplicada deverá ser saldada por seu operador ou por um fundo de responsabilidade, de forma que a sanção não atingiria o agente inteligente; e muito embora uma punição "pessoal", como, por exemplo, a total destruição física ou a total reprogramação do agente inteligente, pareça, de fato e olhando de fora, uma forma de pena de morte, ela não atinge o agente da mesma forma que um ser humano - ao menos não enquanto os agentes inteligentes não forem dotados de um desejo de (sobre)viver humano. Por esta razão, no estágio atual de desenvolvimento, a punição penal de agentes inteligentes fracassa porque eles não podem sentir a pena como tal. Os humanos podem entender a destruição de um robô como sanção reprovadora por um comportamento desviado, o próprio robô, porém, não acessa esse sentido da medida sancionadora. A adoção de uma (ainda que "imperfeita") responsabilidade penal de um agente inteligente pode, porém, fazer sentido jurídico se ela puder exonerar dessa responsabilidade um agente humano que atua por trás da máquina. [...] Enquanto os agentes inteligentes só puderem "decidir" dentro dos limites de sua programação, faltar-lhes-á - em conformidade com o conceito de comportamento acima estabelecido -, possivelmente, a própria capacidade para a prática de um "comportamento" penalmente relevante. Ali onde esta capacidade for admitida, deparar-se-á com a questão fundamental sobre se é sequer possível lhes atribuir culpabilidade. Isto é questionável não só quando eles executam um processo de decisão já previsto ou ao menos previsível, mas também quando interpretam - a partir de sua própria experiência - os dados coletados no ambiente que os circunda e se decidem por um caminho próprio. Isto porque sujeitos culpáveis só podem sê-lo, de acordo com nosso atual entendimento, aqueles que têm uma consciência, portanto quem for capaz de uma autorreflexão ética. No estágio atual de desenvolvimento dos agentes inteligentes, isto não parece possível; mas é totalmente factível, para os futuros agentes inteligentes, que passem a ter uma capacidade, no mínimo, análoga para valorações morais sobre o próprio comportamento.? O último passo seria, então, a construção de uma capacidade penal de agentes inteligentes, ou seja, sua construção de uma forma que, a determinadas alterações externas, pudesse ser associado um desvalor moral de seus

[90] Para maiores informações sobre o tema, ler: SALVADOR NETTO, Alamiro Velludo. Responsabilidade penal da pessoa jurídica. São Paulo: Revista dos Tribunais, 2018 e RAGUÉS I VALLÈS, Ramon. La actuación en beneficio de la persona jurídica como presupuesto de su responsabilidad penal. Madri; Barcelona; Buenos Aires; São Paulo: Marcial Pons, 2017.

> comportamentos. Até lá, porém, há um longo caminho a percorrer. (GLESS; WEIGEND, 2019, p. 52, 53)

Apesar da ampla discussão jurídico-filosófica possível, a ideia de se responsabilizar penalmente as próprias máquinas/robôs por suas condutas violadoras de bens jurídicos está longe da realidade mundial, e mais longe ainda está do Brasil, que não detém a mínima pretensão legislativa nesse sentido, pelo contrário, ainda dá os primeiros passos na regulamentação da inteligência artificial a fim de viabilizá-la adequadamente em solo nacional.

> Segundo a legislação atual, não é possível atribuir responsabilidade à própria máquina, porque a ela falta uma condição essencial para a atribuição de responsabilidade, qual seja, a qualidade de pessoa. Segundo o direito, a pessoa capaz de atuar responsavelmente é, sobretudo, o ser humano (natural). (HILGENDORF, 2019, p. 69)

Mundialmente quem tem sido responsabilizado pelos casos de violação a bens jurídicos por sistemas autônomos, sob o aspecto criminal, até o presente momento, em 2023, são os usuários das máquinas, sejam elas máquinas de fábricas, sejam veículos autônomos, sempre com a justificativa de erro humano, porquanto a tecnologia fornecida para esses sistemas ainda obriga a participação efetiva da pessoa por detrás da máquina. Para os veículos autônomos, como se viu, a título de exemplo, os operadores ainda devem conduzir com total atenção e com as duas mãos no volante.

Ocorre que a história seguirá rapidamente por um caminho diferente. Logo as máquinas com inteligência artificial com autoaprendizagem não precisarão de interferência humana alguma em sua funcionalidade, caso contrário, as tecnologias estarão fadadas ao fracasso. Esse é o caminho lógico e até natural, porque, é presumível que ninguém quer pagar um pequena fortuna em um veículo autônomo e precisar dirigi-lo tal como se fosse um veículo nível 0 de automação, por exemplo.

Apesar do que concluiu a Professor Heloísa Estellita (2022) no Relatório Final da Comissão de Inteligência Artificial apresentado ao Congresso Nacional,

de que o mais correto seria, por ora, não autorizar a introdução dos sistemas autônomos no Brasil, parece inevitável que isso ocorra em um futuro próximo.

A partir do ingresso e comercialização dessa tecnologia no mercado nacional, o Brasil precisará enfrentar os mesmos questionamentos que os demais países do mundo já vêm recebendo com o avanço rápido da tecnologia, ainda que seja para, eventualmente, estudar uma alteração legislativa que abarcará a responsabilização tanto no âmbito cível, quanto penal, para trazer de um lado, a proteção da sociedade e, de outro, segurança jurídica a todos os participantes do processo de desenvolvimento e implementação dessas máquinas.

Regular a matéria ou definir como ela será tratada é relevante para o incentivo de seu desenvolvimento, que é objetivo tão caro das regulamentações sobre inteligência artificial. Dizendo de outro modo, não seria eficiente desenvolver planos de atuação, incentivar financeiramente etc., se há tamanha insegurança jurídica aos desenvolvedores, fabricantes e usuários.

Enquanto não houver um aprofundamento na verificação sobre a necessidade de regulação da responsabilidade penal dos próprios sistemas autônomos, ao menos é essencial que o direito delimite as zonas do lícito e do ilícito e assim, dimensione adequadamente quais são os requisitos específicos para responsabilizar as chamadas pessoas “detrás” (GLESS, WEIGEND, 2019), porque, como visto anteriormente, as violações a bens jurídicos protegidos já vêm ocorrendo.

Isso tem um contorno ainda mais relevante numa tecnologia tão avançada, especialmente dentro da tipicidade, no que tange ao nexo causal, porque diversas são as pessoas envolvidas no desenvolvimento e manutenção das máquinas.

> A introdução de robôs na interação com humanos envolverá um plexo de atores envolvidos em sua criação, fabricação, manutenção, operação e controle. Isso coloca a questão de quem (e a que título) deverá ser responsabilizado quando o resultado típico é causado pela interposição de um sistema autônomo, ou mesmo híbrido. Pode-se pensar, então, em

> analisar desde a possível responsabilidade penal de um pesquisador, passando pela do programador, do fabricante, do vendedor, do proprietário e do usuário... (ESTELLITA, LEITE, 2019, p. 32)

As violações a bens jurídicos decorrentes de sistemas autônomos, em certa medida, podem propor as mesmas dificuldades enfrentadas pela criminalidade de empresa, que também impacta a imputação individual.[91]

> Se a pergunta inicial e fundamental para a imputação de responsabilidade penal individual é "quem praticou a conduta típica, a resposta, no âmbito da criminalidade de empresa, poder enormemente laboriosa, quando não, impossível (ESTELLITA, 2017)

Existe um perceptível sinal amarelo diante da dificuldade de imputação nos casos em que um crime aparenta ser praticado por uma máquina, pois, como abordado, os "robôs" não têm capacidade penal (HIGELDORF, 2020) e há risco de "dispersão de responsabilidade" em relação aos humanos detrás, ou seja, aqueles envolvidos no desenvolvimento e implementação das máquinas e eventuais manutenções, também porque a violação ao bem jurídico estará despersonalizada, diluída em muitas condutas e, como regra, ocorrerá longe do agente. (ESTELLITA, 2017)

> Com os novos desenvolvimentos tecnológicos, essa compreensão de responsabilidade focada no indivíduo concreto encontra seus limites nos sistemas tecnológicos em rede: quem deve ser responsabilizado, caso o agente individual seja apenas um de muitos que, só por meio da soma de suas contribuições no sistema, tenham dado causa à específica consequência? Qual é o papel desempenhado por agentes tecnológicos (sistemas computacionais autônomos)? A atribuição de responsabilidade, nesses casos, torna-se nebulosa. Com isso, surge o risco de uma dissolução – dispersão – de responsabilidade (HILGENDORF, 2020, 110).

Como citado, a dificuldade parece existir especialmente em razão das diversas pessoas que participam da cadeia de criação, desenvolvimento e

[91] Para maiores informações ler: ESTELLITA, Heloísa. Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas , limitadas e encarregados de cumprimento por crimes praticados por membros de empresa – 1. ed. – São Paulo: Marcial Pons, 2017.

disponibilização dessas máquinas, cuja participação se estende até o próprio operador. Hilgendorf (2020), citando o caso Tay já mencionado neste trabalho:

> "Suponha-se que o sistema Tay, manipulado, ofenda a usuária N. Alguém pode responder penalmente por isso? O próprio Tay não é capaz de culpabilidade, os manipuladores, em caso de dúvida, não são conhecidos. Mesmo que fosse possível encontrá-los, seria necessário perguntar se lhes seria imputável um dolo em relação à concreta ofensa à usuária N, como exigido pelo §185 StGB (não há crime de ofensa culposa). Em relação ao programador que, em ultima instancia, deixou aberto um espaço de possibilidade, que permitia o aprendizado de comportamentos ofensivos, também dificilmente se poderia afirmar um dolo. Portanto, precisamos lidar, aqui, com um caso relativamente claro de dispersão de responsabilidade – uma ofensa sem ofensor penalmente responsável. De uma perspectiva de lege ferenda, surge a questão de se faria sentido criar um tipo penal que criminalizasse o dano a bens jurídicos por máquinas de autônomas de autoaprendizagem. O pano de fundo da questão – como mencionado anteriormente – são os fatos de que 1) máquinas não têm capacidade penal e 2) uma imputação de dano a um sujeito penal humano e, frequentemente, impossível." (HILGENDORF, 2020, p. 120)

Mas, no direito penal brasileiro, de forma geral, quem dá causa ao resultado final pode, em tese, ser responsabilizado, conforme estabelece o *caput* do art. 13, do Código Penal. Basta entender como pode-se - ou deve-se - responsabilizar as pessoas participantes dessa cadeia de desenvolvimento.

6. DO PROCESSO DE IMPUTAÇÃO

Na teoria do delito, no âmbito do injusto, é fundamental o processo de imputação que se baseia na atribuição de responsabilidade a alguém pela prática de uma conduta proibida. Esse processo de imputação abarca tanto aspectos objetivos como subjetivos.

A análise, para fins de imputação, deve se iniciar sob os aspectos objetivos “porque o crime manifesta sua existência como realidade objetiva, cuja configuração concreta é o ponto de partida da pesquisa empírica do fato criminoso, o tipo objetivo constitui a base do processo analítico...”. (CIRINO DOS SANTOS, 2017)

A partir da existência de uma ação típica e de um resultado, é necessário verificar o processo de imputação porquanto o injusto somente poderá ser atribuído a um sujeito quando o resultado decorrer de um comportamento seu (TAVARES, 2019).

> O processo de imputação, por isso mesmo, deve-se desenvolver objetiva e subjetivamente, como forma de medição dessa intensidade, sobre duas bases. Na primeira, assenta-se em que, dentro da perspectiva de garantia, é indispensável a demonstração inequívoca de que o injusto tenha que ser objetivamente determinado, de modo que não reste dúvida de que a conduta incriminada fora realizada pelo sujeito. Na segunda, de que essa conduta tenha que ser individualizada, quer dizer, sobre ela se proceda a uma depuração empírica de seus elementos de modo a identificar com precisão a exata contribuição do sujeito na sua execução [...] A imputação objetiva tem como pressuposto indeclinável a afirmação da causalidade entre a conduta do agente e o resultado. (TAVARES, 2019)

Para fins de imputação é essencial a análise do conceito de causalidade. Assim, são diversas as teorias da causalidade, sendo as mais relevantes a teoria da equivalência de condições, teoria da causalidade adequada, teoria da relevância jurídica e teoria da causalidade funcional. (TAVARES, 2018b).

O Brasil adota no art. 13, do Código Penal, a teoria da equivalência de condições, ou teoria da condição, para a qual não se procede distinção entre todas as condições que causam o resultado (MASSON, 2023).

> Como mencionado, o Código Penal brasileiro adotou a teoria da equivalência dos antecedentes causais, também conhecida como teoria da conditio *sine qua non*. Dessa maneira, considera-se causa todo fato humano sem o qual o resultado não teria ocorrido, o que se afere pelo critério do juízo hipotético de eliminação. (ANDERSON DE SOUZA, 2022)

> Na lei penal brasileira, a fórmula da exclusão hipotética da condição para determinar a relação de causalidade - embora critérios científicos não devam ser fixados na lei - está inscrita no art. 13, CP: Art. 13. O resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido. (CIRINO DOS SANTOS, 2017)

Mas é compatível com o sistema brasileiro a separação entre causação do resultado e sua imputação. Como ensina Juarez Cirino dos Santos:

> A moderna distinção entre causação do resultado e imputação do resultado, correspondente aos processos de determinação causal e de imputação pessoal do resultado, além de ajudar a resolver velhos problemas da teoria da equivalência das condições, é inteiramente compatível com a legislação brasileira, observados os seguintes princípios: 1) O resultado é o produto real de todos os fatores que o constituem: no limite, a ação do médico que protela a morte inevitável do paciente é condição do resultado de morte deste, porque influi na existência real do acontecimento concreto; mas como a causalidade não é o único critério de atribuição do resultado, a mera relação de causalidade não permite atribuir o resultado de morte ao médico. (CIRINO DOS SANTOS, 2017)

O §1º do art. 13, do Código Penal adota a teoria da causalidade adequada que prevê que para que o resultado seja atribuído a uma determinada pessoa, é necessário que ela realize uma atividade adequada à concretização do resultado (MASSON, 2023).

> É importante notar que a lei brasileira considera a independência relativa do novo curso causal como excludente da imputação do resultado - e não como excludente da relação de causalidade, admitindo, portanto, a moderna distinção entre causação e imputação do resultado: Art. 13, §1°. A superveniência de causa relativamente independente exclui a imputação quando, por si só, produziu o resultado; os fatos anteriores, entretanto, imputam-se a quem os praticou. (CIRINO DOS SANTOS, 2017)

A teoria da adequação entende como causa uma conduta adequada à produção do resultado, excluindo condutas aleatórias que venham a alcançar o

resultado coincidentemente, ou por acidente. É o famoso exemplo de uma pessoa que convence outra a fazer uma viagem de avião e o avião cai, causando a morte do viajante. A pessoa sobrevivente não será responsabilizada criminalmente por esse fato.

Se a teoria da adequação identifica a causa como condição adequada à produção do resultado seria ela capaz de resolver, a um só tempo, a questão do nexo causal, mas também, a questão da imputação do resultado, pois entender qual é a causa adequada à realização do tipo é entender qual o fundamento da atribuição do resultado ao autor. (CIRINO DOS SANTOS, 2017)

Conforme Juarez Tavares (2019, p. 260) a análise da imputação, via de regra, é realizada de forma vinculada ao nexo causal, exatamente porque o art. 13 do Código Penal "seguindo a tradição legislativa, a pressupõe como condição do resultado" (TAVARES, 2019). Mas caso esse entendimento seja adotado com rigor apenas terá sentido a imputação aos crimes de resultado e não nos de mera atividade. Defende, assim, que a partir da demonstração do nexo de causalidade entre a conduta e o resultado, esta, sozinha, não pode servir a fundamentar a responsabilidade típica objetiva. Até porque admite-se a causalidade na omissão[92], portanto, o processo de imputação se estende ao "risco de produção do resultado em face da ação devida" (TAVARES, 2019).

A ideia do risco surge de forma consolidada com a teoria da imputação objetiva, que pretende estabelecer critérios normativos para fundamentar a imputação de um resultado, o que indica a melhor alternativa às resoluções das problemáticas apresentadas pelas dificuldades de atribuição de responsabilidade penal decorrente de condutas praticadas, a primeira vista, por máquinas/robôs.

> Se a questão da causalidade já está solucionada, positivamente, e como o que agora se discute é acerca de critérios objetivos limitadores da imputação, não haverá necessidade de se projetarem critérios positivos, mas apenas

[92] Para aprofundamento no tema ler: GRECO, Luís. Problemas de causalidade e imputação objetiva nos crimes omissivos impróprios – Luís Greco; tradução Roman Rocha, 1. ed. – São Paulo: Marcial Pons, 2018.

> negativos de atribuição. A teoria da imputação objetiva, portanto, não é uma teoria para atribuir, senão para restringir a incidência da proibição ou determinação típica sobre determinado sujeito. Simplesmente, por não acentuarem esse aspecto, é que falham no exame do injusto inúmeras concepções que buscam fundamentá-lo. [...] Tendo em vista essa finalidade de lançar objetivamente as bases de uma responsabilidade pessoal e não apenas causal, a doutrina busca estabelecer os critérios normativos que possam fundamentar a imputação objetiva em relação a um resultado típico, conforme os fins de proteção da norma e o alcance do tipo de injusto. Situando-se desse modo frente à sociedade pós-moderna, propõe ROXIN que esses critérios normativos tenham que se referir necessariamente aos pressupostos da própria incriminação, quer dizer, pressupõe que o agente, com sua conduta, tenha incrementado um risco para o bem jurídico, risco esse indevido e materializado como resultado no âmbito da extensão do tipo de delito. (TAVARES, 2019)

7. TEORIA DA IMPUTAÇÃO OBJETIVA

A teoria da imputação objetiva tal como se desenvolveu e foi difundida no Brasil surgiu próximo de 1970. A ideia do risco por ela trazida, criada por Claus Roxin, tem origem antes, em 1962, com incremento dos alunos Rudolphi e Werner Schunneman que contribuíram para a ideia do fim de proteção e definição do alcance do tipo. (ROXIN, 2006)

Como teoria normativa, ela origina-se da filosofia de Hegel, a partir da qual Larenz em 1927 extrai a concepção da imputação objetiva (TAVARES, 2019), aplicada depois por Honing na dogmática jurídico-penal. (ROXIN, 2006).

Juarez Tavares (2019, p. 296) indica que para o Direito Penal a verificação da teoria se deu a partir de um livro de Werner Hardwig, conforme informações de Reyes Alvarado e Schunemann.

Independente da paternidade de suas origens, o fato é que a teoria se consolidou e propagou a partir dos estudos formulados por Roxin. Ele próprio, em 1994, esclareceu que o grande diferencial da teoria situa-se no que convencionou chamar de teoria do risco, a fim de superar o sistema jurídico penal clássico que fundamentava o tipo na causalidade (ROXIN, 2006).

A fim de melhor compreender a teoria da imputação objetiva, é relevante abordar sumariamente[93] o contexto histórico de que no começo do século XX a doutrina penal utilizava-se da teoria causal que limitava a teoria do delito pela causalidade (TAVARES, 2018b) e, assim, entendia-se que quem participasse do processo causal como condição essencial ao resultado dava causa a ocorrência do fato típico e, portanto, cometeria o crime (GRECO, 2014).

Como originária do positivismo que imperava à época, na teoria causal o objeto da norma penal é o resultado de dano ou de perigo que é constatado a

[93] Para aprofundamento no tema ler: TAVARES, Juarez. Teoria do Crime Culposo, 5ª ed. São Paulo: Tirant lo Blanch, 2018, p. 53 e ss.

partir da causalidade. Os componentes do delito são meros atributos legais da conduta (TAVARES, 2019).

> O sistema jurídico-penal "clássico" alemão, desenvolvido na virada do século principalmente por Liszt e Beling, fundamentava o tipo no conceito de causalidade. Considerava-se realizado o tipo toda vez que alguém constituía uma condição para o resultado nele previsto, ou seja, toda vez que alguém o causava, no sentido da teoria da equivalência dos antecedentes. Acabava o tipo, assim, com uma grande extensão, pois, nesta perspectiva, praticou uma ação de matar não só aquele que disparou o tiro mortífero, mas todos que contribuíram para o resultado com uma *condictio sine qua non*: o fabricante e o vendedor do revólver e da munição, aqueles que ocasionaram a desavença da qual resultou o tiro, até mesmo os pais e outros antecedentes do criminoso. (ROXIN, 2006)

Essa corrente encontra severas críticas pelo risco de regresso ao infinito, já que é possível incluir no curso causal diversos participantes essenciais ao resultado típico, tendo como exemplo mais comum os pais do agente, que o geraram, e sem os quais, portanto, o resultado não seria alcançado. Outras críticas foram situadas em relação aos crimes omissivos, porquanto neles não há a conduta de interferência no curso causal e sim o contrário. Quem deveria agir para evitar o resultado, não o faz (GRECO, 2018)[94]. Esses e outros problemas imputados à teoria tentavam ser resolvidos pelos doutrinadores no aspecto subjetivo - dolo ou culpa (GRECO, 2014).

> La primeira quebra de este sistema comienza a aparecer em su propia base, em el concepto de acción. Pronto se demonstro que el concepto causal de acción era incapaz de sostener todo el edifício de la Teoría del Delito. Ya em 1904, el filósofo del Derecho y penalista GUSTAV RADBRUCH, discípulo de VON LISZT, demonstro la impossibilidade de reducir los conceptos de acción y omisión a um denominador común al no haber em la omisión movimiento corporal alguno y ser, por esencia, la negación de uma acción. (MUÑOZ CONDE, 2004)

Tanto que até mesmo o tipo omissivo era resumido ao aspecto subjetivo. BOTTINI (2018, p. 25) esclarece que "entendia-se omissão como um não fazer

[94] Para maior aprofundamento no assunto, ler: BOTTINI, Pierpaolo Cruz. Crimes de omissão imprópria. 1ª ed. – São Paulo: Marcial Pons, 2018, p. 24 e ss.; e GRECO, Luís. Problemas de causalidade e imputação objetiva nos crimes omissivos impróprios. 1ª ed. – São Paulo: Marcial Pons, 2018, p. 18 e ss.

algo, que só adquiria sentido quando acompanhado de uma vontade consciente de não fazer".

Houve então na história mundial uma alteração de rumo que fez com que a teoria do delito sofresse influência neokantiana, que se fixa no dever ser e, assim, se afastasse dos aspectos positivistas, de maneira que o objeto da norma penal deixou de ser extraído diretamente do texto da lei e passou a ter um direcionamento normativo, ou seja, ser valorado anteriormente. Isso quer dizer que no neokantismo "o injusto é produto de uma criação normativa, sem referência real, como resultado de juízos de valor, tendo em vista o objetivo visado pelo legislador (TAVARES, 2019).

Há pelo neokantismo uma revolução da relação tipo-antijuridicidade. O tipo perde sua autonomia e começa a existir como fundamento da antijuridicidade, ou seja, o injusto surge "através da realização de uma conduta prevista na lei como crime" (TAVARES, 2019). É a partir do neokantismo que há a ruptura pelo nacional partido socialista alemão, que tem como base fundamental o *Volksgemeinschaft* ou o "são sentimento do povo" (REALE JR, 2000).

> A vida da comunidade não é limitada pelas leis, pois o direito está além das leis positivas, como expresso da comunidade. Desse modo, a um caso concreto pode ser aplicada uma solução não normativa, mas jurídica, derivada do ordenamento concreto. [...] Toda certeza jurídica desaparece quando se procura realizar a justiça material, fundada apenas no sentimento jurídico efetivo ou factual da comunidade. Comprova-se a reforma do §2.º do Código Penal, que não só deu possibilidade de analogia no direito penal, como fixou as diretrizes para a interpretação das normas penais, cuja aplicabilidade deveria ser feita segundo o são sentimento do povo. A analogia é adotada segundo a ideia de que deve ser punível toda a ação de acordo com o pensamento fundamental de uma lei penal, por ser esta a expressão do querer comunitário. (REALE JR., 2000, p. 24/25)

Posteriormente ao fim da Segunda Guerra Mundial a teoria do delito altera seu direcionamento com a teoria finalista, que já havia surgido na década de 30 e que define a atividade criminosa como sendo aquela finalisticamente dirigida, ou seja, o tipo deveria ser complementado por um composto humano,

que seria a finalidade (GRECO, 2014). Também há, como no neokantismo, uma menor preocupação com o resultado.

Conforme Juarez Tavares (2018b, p. 65) ensina “o que marca de modo nítido a postura finalista na teoria do delito é a consideração da ação como atividade consciente dirigida a um objetivo”.

> ....levantou-se, por volta da década de 1930, a teoria finalista da ação, fundada principalmente por WELZEL, que vê a essência da ação humana não no puro fenômeno natural de *causação*, e sim no direcionamento, guiado pela vontade humana, de um curso causai no sentido de um determinado fim antes tomado em vista. Esta compreensão da conduta como ato finalístico, orientado a um objetivo, evita consideravelmente o *regressus ad infinitum* da teoria causai da ação, eis que, ao contrário dela, já analisa o dolo no nível do tipo, como a parte subjetiva deste. Em virtude disso, o posicionamento do dolo no tipo é aceito quase unanimemente pela ciência jurídica alemã. O grande progresso que trouxe a teoria finalista da ação limita-se, porém, ao tipo subjetivo. Para a realização do tipo objetivo, considera ela suficiente a mera relação de causalidade, no sentido da teoria da equivalência. Com isso, o tipo continua demasiado extenso. (ROXIN, 2006)

Percebendo os problemas destas teorias principais, Roxin (2006, p. 103) tenta resolvê-los pela teoria da imputação objetiva que, resumidamente, estabelece que o resultado causado por determinada pessoa só pode ser a ela imputado se preencher determinados requisitos objetivos, sendo eles especialmente: a conduta do autor criar um risco não permitido, este risco se realizar no resultado e este resultado estar dentro do tipo previsto (GRECO, 2014). Melhor dizendo:

> Em sua forma mais simplificada, diz ela: um resultado causado pelo agente só pode ser imputado como obra sua e preenche o tipo objetivo unicamente quando o comportamento do autor cria um risco não permitido para o objeto da ação (1), quando o risco se realiza no resultado concreto (2) e este resultado se encontra dentro do alcance do tipo (3) (ROXIN, 2006, p. 104)

No que tange ao risco, esse deve ser o não autorizado. Isso porque a sociedade admite diversos riscos e perigos para que a vida comum se desenvolva, tendo como exemplo mais comum a direção de veículos. Trata-se, nesse caso, de um risco permitido. (TAVARES, 2018a)

Pretende tal teoria, portanto, estabelecer critérios normativos que justifiquem a imputação de um fato típico a alguém. Para GRECO (2014, p. 23) “a imputação objetiva enuncia o conjunto de pressupostos genéricos que fazem da causação uma causação objetivamente típica”.

> Tendo em vista essa finalidade de lançar objetivamente as bases de uma responsabilidade pessoal e não apenas causal, a doutrina busca estabelecer os critérios normativos que possam fundamentar a imputação objetiva em relação a um resultado típico, conforme os fins de proteção da norma e o alcance do tipo de injusto. Situando-se deste modo frente à sociedade pós-moderna, propõe ROXIN que esses critérios normativos tenham que se referir necessariamente aos pressupostos da própria incriminação, quer dizer, pressupõe que o agente, com sua conduta, tenha incrementado um risco para o bem jurídico, risco esse indevido e materializado como resultado no âmbito de extensão do tipo de delito. (TAVARES, 2019, p. 296)

Claus Roxin (1997) aprofunda a explicação esclarecendo que a imputação do tipo objetivo tem dois grandes passos sucessivos, sendo o primeiro o respeito à causalidade e o segundo o respeito aos demais pressupostos, como se vê:

> “... la imputación al tipo objetivo debe producirse em dos passos sucesivos: en una primeira sección (A) se expondrá la teoría del nexo o relación causal; y a continuación se tratarán en una segunda sección (B) los restantes presupuestos de la imputación.” (ROXIN, 1997)

A teoria tal como desenvolvida se preocupa por excluir do tipo os acontecimentos fortuitos:

> a)Un resultado causado por el agente sólo se puede imputar al tipo objetivo si la conducta del autor ha creado un peligro para el bien jurídico no cubierto por un riesgo permitido y ese peligro también se ha realizado en el resultado concreto. Así p.ej. en el caso de la tormenta mencionado en el nm. falta ya una acción homicida en el sentido del § 212 porque el hecho de enviar a alguien al bosque no crea un peligro Jurídicamente relevante de matar. Em el caso del incendio del hospital el disparo del autor ciertamente ha creado un peligro no permitido de matar a la víctima; pero en el incendio del hospital no se realiza el peligro que parte de una lesión consecuencia de un disparo, de tal modo que por esa razón no se le puede imputar el resultado al autor como homicidio consumado. Mientras que la falta de creación de peligro conduce a la impunidad, la falta de realización del peligro en una lesión

> típicadel bien jurídico sólo tiene como consecuencia la ausencia de consumación, por lo que en su caso se puede imponer la pena de la tentativa. B) Si el resultado se presenta como realización de un peligro creado por el autor, por regla general es imputable, de modo que se cumple el tip objetivo. Pero no obstante, excepcionalmente puede desaparecer la imputación si el alcance del tipo no abarca la evitación de tales peligros y sus repercusiones. Si p.ej. A incita a B a que haga una escalada al Himalaya, en la que éste —tal como A había previsto— sufre un accidente mortal, entonces no sólo A ha causado la muerte de B, sino que en la muerte de B también se há realizado un peligro causado por A. Y sin embargo A no ha cometido una acción punible de homicidio, puesto que si según el Derecho [alemán] vigente es impune incluso la incitación al suicidio, con mayor razón aún ha de ser impune la incitación a una mera autopuesta en peligro, que es de lo que aquí se trata. Por consiguiente, el alcance de los §§ 212, 222 y 230 no se extiende a la evitación de autopuestas en peligro dolosas, con lo que por esa razón no se puede imputar el resultado al incitador. En resumen, pues, se puede decir que la imputación al tipo objetivo presupone la realización de un peligro creado por el autor y no cubierto por um riesgo permitido dentro del alcance del tipo. A continuación se desarrollará este punto de partida con más detalle. (ROXIN, 1997)

Então, em resumo, imputação é o processo pelo qual se fundamenta a atribuição de responsabilidade pela prática de uma conduta ilícita e a teoria da imputação objetiva condiciona esse processo a requisitos normativos, essenciais e objetivos.

> E agora podemos chegar aos dias de hoje à teoria da imputação objetiva. O que essa teoria faz é relegar o tipo subjetivo e a finalidade a uma posição secundária e recolocar o tipo objetivo no centro das atenções. Este tipo objetivo não pode, porém, esgotar-se na mera causação de um resultado — é necessário algo mais para fazer desta causação uma causação objetivamente típica. Este algo mais compõe-se, fundamentalmente, de duas ideias: a criação de um risco juridicamente desaprovado e a realização deste risco no resultado. (GRECO, 2014, p. 9)

Os elementos do fato típico, a partir dessa teoria, passam a ser:

> a) a conduta (ação ou omissão); b) resultado (quando for o caso, ou seja, em crimes de dano ou de perigo concreto); c) nexo causal (com a mesma ressalva anterior); d) tipicidade (juízo de subsunção entre a conduta concreta e a descrição típica); e e) imputação objetiva. A essência da imputação objetiva consiste na identificação de um risco juridicamente desaprovado, criado ou incrementado pelo agente. A base de sua construção encontra-se em critérios políticos-criminais. Cuida-se, então, de um filtro a mais para a atribuição de um evento criminoso a alguém, o que significa que tem a teoria – em sua versão originária – por objetivo refinar a análise, diminuindo, dessa maneira, a incidência penal. (Anderson de Souza, 2022)

Dentre esses requisitos, ao que interessa principalmente ao presente trabalho, é que o agente, por meio de sua conduta, deve criar um risco não permitido para o bem jurídico ou incrementar um risco já existente, risco este que deve ser indevido e materializado no resultado (dentro do âmbito de alcance do próprio tipo).

> O fundamento da adoção de critérios negativos de avaliação do processo de imputação é enunciado pela doutrina, inclusive ROXIN, sobre a base da finalidade protetiva da norma, isto é, não haverá imputação, genericamente, quando a ação do agente e o respectivo resultado não se incluírem no âmbito de proteção fixado pela norma penal. Evidentemente, embora se postule, em sentido contrário, que a norma penal não deve ser compreendida em seu momento protetivo, que é, empiricamente, indemonstrável e, ademais, tão só legitimante da incriminação, mas apenas em seu sentido delimitativo do poder incriminador, pode-se concordar que não haverá imputação quando o fato se situar além dos limites do que é proibido. Está claro, então, que todo o processo de imputação não é matéria exclusiva da tipicidade, mas de toda a ordem jurídica. Isto não obsta, entretanto, a que sejam analisados, desde logo, na própria tipicidade os critérios negativos da imputação. Pode-se dizer, assim, que não haverá, alternativamente, imputação se: a) o agente tiver diminuído o risco para o bem jurídico; b) o agente não tiver aumentado o risco para o bem jurídico; c) o risco era permitido; c) esse risco não se materializar no resultado típico; d) o resultado, na forma como ocorrido, não se incluir no âmbito de alcance do tipo. (TAVARES, 2019, p. 297)

Mas, como o tipo por excelência para condutas praticadas por sistemas autônomos é o culposo, então, além da criação do risco, ou possível aumento do risco e sua realização no resultado, de acordo com a teoria da imputação objetiva sempre será necessário analisar[95] outros requisitos subjetivos, como a previsibilidade e a evitabilidade do resultado (TAVARES, 2018b), como será abordado em tópico próprio.

7.1. DA APLICABILIDADE DA TEORIA DA IMPUTAÇÃO OBJETIVA NO SUPERIOR TRIBUNAL DE JUSTIÇA

[95] Para aprofundamento no tema ver: TAVARES, Juarez. Teoria do Crime Culposo, 5ª ed. São Paulo: Tirant lo Blanch, 2018

No que tange à aplicabilidade da teoria da imputação objetiva no Brasil, o Superior Tribunal de Justiça em algumas oportunidades enfrentou a matéria, adotando-a, como revela a jurisprudência:

Em dezembro de 2022, a Sexta Turma do colendo Superior Tribunal de Justiça no julgamento do Agravo Regimental e Recurso em Habeas Corpus (AgRg no RHC), processo nº 164.698/PE[96], sob Relatoria do Ministro Olindo

[96] AGRAVO REGIMENTAL NO RECURSO EM HABEAS CORPUS. APROPRIAÇÃO INDÉBITA PREVIDENCIÁRIA. SONEGAÇÃO DE CONTRIBUIÇÃO PREVIDENCIÁRIA. TRANCAMENTO DA AÇÃO PENAL POR INÉPCIA DA DENÚNCIA. DESCRIÇÃO INSUFICIENTE DA CONDUTA. FALTA DE RESPONSABILIDADE LEGAL ACERCA DOS FATOS. POSIÇÃO EM GRUPO ECONÔMICO QUE NÃO INDUZ AUTORIA. 1. O trancamento da ação penal em habeas corpus, por falta de justa causa ou por inépcia da denúncia, situa-se no campo da excepcionalidade, somente cabível quando houver comprovação, de plano, a ausência de justa causa, seja em razão da atipicidade da conduta supostamente praticada pelo acusado, seja da ausência de indícios de autoria e materialidade delitiva, ou ainda da incidência de causa de extinção da punibilidade. 2. Existe plausibilidade da alegação defensiva de inépcia, no tocante à ausência de descrição concreta da conduta do paciente, quanto aos crimes imputados, haja vista que a empresa Zhiuatanejo do Brasil Açúcar e Álcool S/A, em Recuperação Judicial, tinha sua própria diretoria, embora integrasse um grupo maior, de modo que a responsabilidade penal é da diretoria da empresa, e não de um acionista, mesmo majoritário, sem falar que a figura do administrador de fato não define responsabilidade penal. 3. Verifica-se da denúncia que, nos anos de 2010 a 2012, em relação à empresa Zhiuatanejo do Brasil Açúcar e Ácool S/A, em processo de recuperação judicial, e após auditoria fiscal realizada pela Receita Federal, constataram-se supostos ilícitos tributários, resultando em duas representações fiscais para fins penais de ns. 10480.722603/2014-78 e 10480.730324/2016-40. 4. Acrescentou a peça que Flávia Coelho detinha a responsabilidade da gestão financeira, mas que as decisões nesse tocante seriam tomadas de modo colegiado, e que havia um comitê na matéria, composto por Flávia, Marco Aurélio (diretor de operações) e Ricardo Chaves (diretor de controladoria) e outras pessoas. 5. Aponta o Ministério Público que as informações dos inquiridos estão em conformidade com as auditorias presente nas representações fiscais, pelo que indica que o agravante, além de acionista, também seria administrador de fato da empresa e o presidente do Grupo "Eduardo Queiroz Monteiro", no qual inserida a empresa Zihuatanejo. 8. Assim postos os fatos, afigura-se procedente a tese do agravante, de que a denúncia, a despeito de imputar os fatos à empresa Zhiuatanejo do Brasil Açúcar e Álcool S/A, em Recuperação Judicial, que tinha diretoria própria, também os imputa ao recorrente, Presidente do Grupo (empresarial) Eduardo Queiroz Monteiro, mas sem descrever, no tempo, na forma e no espaço, que condutas causais teria ele, que não era dirigente da empresa, ainda que acionista majoritário da empresa, praticado ou contribuído para os crimes constantes da denúncia - art. 168-A ("apropriaçao indébita previdenciaria") e art. 337-A, inciso III ("sonegação de contribuição previdenciária"), e art. 1º, inciso I, da Lei 8.137/90, as duas primeiras em concurso material e todas em continuidade delitiva -, cujas molduras fáticas, aliás, vêm superpostas na denúncia. 7. Afirmou o recorrente, conforme consta da denúncia, que era acionista da Zihuatanejo desde o início da empresa, mas que nunca compôs os quadros de diretoria da empresa, havendo uma diretoria executiva da Zihuatanejo composta de diretores e gerentes, detentora de atribuição de gestão financeira. 8. Mas a denúncia, louvando-se em prova testemunhal - declarações prestadas por Flávia, Marcos Aurélio e José Ricardo -, e em matérias jornalísticas colacionadas pela auditoria em ambas as representações fiscais para fins penais, afirma que "Por tudo isso, pode-se concluir que Eduardo Queiroz Monteiro, na qualidade de administrador de fato da Zhiuatanejo do Brasil Açúcar e Álcool S/A Em Recuperação Judicial deixou de repassar aos cofres públicos os valores recolhidos a título de contribuição previdenciária; reduziu o recolhimento de contribuição previdenciária mediante a omissão de remuneração, receitas e demais fatos geradores; e suprimiu tributo mediante a omissão de informações às autoridades fazendárias.9. Dir-se-ia que o recorrente, na

Menezes (Desembargador Convocado do Tribunal Regional Federal da 1ª Região) trancou ação penal por reconhecer a inépcia de uma denúncia que não descrevia as condutas da pessoa física denunciada que seriam voltadas para a finalidade da imputação, *"em termos de imputação objetiva, sob pena um indevido regressus ad infinitum na cadeia causal, que poderia chegar ao todos os acioniatas!"*.

Isso porque, entendeu o STJ que não foi feita a descrição concreta da conduta daquele Paciente quanto aos crimes que foram a ele imputados, pois a empresa, naquele caso, tinha diretoria própria, ainda que fizesse parte de um grupo empresarial maior e, dessa forma, a responsabilidade penal seria da diretoria da empresa e não de um acionista, mesmo se ele fosse majoritário. Decidiu o STJ que a denúncia não descreveu que condutas causais teria ele, que não era dirigente da empresa, ainda que acionista majoritário da empresa, praticado ou contribuído para os crimes constantes da denúncia, que eram o do art. 168-A ("apropriaçao indébita previdenciaria") e art. 337-A, inciso III ("sonegação de contribuição previdenciária"), e art. 1º, inciso I, da Lei 8.137/90. Foi nesse sentido que aplicou a teoria da imputação objetiva, afastando uma análise meramente causal para reconhecer como inepta a denúncia.

No Habeas Corpus, processo nº 68.871/PR, julgado pela Sexta Turma do Superior Tribunal de Justiça, sob Relatoria da Ministra Maria Thereza de Assis Moura, com Relatoria para acórdão do Ministro Og Fernandes, em 06.08.2009, a ação penal respectiva foi trancada porque, à luz da teoria da imputação objetiva não foi demonstrada a criação do risco não permitido pelo então paciente, ou, que teria ele aumentado o risco permitido. Neste sentido, eis a ementa:

---

qualidade de Presidente do Grupo Empresarial, poderia ter alguma participação nas condutas dadas como delitivas, até mesmo como interessado, pois era o maior acioniata a empresa, **mas isso não dispensaria a denúncia de descrever a (s) sua(s) condutas voltadas para a finalidade, na estrutura diretiva da empresa Zhiuatanejo do Brasil Açúcar e Álcool S/A Em Recuperação Judicial, em termos de imputação objetiva, sob pena um indevido regressus ad infinitum na cadeia causal, que poderia chegar ao todos os acioniatas!** 10. Agravo regimental provido, a fim de conceder o habeas corpus e trancar a ação penal n. 0815080-23.2020.4.05.8300 por inépcia. (AgRg no RHC n. 164.698/PE, relator Ministro Olindo Menezes (Desembargador Convocado do TRF 1ª Região), Sexta Turma, julgado em 6/12/2022, DJe de 19/12/2022.)

> HABEAS CORPUS. HOMICÍDIO CULPOSO. VÍTIMA - MERGULHADOR PROFISSIONAL CONTRATADO PARA VISTORIAR ACIDENTE MARÍTIMO. ART. 121, §§ 3º E 4º, PRIMEIRA PARTE, DO CÓDIGO PENAL. TRANCAMENTO DE AÇÃO PENAL. AUSÊNCIA DE JUSTA CAUSA. **1. Para que o agente seja condenado pela prática de crime culposo, são necessários, dentre outros requisitos: a inobservância do dever de cuidado objetivo (negligência, imprudência ou imperícia) e o nexo de causalidade.** 2. No caso, a denúncia imputa ao paciente a prática de crime omissivo culposo, no forma imprópria. **A teor do § 2º do art. 13 do Código Penal, somente poderá ser autor do delito quem se encontrar dentro de um determinado círculo normativo, ou seja, em posição de garantidor.** 3. A hipótese não trata, evidentemente, de uma autêntica relação causal, já que a omissão, sendo um não-agir, nada poderia causar, no sentido naturalístico da expressão. Portanto, a relação causal exigida para a configuração do fato típico em questão é de natureza normativa. 4. Da análise singela dos autos, sem que haja a necessidade de se incursionar na seara fático-probatória, verifico que a ausência do nexo causal se confirma nas narrativas constantes na própria denúncia. 5. Diante do quadro delineado, não há falar em negligência na conduta do paciente (engenheiro naval), dado que prestou as informações que entendia pertinentes ao êxito do trabalho do profissional qualificado, alertando-o sobre a sua exposição à substância tóxica, confiando que o contratado executaria a operação de mergulho dentro das regras de segurança exigíveis ao desempenho de sua atividade, que mesmo em situações normais já é extremamente perigosa. **6. Ainda que se admita a existência de relação de causalidade entre a conduta do acusado e a morte do mergulhador, à luz da teoria da imputação objetiva, seria necessária a demonstração da criação pelo paciente de uma situação de risco não permitido, não-ocorrente, na hipótese. 7. Com efeito, não há como asseverar, de forma efetiva, que engenheiro tenha contribuído de alguma forma para aumentar o risco já existente (permitido) ou estabelecido situação que ultrapasse os limites para os quais tal risco seria juridicamente tolerado.** 8. Habeas corpus concedido para trancar a ação penal, por atipicidade da conduta. (HC n. 68.871/PR, relatora Ministra Maria Thereza de Assis Moura, relator para acórdão Ministro Og Fernandes, Sexta Turma, julgado em 6/8/2009, DJe de 5/10/2009.)

Antes disso, em 2007, a Quinta Turma do Superior Tribunal de Justiça já havia decidido no Recurso Especial nº 822.517/DF[97], sob Relatoria do Ministro

---

[97] CRIMINAL. RESP. DELITO DE TRÂNSITO. RESPONSABILIDADE PENAL. DELITO CULPOSO. RISCO PERMITIDO. NÃO OCORRÊNCIA. IMPUTABILIDADE OBJETIVA. MATÉRIA FÁTICO-PROBATÓRIA. SÚMULA 07/STJ. INCIDÊNCIA. PENA PECUNIÁRIA SUBSTITUTIVA. AUSÊNCIA DE CORRESPONDÊNCIA COM A PENA SUBSTITUÍDA. RECURSO PARCIALMENTE CONHECIDO E DESPROVIDO. **I. De acordo com a Teoria Geral da Imputação Objetiva o resultado não pode ser imputado ao agente quando decorrer da prática de um risco permitido ou de uma ação que visa a diminuir um risco não permitido; o risco permitido não realize o resultado concreto; e o resultado se encontre fora da esfera de proteção da norma. II. O risco permitido deve ser verificado dentro das regras do ordenamento social, para o qual existe uma carga de tolerância genérica. É o risco inerente ao convívio social e, portanto, tolerável. III. Hipótese em que o agente agiu em desconformidade com as regras de trânsito (criou um risco não permitido), causando resultado jurídico abrangido pelo fim de proteção da norma de cuidado - morte da vítima, atraindo a incidência da imputabilidade objetiva. IV. As circunstâncias que envolvem o**

Gilson Dipp, sobre a aplicabilidade da teoria da imputação objetiva, quando decidiu que, de acordo com ela, o resultado não pode ser imputado ao agente quando decorrer da prática de um risco autorizado ou de ação que diminua o risco não permitido; quando o risco não se realiza no resultado concreto ou quando o resultado está fora da zona de proteção da norma. No caso concreto, o réu teria agido em desconformidade com as regras de trânsito e, em razão disso, causado o resultado morte de outrem, portanto, havia criado um risco não permitido que se realizou no resultado abrangido pela norma.

No HC nº 46.525/MT, julgado aos 21.03.2006, também pela Quinta Turma do e. Superior Tribunal de Justiça, sob a relatoria do Ministro Arnaldo Esteves Lima, enfrentou-se, na análise do tipo objetivo, a criação de um risco não permitido, com base na teoria da imputação objetiva, para fins de reconhecer a atipicidade da conduta. A saber:

> PROCESSUAL PENAL. HABEAS CORPUS. HOMICÍDIO CULPOSO. MORTE POR AFOGAMENTO NA PISCINA. COMISSÃO DE FORMATURA. INÉPCIA DA DENÚNCIA. ACUSAÇÃO GENÉRICA. AUSÊNCIA DE PREVISIBILIDADE, DE NEXO DE CAUSALIDADE E DA CRIAÇÃO DE UM RISCO NÃO PERMITIDO. PRINCÍPIO DA CONFIANÇA. TRANCAMENTO DA AÇÃO PENAL. ATIPICIDADE DA CONDUTA. ORDEM CONCEDIDA. 1. Afirmar na denúncia que "a vítima foi jogada dentro da piscina por seus colegas, assim como tantos outros que estavam presentes, ocasionando seu óbito" não atende satisfatoriamente aos requisitos do art. 41 do Código de Processo Penal, uma vez que, segundo o referido dispositivo legal, "A denúncia ou queixa conterá a exposição do fato criminoso, com todas as suas circunstâncias, a qualificação do acusado ou esclarecimentos pelos quais se

---

fato em si não podem ser utilizadas para atrair a incidência da teoria do risco permitido e afastar a imputabilidade objetiva, se as condições de sua aplicação encontram-se presentes, isto é, se o agente agiu em desconformidade com as regras de trânsito, causando resultado jurídico que a norma visava coibir com sua original previsão. V. O fato de transitar às 3 horas da madrugada e em via deserta não pode servir de justificativa à atuação do agente em desconformidade com a legislação de trânsito. Isto não é risco permitido, mas atuação proibida. VI. Impossível se considerar a hipótese de aplicação da teoria do risco permitido com atribuição do resultado danoso ao acaso, seja pelo fato do agente transitar embriagado e em velocidade acima da permitida na via, seja pelo que restou entendido pela Corte a quo no sentido de sua direção descuidada. VII. A averiguação do nexo causal entre a conduta do réu, assim como da vítima, que não teria feito uso do cinto de segurança, com o resultado final, escapa à via especial, diante do óbice da Súmula 07 desta Corte se, nas instâncias ordinárias, ficou demonstrado que, por sua conduta, o agente, em violação ao Código de Trânsito, causou resultado abrangido pelo fim de proteção da norma de cuidado. VIII. Não há simetria entre a pena pecuniária substitutiva e a quantidade da pena privativa de liberdade substituída. IX. Recurso parcialmente conhecido e desprovido. (REsp n. 822.517/DF, relator Ministro Gilson Dipp, Quinta Turma, julgado em 12/6/2007, DJ de 29/6/2007)

> possa identificá-lo, a classificação do crime e, quando necessário, o rol das testemunhas". 2. Mesmo que se admita certo abrandamento no tocante ao rigor da individualização das condutas, quando se trata de delito de autoria coletiva, não existe respaldo jurisprudencial para uma acusação genérica, que impeça o exercício da ampla defesa, por não demonstrar qual a conduta tida por delituosa, considerando que nenhum dos membros da referida comissão foi apontado na peça acusatória como sendo pessoa que jogou a vítima na piscina. 3. Por outro lado, narrando a denúncia que a vítima afogou-se em virtude da ingestão de substâncias psicotrópicas, o que caracteriza uma autocolocação em risco, excludente da responsabilidade criminal, ausente o nexo causal. **4. Ainda que se admita a existência de relação de causalidade entre a conduta dos acusados e a morte da vítima, à luz da teoria da imputação objetiva, necessária é a demonstração da criação pelos agentes de uma situação de risco não permitido, não-ocorrente, na hipótese, porquanto é inviável exigir de uma Comissão de Formatura um rigor na fiscalização das substâncias ingeridas por todos os participantes de uma festa.** 5. Associada à teoria da imputação objetiva, sustenta a doutrina que vigora o princípio da confiança, as pessoas se comportarão em conformidade com o direito, o que não ocorreu in casu, pois a vítima veio a afogar-se, segundo a denúncia, em virtude de ter ingerido substâncias psicotrópicas, comportando-se, portanto, de forma contrária aos padrões esperados, afastando, assim, a responsabilidade dos pacientes, diante da inexistência de previsibilidade do resultado, acarretando a atipicidade da conduta.6. Ordem concedida para trancar a ação penal, por atipicidade da conduta, em razão da ausência de previsibilidade, de nexo de causalidade e de criação de um risco não permitido, em relação a todos os denunciados, por força do disposto no art. 580 do Código de Processo Penal. (HC n. 46.525/MT, relator Ministro Arnaldo Esteves Lima, Quinta Turma, julgado em 21/3/2006, DJ de 10/4/2006, p. 245.)

Portanto, verifica-se que a teoria da imputação objetiva, sob a análise do risco, é amplamente admitida na jurisprudência nacional e parece ser adequada a resolução dos problemas de tipicidade relacionados às violações a bens jurídicos decorrentes de sistemas autônomos quando ocorrer pratica delituosa comissiva ou omissa, dolosa ou culposa, como será analisado.

8. O INJUSTO DOS DELITOS COMISSIVOS DOLOSOS

Os tipos comissivos dolosos são formados, basicamente, por ação e objeto, sendo objeto a pessoa ou coisa sobre a qual recai a conduta do agente (ação). Além disso integram o tipo: o resultado, o nexo de causalidade, os critérios de imputação e o aspecto subjetivo. Com isso podemos separar o injusto em dois grandes grupos: o tipo objetivo e o tipo subjetivo. (TAVARES, 2018a).

O tipo objetivo é formado por elementos descritivos e normativos enquanto o tipo subjetivo está relacionado ao aspecto intrínseco do sujeito, vinculados à vontade, intenção, direcionamento dos meios causais, etc. (TAVARES, 2018a).

A partir da verificação do nexo de causalidade e dos critérios de imputação (objetiva), para além dos requisitos objetivos, é necessário à configuração do crime doloso a análise do elemento subjetivo, inclusive para fins de restringir o conceito causal. (ANDERSON DE SOUZA, 2022)

O elemento subjetivo geral dos tipos dolosos é dolo. “O tipo subjetivo volta-se ao vínculo psicológico do agente com relação ao comportamento delitivo” (ANDERSON DE SOUZA, 2022)

O tipo então é integrado por um elemento geral, que é o dolo, e as vezes, por elementos especiais (ANDERSON DE SOUZA, 2022). “O estudo do tipo objetivo dos crimes dolosos tem por objeto o dolo (elemento subjetivo geral), e as intenções, tendências ou atitudes pessoais (elementos subjetivos especiais) ...” (CIRINO DOS SANTOS, 2017).

Dolo é entendido majoritariamente como a vontade consciente de realizar o resultado típico. Portanto, é entendido comumente como *consciência* e *vontade*, possuindo assim “dois elementos, um intelectivo, outro volitivo” (ANDERSON DE SOUZA, 2022).

Em contrapartida, respeitável porção da doutrina[98] entende dolo apenas como conhecimento, porquanto é o conhecimento (consciência) que traz domínio e é ao domínio que deve ser direcionada a resposta estatal que é dada ao dolo (GRECO).

Em âmbito nacional existem espécies de dolo, sendo dolo direto (consciência e vontade) e eventual (assunção de risco), conforme art. 18, I, do Código Penal.

De toda forma, no que diz respeito aos crimes dolosos, caso superada a configuração do tipo sob o aspecto objetivo, não aparenta haver grandes dificuldades ao direito penal brasileiro para responsabilização a partir de violação a bens jurídicos por máquinas quando alguém conscientemente as utilize como instrumentos. Tratar-se-ia de autoria imediata dolosa:

> Não há problemas para estabelecer a responsabilidade penal de um fornecedor quando ele pretende ou conscientemente programa um agente inteligente de forma a que este cause resultados penalmente relevantes: se um comandante militar conscientemente emprega um drone para matar civis, ou um carro autônomo é dolosamente programado para atropelar ciclistas que estejam na pista de carros, então não temos qualquer dificuldade em identificar o comandante e o fornecedor (em sentido amplo) do carro como causadores das consequências danosas e fazê-los penalmente responsáveis por isso, porque eles se serviram de um agente inteligente tal qual um homem se serve de uma ferramenta ou de um outro instrumento para realizar seus planos. Trata-se de um caso de autoria imediata dolosa de uma pessoa que controla a máquina de acordo com sua vontade. (GLESS; WEIGEND, 2019)

No máximo ocorreria um crime de autoria mediata, caso houvesse um terceiro envolvido, e na circunstância dessa outra pessoa operar o sistema sem tal conhecimento.

> A autoria mediata define a realização do tipo de injusto com o domínio da vontade de outrem, utilizado como instrumento, que realiza o fato em posição subordinada ao controle do autor. Logo, não existe autoria mediata: a) se o terceiro não é instrumento nas mãos do autor mediato, mas (co)autor plenamente responsável; b) nos tipos especiais próprios, que exigem autores com qualificação especial; c) nos tipos de mão própria, que exigem realização corporal da ação típica pelo autor; d) nos tipos de imprudência, por ausência

[98] Para saber mais: VIANA, Eduardo. Dolo como compromisso cognitivo. São Paulo: Marcial Pons, 2017.

> de vontade construtora do acontecimento - e, portanto, por ausência de domínio do fato. (CIRINO DOS SANTOS, 2017)

Portanto, os delitos dolosos não apresentam grande dificuldade à equação, tal como reconheceu a Prof. Dra. Heloisa Estellita (2020) no referido Relatório Final da Comissão de Inteligência Artificial apresentado ao Congresso Nacional:

> No âmbito de uma responsabilidade por ação dolosa (…), o Direito Penal atual não tem muito problema para responder. Todas as contribuições são puníveis, todos que conheciam que aquilo ia causar dano e puseram isso em ação são puníveis também; eles sabiam que iam causar danos ou contavam com a possibilidade ou com a alta probabilidade de causação de danos (...)

Ou seja, desde que superado o preenchimento dos requisitos objetivos do tipo, qualquer pessoa dentro da cadeia de desenvolvimento dos sistemas autônomos (e inclusive os usuários) poderá responder por delito doloso praticado utilizando uma máquina, desde que esteja demonstrado também o conhecimento necessário de que aquela conduta causaria dano, ou ao menos a assunção do risco, na forma do art. 18, I do Código Penal.

Mas o cenário comum para esses casos não indica ser esse. A dificuldade se evidencia para os casos de falha técnica, em que a máquina foi programada para agir de determinada maneira, como, por exemplo, um veículo autônomo que foi programado para frear para um pedestre, mas não o faz.

Ou ainda mais grave, nos casos de sistema autônomo dotado de autoaprendizagem que, apesar da máquina agir da forma inicialmente prevista, tal como foi programada, ou seja, sem que haja defeito, inconsistência etc, gerar danos aos seres humanos em razão de uma eventual informação equivocada (que se tornou *dirty data*) que recebeu e aprendeu ou, ainda, decorrente de uma cadeia inesperada de acontecimentos.

Nesses casos de falhas técnicas e de decisão decorrente de autonomia dos robôs estar-se-á, aparentemente, de frente a tipos culposos.

> Um outro aspecto relevante diz respeito ao título da imputação subjetiva. Como registram Gless/Weigend, a forma por excelência imputação da responsabilidade penal oriunda da introdução desses sistemas autônomos e híbridos seria a culposa. Isso se deve ao fato de que entre as pessoas naturais por trás do robô e o resultado típico se interpõe justamente um sistema caracterizado por sua autonomia, o que impediria, normalmente, a configuração do conhecimento necessário do risco de superveniência do resultado danoso, conhecimento essencial à configuração do dolo. (ESTELLITA, LEITE, 2019, p. 32)

Isso traz uma dificuldade muito própria, já que a responsabilidade na modalidade culposa é, como regra, exceção. Tendo como exemplo os casos já citados no presente trabalho, o delito de homicídio ou lesão corporal admitiriam, no Brasil, modalidade culposa, mas racismo e injúria racial, não.

> Não há responsabilidade pelo risco no direito penal, que sempre pressupõe culpabilidade. Os juristas continentais falam no chamado princípio da culpabilidade (Baumann et al. 2016, $ 16 nm. 1 s.; Hilgendorf e Valerius 2015, § 1 nm. 36 s.). Isso significa que uma pena só pode ser imposta se o modelo de culpa clássico estiver satisfeito: o autor executa uma ação que causa um dano e age dolosa ou, pelo menos, culposamente. Note-se que na maioria dos sistemas de direito penal, incluindo o alemão, a atuação a título de culpa é punível apenas em casos excepcionais. (HILGENDORF, 2020, p. 156)

Ainda, no restrito campo dos delitos culposos, diversos requisitos precisariam estar presentes para poder afirmar responsabilidade penal de algum dos participantes da cadeia de desenvolvimento destas máquinas. Isso porque os crimes culposos têm como núcleo uma ação descuidada, motivo por que faz-se necessário ao presente estudo abordar tal ideia, porquanto torna-se relevante entender onde tais condutas estão localizadas, como aponta SILVA SANCHEZ:

> Isto é, as consequências lesivas da “falha técnica”, que aparecem como um problema central nesse modelo, no qual se parte de que certo porcentual de acidentes graves resulta inevitável à vista da complexidade dos desenhos técnicos. Assim, se trata de decidir, entre outras coisas, a questão crucial dos critérios de localização das “falhas técnicas”, ou no âmbito do risco penalmente relevante, ou no âmbito do próprio risco permitido. (SANCHEZ, 2013)

8.1. O INJUSTO DOS DELITOS CULPOSOS

Como visto, por excelência os crimes relacionados aos sistemas autônomos são culposos, motivo porque o injusto nessa modalidade demanda enfrentamento.

> Mais frequentes deveriam ser os casos nos quais a introdução de um agente inteligente conduz a um dano indesejado: o drone que, em conformidade com o desejo de seu fornecedor, devesse apenas atingir os alvos militares pré-determinados, desvia-se, por erro de funcionamento, do alvo militar original e mata civis; um carro autônomo, que só deveria seguir sua rota em conformidade com as regras de trânsito, viola essas regras e fere um ciclista em um cruzamento. (GLESS; WEIGEND, 2019)

O crime culposo se estrutura a partir de critérios normativos (ANDERSON DE SOUZA). A imputação depende, no tipo culposo, que a ação (ou omissão) exceda “os limites dos riscos autorizados na relação jurídico-social e com isso vem a lesar ou a pôr em perigo um bem jurídico-penalmente relevante” (TAVARES, 2018b)

> A culpa, no sentido de negligência, ou crime culposo, constitui uma criação da ordem jurídica. Não há crime culposo em sentido natural. O crime culposo decorre de um processo de imputação que tem por fundamento a realização de uma conduta que exceda os limites do risco autorizado e se veja assinalada como penalmente relevante em um tipo de delito. (TAVARES, 2018b)

> A base da estrutura do delito culposo, portanto, não se situa no conceito de conduta, mas na forma e no modo de sua imputação, quer dizer, a relevância penal de uma conduta para caracterizá-la como culposa irá de pender menos de sua configuração natural e muito mais dos requisitos que a norma jurídica lhe empreste. **Somente por meio da norma que fixe os limites do risco autorizado ou desautorizado, portanto, que assinale os contornos do lícito e do ilícito, será possível afirmar-se que a conduta realizada conduz à produção de um resultado danoso, juridicamente relevante, em face de haver lesado ou posto em perigo um bem jurídico**. (TAVARES, 2018b)

No que tange aos crimes culposos estes apenas existem a partir dos tipos dolosos, e enquanto preveem normas proibitivas, os últimos preveem normas mandamentais (TAVARES, 2018b).

Um delito apenas pode ser considerado culposo se o tipo penal assim prever a possibilidade. Quando não estiver expressamente previsto, o crime apenas poderá ocorrer na modalidade dolosa, conforme está disposto no parágrafo único do art. 18 do Código Penal (CALLEGARI, 2014)

O delito culposo, enquanto construção normativa, tem suas especificidades. A ação terá duas características: a conduta voluntária e a conduta descuidada violadora do risco autorizado. (TAVARES, 2018b) Ainda, haverá nexo causal no delito culposo quando se puder afirmar (i) a previsibilidade, ou seja, que o resultado a partir daquela conduta era previsível; (ii) resultado como consequência de uma violação de dever de cuidado e (iii) que a "relação de causalidade deve ser penalmente relevante ou típica, comprovando-se que o evento produzido está contemplado como resultado que a norma de cuidado busca evitar" (ANDERSON DE SOUZA, 2022).

Esses critérios adotados pela teoria da imputação objetiva são "limitadores da própria causalidade, na forma de fatores que se desenvolvem de sua explicação teórica" (TAVARES, 2018b), de maneira que ao presente tópico, no que se refere à configuração dos tipos culposos, resta verificar três critérios, sendo eles: a) previsibilidade; b) evitabilidade e c) critérios relacionados ao aumento do risco e sua realização no resultado (TAVARES, 2018b)

A previsibilidade é limitadora da imputação, de forma que o delito culposo somente será imputado a alguém se o resultado era previsível. Portanto, apenas será atribuída responsabilidade culposa "do fornecedor quando o resultado tipicamente relevante fosse previsível e não tenha ele empregado os deveres de cuidado devido para evitar tal resultado" (GLESS; WEIGEND, 2019, p. 54)

O que, relacionado aos sistemas autônomos com autoaprendizagem pode representar uma dificuldade porque infinitas são as possibilidades de situação concretas da vida a partir do que os sistemas podem aprender:

> ...no âmbito da produção e fornecimento de agentes inteligentes, a previsibilidade da ocorrência do resultado, como elemento da conduta culposa, apresenta dificuldades. Os agentes inteligentes avaliam autonomamente as informações tomadas do seu entorno e reagem ao produto dessa avaliação sem uma influência humana, de forma a cumprir de forma ótima a missão que lhes foi assignada. Mesmo quando o fornecedor observe permanentemente as (re)ações de um de um agente inteligente complexo, não pode prever em detalhes qual padrão o robô reconhecerá nos dados coletados, como os interpretará e como reagirá. Disso decorre, ainda, que, em tais sistemas abertos, as regras de decisão pré-estabelecidas serão normalmente lacunosas, uma vez que nem todas as situações da vida podem ser previstas e traduzidas por um algoritmo em um determinado comportamento e, finalmente, porque o sistema, durante sua própria execução, aprende de forma autônoma. Isso quer dizer que uma certa imprevisibilidade dos agentes inteligentes e o correlato risco para terceiros é como que "pré-programada". Pode suceder, por exemplo, que um carro autônomo não consiga "ler" corretamente uma placa de trânsito levemente suja que indique o dever de dar preferência e, com isso, não dê preferência a um ciclista, ferindo-o. (GLESS; WEIGEND, 2019)

Mas a previsibilidade, sozinha, não preenche o tipo culposo. Há um certo consenso na doutrina[99] de que para a configuração dos tipos culposos a imputação terá como base a relação entre uma lesão de um dever de cuidado e o resultado alcançado por essa conduta. (TAVARES, 2018b)

Em resumo, para a imputação no injusto culposo há de ocorrer uma infração de uma norma de cuidado (necessário agir descuidado do sujeito em face do objeto). A partir disso é necessário verificar, para fins de imputação, se o resultado alcançado poderia ser evitado caso a conduta, adequada ao caso concreto, tivesse se dado conforme o cuidado devido. Se o resultado não pudesse ser evitado mesmo com a prática da conduta devida a lesão ao dever de cuidado seria irrelevante. (TAVARES, 2018b).

Então, o critério da evitabilidade do resultado pretende responder a pergunta: o resultado do delito era evitável? Se a resposta é não, deve ser

[99] Para aprofundamento no tema ver: TAVARES, Juarez. Teoria do Crime Culposo, 5ª ed. São Paulo: Tirant lo Blanch, 2018

afastada a imputação em face do agente. Ou seja, se o agente agir de forma cuidadosa em face do bem jurídico e o resultado for alcançado de toda forma, não deve ele ser responsabilizado (TAVARES, 2018b).

No que tange aos critérios relacionados ao aumento do risco (a partir da contribuição de ROXIN) e sua realização no resultado, estes servem a *"*estabelecer as exatas linhas divisórias entre o lícito e o ilícito" (TAVARES, 2018a) e podem ser subdivididos em a) criação ou incremento do risco não permitido; b) realização do risco não permitido e c) alcance do tipo pelo resultado.

> Dogmaticamente, a teoria do risco assevera que o tipo do delito culposo só estará configurado quando a conduta ultrapassar os limites do risco autorizado e o resultado constituir a concretização desse comportamento desautorizado. Ao ultrapassar os limites do risco autorizado, a conduta implicou por seu turno, um perigo relevante ao bem jurídico e, pois, um aumento do risco da ocorrência do resultado. Quer dizer, então, que haverá imputação quando a conduta implicou um aumento do risco da ocorrência do resultado e quando este resultado constituir, concretamente, a realização material daquele risco não autorizado. (TAVARES, 2018b)

A exceção são os casos em que apesar de ocorrer uma conduta perigosa, essa não representa um aumento do um risco não autorizado. Isso ocorrerá quando a conduta diminuir o risco do resultado, quando não representar, por si, um aumento do risco para o resultado, quando a conduta arriscada não se concretizar no resultado e quando a conduta não se inclui no âmbito do tipo delitivo (TAVARES, 2018b).[100]

8.2. DOS DELITOS OMISSIVOS (IMPRÓPRIOS)

Nessa oportunidade o presente trabalho se ocupará a mencionar as questões acerca da omissão imprópria, prevista no Código Penal brasileiro no art. 13, §2º, que como regra, equipara omissões à conduta causadora do resultado lesivo que ofende o bem jurídico protegido (SCHIETTI CRUZ; SANTOS; ORTIZ, 2022)

---

[100] Para aprofundamento no tema ver: TAVARES, Juarez. Teoria do Crime Culposo, 5ª ed. São Paulo: Tirant lo Blanch, 2018

Nos delitos de omissão imprópria a imputação decorre de um dever de garantia direcionado a pessoas determinadas que têm como dever de evitar o resultado lesivo (BOTTINI, 2018).

> Diante da dificuldade de imputar resultados à omissão pelo prisma causal e dos limites e problemas ligados à teoria dos deveres formais, a doutrina partiu em busca de critérios materiais para construir um dever de garante, um dever de proteção/salvamento capaz de imputar ao omitente o resultado típico de forma equiparada à ação. (BOTTINI, 2018)

Então, omitir é voluntariamente não realizar algo que seria possível. No aspecto jurídico-penal, esse “algo” seria, em verdade, a atitude esperada daquele sujeito, que é o que se convencionou chamar de omissão relevante ou omissão socialmente relevante. (BOTTINI, 2018)

Quem tem o dever de garantia, resumidamente, são aqueles sujeitos que detêm uma condição especial, decorrente de determinada “situação específica ou uma posição jurídica que faz surgir o dever de evitar o resultado”. (BOTTINI, 2018)

Assim, é garante/garantidor quem tem o “dever de atuar como meio de proteção de bens jurídicos ameaçados” (ESTELLITA, 2017), de maneira que o tipo omissivo impróprio estará configurado com o alcance do resultado lesivo pelo “desatendimento a esse dever por meio da falta de prática da ação legalmente devida.” (ESTELLITA, 2017).

O que justifica a posição de garantidor de alguém é a “assunção fática de uma fonte de perigo ou da proteção de um bem jurídico” (ESTELLITA, 2017). Essas posições podem ser subdividias em garantidores de proteção de bem jurídico e garantidores de vigilância sobre as fontes de perigo, podendo esses deveres serem cumulados (ESTELLITA, 2017).

Os garantidores de proteção de bem jurídico tem que preservar e resguardar o bem protegido dos perigos externos, enquanto que o fundamento

da posição dos garantidores de vigilância surge da liberalidade, fazendo com ela contraponto (ESTELLITA, 2017). “É a criação da fonte de perigo que legitima a exigência de que seja mantida dentro do patamares permitidos ou de que, extrapolando-os, seja reconduzida a estes patamares.” (ESTELLITA, 2017).

Para Heloísa Estellita[101], a posição de garantidor por ingerência para os crimes praticados no âmbito empresarial não demonstra ser adequada para abarcar todos os casos passíveis de ocorrer (penalmente relevantes), motivo por que entende que o fundamento que justifica a posição de garante nesse cenário empresarial é entender a estrutura empresarial como fonte de perigo permitida de forma que essa atrai, para si, o dever de controlar riscos e agir para evitar resultados:

> A análise da responsabilidade omissiva imprópria de dirigentes por crimes praticados a partir da empresa contra bens jurídicos de terceiros ou da coletividade se coloca no âmbito da análise da constituição de posições de garantia de vigilância oriundas da criação de uma fonte de perigo ou da assunção, total ou parcial dessa vigilância. [...] A fundamentação da posição de garantidor por ingerência parece ser insuficiente para contemplar todas as constelações de casos penalmente relevantes diante do costumeiro distanciamento temporal e pessoal entre a criação do perigo e a realização do resultado nos crimes econômicos. O fundamento que melhor parece se ajustar à estrutura de gestão de pessoas e objetos nas empresas é o que a considera como fonte de perigo permitida, criada no âmbito da liberdade de empreender, e que atrai para si, como contrapartida, o dever de controlar os riscos e agir para evitar resultados. A posição de garantidor de seus dirigentes individualmente considerados se funda no controle sobre essa fonte de perigo. Os perigos podem ser intrínsecos às atividades desenvolvidas pela empresa ou resultar de atos de organização e gestão dos administradores, pois a própria coordenação de tarefas na empresa é, em si, um fator de risco. Nas atividades econômicas desenvolvidas no contexto de sociedades empresárias, constituídas na forma de pessoas jurídicas, o risco da atividade empresarial é assumido primeiramente por esta. A pessoa jurídica atua por meio de pessoas naturais que gerem seu patrimônio e representam seus interesses nas atividades econômicas e praticam os atos de organização, gestão de funções e tarefas (departamentalização e delegação) para o atingimento de seu objetivo social. Sobre essas pessoas naturais recairão os encargos de vigilância relativos às atividades intrinsecamente perigosas da empresa e, ainda, aqueles oriundos de departamentalização e delegação. Serão garantidores originários na empresa aquelas pessoas que tenham uma relação juridicamente fundada de controle sobre a fonte de perigo empresa, confirmada pela assunção fática dessas tarefas. Essa relação dá origem ao dever especial de vigiar pessoas (um dever de garantidor). A mera

[101] Para saber mais, ver: ESTELLITA, Heloísa. Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas , limitadas e encarregados de cumprimento por crimes praticados por membros de empresa – 1. ed. – São Paulo: Marcial Pons, 2017.

> designação nos documentos sociais ou no organograma da companhia será irrelevante se não corresponder ao seu exercício fático. Para que se possa aproximar o máximo possível da concreção das posições de garantidores e de seus respectivos deveres sem abrir mão de algum grau de generalidade, é necessário partir da hipótese de que as pessoas que ocupam os cargos na empresa efetivamente desempenham as funções a eles atreladas. (ESTELLITA, 2017).

Sendo a estrutura empresarial considerada fonte de perigo permitida, que traz, em si, o dever de controlar os riscos e agir para evitar resultados, a posição de garantidor de seus dirigentes se fundamenta no controle sobre essa fonte de perigo (relacionados diretamente à atividade ou à gestão empresarial). Enquanto que, às demais pessoas físicas envolvidas nas atividades, incidirão as obrigações e deveres de vigilância relacionados às atividades perigosas da empresa como, ainda, os decorrentes de distribuição de responsabilidade e delegação. (ESTELLITA, 2017)

Isso é relevante ao presente estudo porquanto as pessoas naturais envolvidas no processo de criação de sistemas autônomos apenas poderão responder por uma conduta omissiva penalmente relevante se estiverem, concretamente, na posição de garantidor, diante de seu dever de vigilância relacionado ao desenvolvimento da atividade perigosa.

Para Pierpaolo Bottini[102], a ingerência, prevista no §2º, do art. 13, do Código Penal fundamenta parte da responsabilidade do empresário, mas não afasta outras posições de garante possíveis:

> A nosso ver valem aqui algumas considerações. Em primeiro lugar, reconhecer que a ingerência (CP, art. 13, §2.º, c) fundamenta parte da responsabilidade do empresário não significa afastar outras fontes de posição de garante, como aquelas decorrentes da lei (alínea a) ou da assunção (aliena b). Em uma série de situações nas quais não existe criação de risco próprio pelo empresário será ainda possível a imputação por omissão, desde que exista um *dever de garante* previsto em lei ou adquirido por assunção, que o obrigue a gerenciar riscos alheios. Em segundo lugar, identificar a ingerência como uma das fontes da posição de garantia do empresário não significa expandir em demasia sua responsabilidade penal. Basta que a imputação respeite os critérios de limitação de responsabilidade aos desdobramentos do risco não permitido, como a seguir proposto. Em síntese,

[102] Para saber mais, ver: BOTTINI, Pierpaolo Cruz. Crimes de omissão imprópria. 1ª ed. – São Paulo: Marcial Pons, 2018

> sempre que um membro da organização empresarial *criar um risco* - isolado ou cumulativo com outros integrantes da corporação - tem o dever de observar as *normas de cuidado* para manter esse *risco dentro do permitido*, gerindo corretamente seu âmbito de competência organizacional. O descumprimento das *normas de cuidado* que transforme o *risco* em não permitido e cause um resultado típico permite a atribuição da responsabilidade penal a título de *ingerência* (CP, art. 13, § 2.°, c), sem que seja necessária a identificação de qualquer ato de assunção ou dever legal. (BOTTINI, 2018)

Entende ainda BOTTINI que, no âmbito empresarial, às pessoas que têm deveres de controlar e gerenciar riscos alheios, o resultado não deve ser imputado por ingerência, mas, sim, pela existência de um dever de garante específico, que seja previsto em lei ou adquirido por assunção, conforme previsão do art. 13, a e b do CP:

> Ao lado da responsabilidade por riscos próprios, também na seara empresarial é possível identificar pessoas com atribuições de controlar ou gerenciar riscos alheios. Nesse caso, o foco não é o perigo por eles criado, mas aquele oriundo de outras pessoas ou setores, diante dos quais existe um dever de agir, seja para mantê-los dentro dos limites permitidos, seja para iniciar um processo de salvamento caso saiam do controle.

Aduz, portanto, que é mais adequado fundamentar a responsabilidade do "empresário" da seguinte forma:

> Assim, mais adequado fundar a responsabilidade do empresário em dois pilares: (i) quando cria um risco próprio, se sustenta nas faculdades individuais de auto organização, que impõem deveres de cuidado positivos e negativos cujo descumprimento enseja a responsabilidade por comissão ou omissão (CP. art. 13, § 2.°, c); e (i) quando está diante de um risco alheio, a posição de garante deriva da lei ou da assunção (CP, art. 13, § 2.°, a e b) [...] A identificação, no contexto empresarial, de quando a omissão se dá diante de um risco próprio ou alheio tem significativo interesse prático. A uma porque, como já exposto, revela o desvalor da omissão, sendo, a nosso ver, maior a gravidade da omissão diante de um risco próprio do que de um risco alheio. A duas porque tal distinção auxilia na identificação do tipo penal aplicável, incidindo diretamente o dispositivo nos casos de riscos próprios e exigindo-se o recurso a uma cláusula geral nas hipóteses de riscos alheios. Por fim, facilita a fundamentação da responsabilidade do empresário, uma vez que nos riscos próprios ela advém do risco criado e da subsequente ou concomitante violação de um *dever de cuidado*. Nos *riscos alheios* tal responsabilidade deve derivar de uma previsão legal expressa que indique um *dever de garantia* atribuído àquela pessoa - ou àquela categoria de pessoas - estabelecida em um dispositivo expresso do ordenamento penal.

> Assim, o empresário que cria um *risco não permitido* e omite controlá-lo (*risco próprio*) realiza um ato mais grave do que aquele membro da companhia que tinha o dever de gerenciá-lo e não o fez (risco alheio). Ademais, a responsabilidade penal pela produção de eventual resultado típico do primeiro prescinde da verificação da existência de um dever de garante específico previsto na lei ou decorrente de assunção, uma vez que a própria violação das normas de cuidado que caracteriza o risco não permitido torna o resultado imputável. Já no caso dos riscos alheios, a responsabilidade penal exigirá a identificação de um dever de garante por parte do omitente - previsto expressamente em lei ou decorrente de assunção - do contrário o ato será atípico ou se tratará de omissão própria. (BOTTINI, 2018)

Para a presente análise tal entendimento tem especial importância porque para a atribuição de responsabilidade penal por omissão a um dos membros da cadeia de desenvolvimento de sistemas autônomos (garante de risco alheio) exigir-se-ia, em tese, uma previsão legal expressa que indicasse o dever de garantia atribuído àquela categoria de pessoas, estabelecida em disposição legal no ordenamento jurídico.

De toda forma, como aponta Heloísa Estellita[103] a responsabilização omissiva imprópria é uma boa estratégia para manejar as problemáticas que surgem na tentativa de responsabilização penal individual no âmbito do contexto empresarial, o que pode ser transposto às dificuldades de responsabilização no desenvolvimento de sistemas autônomos (também em ambientes empresariais).

Por isso, nos casos dos robôs que mataram pessoas em fábricas por aparente violação de um dever de cuidado, a título de exemplo, seria possível se discutir a responsabilidade dos operadores das máquinas ou eventuais gerentes de áreas, tudo a depender do caso concreto e desde que verificadas suas posições de garante (riscos alheios), pois os delitos, nesse caso, seriam omissivos impróprios[104] (e culposos).

---

[103] Para saber mais, ver: ESTELLITA, Heloísa. Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas , limitadas e encarregados de cumprimento por crimes praticados por membros de empresa – 1. ed. – São Paulo: Marcial Pons, 2017.

[104] Para maiores informações ler: BOTTINI, Pierpaolo Cruz. Crimes de omissão imprópria. 1ª ed. – São Paulo: Marcial Pons, 2018

Da mesma forma, indica-se que poderá ser averiguada a responsabilidade de todos os demais envolvidos na cadeia de produção de sistemas autônomos, caso ocupem posição de garante.

Para tanto, tem-se por base esquema analítico apresentado (ESTELLITA, 2017) acerca dos pressupostos para configuração dos tipos omissivos:

1. Tipicidade
   1.1 Tipicidade objetiva
      1.1.1. Situação típica e resultado
      1.1.2. Posição de garantidor
      1.1.3. Omissão da conduta determinada e exigida de evitação do resultado, apesar da capacidade físico-real de fazê-lo
      1.1.4. Nexo de causalidade e imputação objetiva do resultado
   1.2 Tipicidade subjetiva
      1.2.1 Dolo
      1.2.2 (ou) Culpa (quando prevista)
2. Antijuridicidade
3. Culpabilidade (ESTELITTA, 2017)

8.3. DA ALTERNATIVA VIÁVEL

Há um risco concreto de lacuna de proteção a determinados bens jurídicos e, também, de dispersão de responsabilidade nos casos em que condutas penalmente relevantes sejam praticadas por máquinas com sistemas autônomos.

Isso porque, como a imputação criminal não pode se dar em face dos próprios robôs/máquinas, o processo de imputação será direcionado a um dos membros da cadeia de produção (desenvolvedores de softwares, engenheiros, programadores etc) e até usuários finais.

Há uma dificuldade inicial evidente de separar (no curso causal) as diversas condutas possíveis de terem gerado o resultado lesivo, porque essas podem estar situadas dentro do processo de criação, ou na implementação do software, na manutenção do sistema e até mesmo quando do uso (má utilização).

Além disso, via de regra, essas pessoas relacionadas à cadeia de produção estarão muito distantes da conduta delitiva, temporal e fisicamente.

Para tentar restringir essa dificuldade de responsabilização o caminho viável aparenta ser traçar, com brevidade e de forma concreta, as zonas do lícito e do ilícito da atividade por meio de sua regulamentação (por normas administrativas, técnicas e de compliance), como também, viabilizar eventual alteração legislativa para fins de previsão legal expressa (no ordenamento penal) que indique o dever de garantia atribuído a essa categoria de pessoas.

Certo que muitos são os desafios de regulamentação da atividade, especialmente diante da alta velocidade com que essas tecnologias surgem e se aprimoram, além da evidente dificuldade porque o tema “inteligência artificial” demanda específico *know-how* e, assim, é limitado o número de pessoas disponíveis a participar do debate público, muitas delas já vinculadas e/ou empregadas nas grandes empresas que devem ser reguladas.

Além do que, uma legislação muito restritiva pode vir a representar uma ameaça à inovação e com isso dificultar a criação de novas tecnologias.

Mas, o foco inicial precisa estar em minimizar os perigos causados à população pela inserção dos sistemas autônomos na vida em sociedade, o que aparenta ser possível pela via da regulamentação e do controle amplo da atividade, como vêm fazendo os regulamentos internacionais sobre inteligência artificial.

Apenas a partir dessa regulamentação concreta será possível começar a delimitar o que se insere no âmbito do risco permitido e o que se insere no risco não permitido. Diz-se começar a delimitar porque “muitas vezes, não basta atender às regras normais da profissão; será preciso ir mais além, caso o agente detenha um conhecimento especial que o faça antever que, com aquela forma de agir, irá acarretar um dano a outrem, o evento lhe será imputado. ” (TAVARES, 2018a)

De toda forma, a alternativa viável indica ser a de definir, de antemão, e de forma muito clara a todos os envolvidos na cadeia de produção quais são os riscos permitidos em matéria de desenvolvimento de inteligência artificial de sistemas autônomos, especialmente daqueles dotados de autoaprendizagem. Com isso, será possível obrigar, por exemplo, aos desenvolvedores e fornecedores que mantenham um controle regular do funcionamento das máquinas enquanto elas operem em sociedade, assim, tornar-se-ia mais fácil a indicação de quais os deveres de cuidado e a posição de garante desse grupo de pessoas e, assim, a responsabilização penal.

A partir da delimitação da zona do lícito e do ilícito, poderá ser responsabilizado quem, na cadeia de desenvolvimento, por sua conduta criar um risco não permitido, esse risco se realizar no resultado e esse resultado estiver dentro do tipo previsto, desde que preenchidos os demais requisitos objetivos (como o nexo de causalidade e para tipos omissivos esteja a pessoa na posição de garantidora e haja omissão da conduta determina e exigida de evitação do resultado, apesar da capacidade físico-real de fazê-lo) e, ainda, os requisitos subjetivos.

A regulamentação é essencial, inclusive, para que possa a sociedade desde logo enfrentar se está disposta a, eventualmente, dispensar determinados produtos[105] ou, ainda, no aspecto penal, renunciar à responsabilização criminal

[105] O ChatGPT, por exemplo, foi temporariamente banido na Itália. Outros países como França e Alemanha estudam o mesmo caminho. Disponível em: https://tecnoblog.net/noticias/2023/03/31/chatgpt-foi-banido-na-italia-e-esta-sendo-investigado-pelas-autoridades-do-pais/ Acesso em 20 de junho de 2023. Também disponível em: https://vpnoverview.com/pt/desbloqueando/a-censura/chatgpt-como-

individual (culposa) do homem “detrás” (criador, desenvolvedor e/ou fornecedor) aos casos relacionados às máquinas de sistemas autônomos com autoaprendizado, em prol de usufruir dos benefícios sociais gerado a partir delas (GLESS; WEIGEND, 2019).

> Uma outra variante da exclusão da imputação objetiva pode se dar quando a decisão "própria" do robô autônomo interrompa a relação de imputação entre a atividade do fornecedor e a ocorrência do resultado penalmente relevante. Essa não é uma possibilidade longínqua, caso se construa, por exemplo, a lesão corporal causada por um carro autônomo, de certa forma, não como um fato do construtor, mas do "próprio carro". Vimos acima (II.) que um sancionamento dos agentes inteligentes em conformidade com o "direito penal dos humanos" não é possível atualmente. Mas isso não significa, necessariamente, que a introdução de tecnologias autônomas seja irrelevante para a imputação do resultado ao homem por trás da máquina. Quando a conduta de um agente inteligente puder ser qualificada como a conduta de um "homem da frente", então a relação de imputação ao "homem de trás" (o fornecedor) poderá ser rompida. Todavia, não poderemos falar de um comportamento danoso do agente inteligente enquanto não lhe pudermos atribuir uma capacidade de formar vontade própria. Isto não é possível nos tempos atuais. Já sugerimos acima, porém, que uma tal atribuição não está descartada para o futuro relativamente a agentes inteligentes capazes de aprender e de ter memória. Mas mesmo quando se conseguir desenvolver seres antropomórficos, dever-se-ia ainda assim permitir o regresso da responsabilidade penal ao fornecedor que age culposamente enquanto os agentes inteligentes não possuírem capacidade de receber pena; é que, se não for assim, a vítima de um fato danoso estará na já mencionada situação insatisfatória de uma difusão da responsabilidade entre humanos e agentes inteligentes... (GLESS; WEIGEND, 2019)

---

acessar/#:~:text=Na%20verdade%2C%20ele%20est%C3%A1%20bloqueado,os%20dados%20de%20seus%20usu%C3%A1rios. Acesso em 20 de junho de 2023.

CONCLUSÃO

Com o avanço acelerado das tecnologias envolvendo inteligência artificial, as grandes nações, reconhecendo a relevância da matéria e os riscos implicados, têm enfrentado desafios para regulá-la de modo a preservar os direitos das pessoas e da sociedade, ao mesmo tempo em que torna viável e incentiva o seu desenvolvimento e implantação.

O direito, enquanto regulador das relações sociais, é chamado ao debate. O direito penal, objeto central do presente trabalho, é alcançado porquanto bens jurídicos tutelados mundialmente vêm sendo violados por máquinas com inteligência artificial, especialmente dotadas de sistemas autônomos e há, com o avanço rápido da tecnologia, previsão de que esse cenário se expanda.

Isso acende um alerta de perigo concreto de lacuna de proteção a determinados bens jurídicos e dispersão de responsabilidade, porque inexiste qualquer previsão legal de imputação aos próprios robôs/máquinas, especialmente no âmbito criminal, cuja teoria do delito é fundada no conceito de conduta praticada por pessoa humana.

Por outro lado, há enorme insegurança jurídica, pois, face aos casos concretos, atualmente se tem atribuído a responsabilização penal aos operadores das máquinas, ou seja, aos usuários finais - e, muitas vezes, consumidores - , a título de culpa, porque o usuário ainda tem a obrigação (dever de cuidado) de utilizar os produtos como se os sistemas não fossem autônomos.

Entretanto, em pouco tempo as máquinas agirão totalmente sozinhas, inclusive a partir de autoaprendizado. Como visto, tais sistemas já existem e estão disponíveis. A discussão que surge a partir disso é: quem – e de que modo - poderá ser responsabilizado, caso haja violação à bens jurídicos tutelados pelo direito penal brasileiro?

Necessário responder a essa pergunta, porque é fundamental trazer luz e segurança aos envolvidos na cadeia de produção dessas máquinas – como fabricantes, desenvolvedores de softwares, programadores, engenheiros e, até mesmo, usuários finais – sobre os riscos e implicações.

Motivo por que a alternativa viável ao cenário nacional parece ser, assim como os países desenvolvidos têm feito, a regulamentação específica da matéria pelo legislativo, no que tange à normas técnicas, administrativas e de compliance, a fim de estabelecer concretamente quais são as zonas do lícito e do ilícito no desenvolvimento da atividade.

A partir disso a imputação de responsabilidade penal a um sujeito pressuporá, inicialmente, a violação do risco permitido que se verifique no resultado.

Mas, ainda que estes regramentos específicos venham a existir num futuro próximo e pautem o debate do risco, o processo de imputação penal ainda poderá apresentar dificuldades.

Essas dificuldades não aparentam existir quanto aos tipos comissivos dolosos para fins de responsabilização do chamado homem “de trás”, pois nesses casos a máquina/robô seria usada apenas como instrumento.

Entretanto, o tipo dessas condutas, geralmente, é culposo, o qual é sempre excepcional e não abarca, ao menos até o presente momento, todas as violações a bens jurídicos possíveis por ausência de previsão legal, o que também poderá ser objeto de futuras alterações legislativas.

Para além da violação do risco, o tipo culposo demandará análise da violação do dever de cuidado, da previsibilidade e da evitabilidade, o que por certo representará uma dificuldade extra para imputação, principalmente em razão do distanciamento de tempo e espaço entre a conduta (por exemplo uma programação inicial de software) e o resultado lesivo (ofensa a bem jurídico). Como também, nos sistemas de autoaprendizagem, a previsibilidade pode ser

pulverizada por novos dados e informações e/ou cadeia inesperada de acontecimentos.

Além disso, os tipos dessas condutas também indicam ser omissivos, portanto, é possível que a sociedade brasileira, em um momento próximo, precise enfrentar a questão acerca de eventuais alterações legislativas também para prever no ordenamento penal o dever de garantia atribuído a essa categoria de pessoas (envolvidas na cadeia de desenvolvimento de tais tecnologias).

Por outro lado, é necessário cuidado para a criação de normativas e regramentos que regulem a matéria, a fim de que a "ameaça" de responsabilidade não leve a uma restrição do próprio desenvolvimento da tecnologia em âmbito nacional.

De toda forma, parece essencial que se defina, imediatamente, ao menos quais são os riscos permitidos em matéria de desenvolvimento de inteligência artificial de sistemas autônomos. Inclusive para que a sociedade possa enfrentar se está preparada para aceitar os riscos inerentes ao uso desses sistemas, especialmente os dotados de autoaprendizagem, porquanto inevitavelmente estará excluída a possibilidade de controle total pelos humanos.

Por fim, em certa medida, a sociedade ainda precisa enfrentar se dispensará a utilização de determinados produtos ou, eventualmente, pelo benefício de conviver com a tecnologia, se estará disposta a não responsabilizar criminalmente o sujeito humano participante da cadeia de desenvolvimento (criador, desenvolvedor e/ou fornecedor etc.) para os casos de condutas penalmente relevantes praticadas por máquinas com sistemas autônomos com autoaprendizado.

REFERÊNCIAS

5G: entenda a briga entre Estados Unidos e China. **G1**. São Paulo, 05 de maio de 2021. Disponível em: https://g1.globo.com/tecnologia/noticia/2021/11/05/5g-entenda-a-briga-entre-estados-unidos-e-china.ghtml Acesso em 28 de janeiro de 2023

ALMEIDA, Ursula Ribeiro de. A regulação da inteligência artificial no Brasil. **JOTA.** 21 de maio de 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-regulacao-da-inteligencia-artificial-no-brasil-21052022 Acesso em 11 de fevereiro de 2023

ANDERSON DE SOUZA, Luciano. Direito Penal. Parte Geral: Volume 1. 3ª ed. São Paulo: Thomson Reuters Brasil, 2022.

ATAYDE, Gisele Rodrigues; OTTONICAR, Selma Leticia Capinzaiki; SANTA-EULALIA, Luis Antonio de. O Big Data no desenvolvimento da indústria 4.0: novas perspectivas para o empreendedorismo acadêmico. *In:* org. MARTÍNEZ-ÁVILA, Daniel; ALVES DE SOUZA, Edna; QUILICI GONZALEZ, Maria Eunice. Informação, conhecimento, ação autônoma e big data: continuidade ou revolução? – Marília: Oficina Universitária; São Paulo: Cultura Acadêmica, 2019 [e-book]

BARBOSA, Andressa. 5 empresas que fazem delivery com drones e robôs. Forbes. 05 de janeiro de 2022. Disponível em: https://forbes.com.br/forbes-tech/2022/01/conheca-5-empresas-que-ja-utilizam-drones-e-robos-para-entregas/ Acesso aos 25 de janeiro de 2023

BARBOSA DE MIRANDA, Lorrayne; LANNES, Yuri Nathan da Costa;. SIQUEIRA NETO, José Francisco; Inteligência artificial e veículos autônomos: aspectos éticos, políticos e jurídicos. *In: Org.:* FABRI, Andrea Queiroz; NASCIMENTO, Carlos Eduardo do; CHIARELLO DE SOUZA PINTO, Felipe. Compliance and technology law. Uberlândia: Composer, 2020

BOTTINI, Pierpaolo Cruz. Crimes de omissão imprópria. 1ª ed. – São Paulo: Marcial Pons, 2018

CALLEGARI, André Luís. Teoria geral do delito e da imputação objetiva. 3 ed. rev. E ampl. – São Paulo: Atlas, 2014.

Case 3:22-cv-05240. Disponível em: <https://www.maricopacountyattorney.org/CivicAlerts.aspx?AID=751> Acesso em: 10 de fevereiro de 2023

CASTRO, Bernardo. Uber começa a utilizar carros autônomos a partir de 2022. **Uol.** 07 de outubro de 2022. Disponível em: https://autopapo.uol.com.br/curta/uber-comeca-a-utilizar-carros-autonomos-a-partir-de-2022/ Acesso aos 25 de janeiro de 2023

CAVA, Marco Della. Tesla announces fully self-driving cars. **USA Today.** São Francisco, 19 de outubro de 2016. Disponível em: https://www.usatoday.com/story/tech/news/2016/10/19/tesla-announces-fully-self-driving-fleet/92430638/ Acesso em 10 de fevereiro de 2023

CHATGPT. Disponível em: https://chat.apps.openai.com/auth/login Acesso em: 10 de fevereiro de 2023

CHATGPT Chat. Disponível em: https://chat.openai.com/chat Acesso em: 12 de fevereiro de 2023

ChatGPT: como acessar em países onde ele está bloqueado. **VPNoverview.** 10 de junho de 2023. Disponível em: https://vpnoverview.com/pt/desbloqueando/a-censura/chatgpt-como-acessar/#:~:text=Na%20verdade%2C%20ele%20est%C3%A1%20bloqueado,os%20dados%20de%20seus%20usu%C3%A1rios Acesso em 20 de junho de 2023

ChatGPT: Itália baniu a IA; saiba a situação em outros países, inclusive no Brasil. **Olhar Digital.** 05 de abril de 2023. Disponível em: https://olhardigital.com.br/2023/04/04/pro/chatgpt-italia-baniu-a-ia-saiba-a-situacao-em-outros-paises-inclusive-no-brasil/ Acesso em 20 de junho de 2023

ChatGPT 'passa' em prova de MBA, 'OAB' dos EUA e de capacitação médica. **Terra.** 24 de janeiro de 2023. Disponível em: https://www.terra.com.br/byte/chatgpt-passa-em-prova-de-mba-oab-dos-eua-e-de-capacitacao-medica,9b884393b116e0c0bc5bf35b5e066d63wj7tf4rv.html Acesso em 12 de fevereiro de 2023.

CIRINO DOS SANTOS, Juarez. Direito penal: parte geral. 7ª ed. Florianópolis, SC: Empório do Direito, 2017

COHN, Jonathan. Google's algorithms discriminate against women and people of colour. **The conversation**. 24 de abril de 2019. Disponível em: https://theconversation.com/googles-algorithms-discriminate-against-women-and-people-of-colour-112516 Acesso em: 11 de janeiro de 2023

Comissão conclui texto sobre regulação da inteligência artificial no Brasil, **Agência Senado.** Brasília, 06 de dezembro de 2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/12/06/comissao-conclui-texto-sobre-regulacao-da-inteligencia-artificial-no-brasil Acesso em 12 de fevereiro de 2023.

Convention of Certain Conventional Weapons, 2022. Disponível em: <https://meetings.unoda.org/ccw-mhcp/convention-certain-conventional-weapons-meeting-high-contracting-parties-2022> Acesso em: 05 de fevereiro de 2023.

CUNHA, Maria Alexandra. Smart cities: transformação digital de cidades / Maria Alexandra Cunha, Erico Przeybilovicz, Javiera Fernanda Medina Macaya e Fernando Burgos. São Paulo, 2016. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/18386 Acesso em 13 de janeiro de 2023

Declaração de ministros do G20 identifica 12 ações para acelerar a transformação digital. **GOV.BR**. Brasília, 05 de agosto de 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2021/08/declaracao-de-ministros-do-g20-identifica-12-acoes-para-acelerar-a-transformacao-digital Acesso em 11 de fevereiro de 2023

DOMONOSKE. Camila. Uber Sells Its Autonomous Vehicle Research Division. **NPR.** 08 de dezembro de 2022. Disponível em: https://www.npr.org/2020/12/08/944337751/uber-sells-its-autonomous-vehicle-research-division#:~:text=Uber%20Sells%20Its%20Autonomous%20Vehicle%20Research%20Division%20%3A%20NPR&text=Uber%20Sells%20Its%20Autonomous%20Vehicle%20Research%20Division%20Uber%20has%20sold,core%20investment%20for%20its%20future. Acesso em 10 de fevereiro de 2023.

ERGLANDER, Armin. [...] Veículos autônomos e direito penal / Englander, Armin. [...] Estellita, Heloísa; Leite, Alaor (org.) – 1. ed. – São Paulo: Marcial Pons, 2019.

ESTELLITA, Heloísa. Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas , limitadas e encarregados de cumprimento por crimes praticados por membros de empresa – 1. ed. – São Paulo: Marcial Pons, 2017.

_____. Veículos autônomos e direito penal – 1. ed. – São Paulo: Marcial Pons, 2019.

First human killed by a robot. **Guinness World Records.** Disponível em: <https://www.guinnessworldrecords.com/world-records/first-human-to-be-killed-by-a-robot> Acesso em 10 de outubro de 2022

G20. Declaration of G20 digital ministers, 2021 Disponível em: https://www.g20.org/content/dam/gtwenty/about_g20/previous_summit_documents/2021/declaration-of-g20-digital-ministers-2021final.pdf Acesso em 11 de fevereiro de 2023

GERMANO, Camila. 6G: Pesquisador brasileiro explica tecnologia que substituirá o 5G em 2030. **Correio Braziliense.** São Paulo, 19 de outubro de 2020. Disponível em: https://www.correiobraziliense.com.br/ciencia-e-saude/2022/10/5045335-6g-pesquisador-brasileiro-explica-tecnologia-que-substituira-o-5g-em-2030.html Acesso em: 28 de janeiro de 2023

GLEIZER, Orlando. In: Hilgendorf, Eric. Digitalização e direito; organizador e tradutor Orlando Gleizer, São Paulo, SP: Marcial Pons, 1ª ed., 2020

GLESS, Sabine; WEIGEND, Thomas. Trad.: Heloisa Estellita. Agentes Inteligentes e o Direito Penal. *In:* Veículos autônomos e direito penal. Org.: Estellita, Heloisa; LEITE, Alaor - São Paulo, SP: Marcial Pons, 1ª ed., 2020

Google apologises for Photos app's racist blunder. **BBCNews.** 1 de julho de 2015. Disponível em: https://www.bbc.com/news/technology-33347866 Acesso em: 11 de janeiro de 2023

GOVERNO DO REINO UNIDO. Our ten-year plan to make Britain a global AI superpower Disponível em: https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version#our-ten-year-plan-to-make-britain-a-global-ai-superpower Acesso em 12 de fevereiro de 2023

GRECO, Luís. Problemas de causalidade e imputação objetiva nos crimes omissivos impróprios – Luís Greco; tradução Roman Rocha, 1. ed. – São Paulo: Marcial Pons, 2018.

____. Um panorama da teoria da imputação objetiva. 4ª ed. – São Paulo: Editora Revista dos Tribunais, 2014

____. Dolo sem vontade.

HILGENDORF, Eric. Digitalização e direito; org. e trad. Orlandino Gleizer – São Paulo, SP: Marcial Pons, 2020.

____. Direito e máquinas autônomas. Um esboço do problema. *In:* Veículos autônomos e direito penal. Org.: Estellita, Heloisa; LEITE, Alaor - São Paulo, SP: Marcial Pons, 1ª ed., 2020

HUNT, Elle. Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter. **The Guardian.** 24 de março de 2016. Disponível em: https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech Acesso em: 22 de dezembro de 2022

'I'm the Operator': The Aftermath of a Self-Driving Tragedy. **Wired.** 08 de março de 2022. Disponível em: https://www.wired.com/story/uber-self-driving-car-fatal-crash/ Acesso em 10 de fevereiro de 2023

Killer Robot. **Deseret News**. 08 de dezembro de 1981. Disponível em: <https://news.google.com/newspapers?id=1t00AAAAIBAJ&sjid=xoMDAAAAIBAJ&pg=6313,2597702&dq=kenji+urada&hl=en> Acesso em 22 de fevereiro de 2022

KLIPPENSTEIN, Ken. Exclusive: Surveillance footage of Tesla crash on SF's bay bridge hours after Elon Musk announces "self-driving" feature. **The intercept.** Disponível em: https://theintercept.com/2023/01/10/tesla-crash-footage-autopilot/ Acesso em: 25 de janeiro de 2023

KOLODNY Lora.Tesla under investigation by NHTSA for two more crashes that may have involved Autopilot or FSD. **CNBC**. 22 de dezembro de 2022. Disponível em: https://www.cnbc.com/2022/12/22/nhtsa-initiates-two-more-tesla-crash-investigations.html Acesso em 10 de fevereiro de 2023

Künstliche Intelligenz: Verbraucher vor Risiken schützen. Parlamento Europeu. 10 de fevereiro de 2020 Disponível em: https://www.europarl.europa.eu/news/de/headlines/society/20200206STO72030/kunstliche-intelligenz-verbraucher-vor-risiken-schutzen Acesso em: 23 de dezembro de 2022.

LEVINE, Dan; SPECTOR, Mike. Exclusive: Tesla faces U.S. criminal probe over self-driving claims. **Reuters.** 27 de outubro de 2022. Disponível em: https://www.reuters.com/legal/exclusive-tesla-faces-us-criminal-probe-over-self-driving-claims-sources-2022-10-26/ Acesso em 10 de fevereiro de 2023

LOBO DA COSTA, Regina Helena. Considerações sobre o estado atual da teoria do bem jurídico à luz do *harm principle. In:* Direito penal como crítica da pena. Estudos em homenagem a Juarez Tavares por seu 70º Aniversário em 2 de setembro de 2012. Ed. Marcial Pons: Madrid, 2012.

Mercedes opens sales of Level 3 self-driving system on S-Class, EQS. **Automotive News Europe**. 06 de maio de 2022. Disponível em: <https://europe.autonews.com/automakers/mercedes-opens-sales-level-3-self-driving-system-s-class-eqs> Acesso em 10 de fevereiro de 2023

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. Estratégia Brasileira de Inteligência Artificial, 2021. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-diagramacao_4-979_2021.pdf> Acesso em: 11 de fevereiro de 2023

____. Portaria MCTI Nº 4.979, de 13 de julho de 2021. Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-4.979-de-13-de-julho-de-2021-332164912> Acesso em: 12 de fevereiro de 2023

____.Portaria GM Nº 4.617, de 6 de abril de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gm-n-4.617-de-6-de-abril-de-2021-*-313212172 Acesso em 12 de fevereiro de 2023

MADAKAM, Somayya; RAMASWAMY R., TRIPATH Siddharth. Internet of things (IoT): A literature review. 2015. Disponível em: https://www.scirp.org/journal/paperinformation.aspx?paperid=56616 Acesso em 10 de outubro de 2022

MASSON, Cleber. Código penal comentado. 11 ed. Rio de Janeiro: Método, 2023

META. Disponível em: https://about.meta.com/company-info/ Acesso em 28 de janeiro de 2023; <https://about.meta.com/br/what-is-the-metaverse/> Acesso em: 28 de janeiro de 2023 e https://www.meta.com/work/workrooms/ Acesso em: 28 de janeiro de 2023

MUÑOS CONDE, Francisco/Bittencourt, Cezar Roberto. Teoria Geral do Delito, 2ª ed. – São Paulo: Saraiva, 2004

MORRIS, James. Why Is Tesla's Full Self-Driving Only Level 2 Autonomous?. **Forbes**. 13 de março de 2021. Disponível em: <https://www.forbes.com/sites/jamesmorris/2021/03/13/why-is-teslas-full-self-driving-only-level-2-autonomous/> Acesso em 10 de fevereiro de 2023

OECD. Recommendation of the Council on Artificial Intelligence. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 Acesso em 11 de fevereiro de 2023

O`NEIL, Cathy. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia / Cathy O`Neil; Tradução Rafael Abraham. 1ª ed. Santo André-SP: Editora Rua do Sabão, 2020

O que é IoT? **ORACLE**. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/ Acesso em: 28 de janeiro de 2023

ORTIZ, Mariana Fleming S.; SAYEG, Rodrigo. Do uso de dados tratados pelo poder judiciário. *In: Org.:* FABRI, Andrea Queiroz; NASCIMENTO, Carlos Eduardo do; CHIARELLO DE SOUZA PINTO, Felipe. Compliance and technology law. Uberlândia: Composer, 2020, p. 32.

Paulo de Oliveira, Danilo. Internet 6G chega em 2030 e será 100 vezes mais rápida que o 5G. TechTudo. 23 de junho de 2022. Disponível em: <https://www.techtudo.com.br/noticias/2022/06/internet-6g-chega-em-2030-e-sera-100-vezes-mais-rapida-que-o-5g.ghtml> Acesso em 28 de janeiro de 2023

PEDREIRA, Patrick. O preconceito na inteligência artificial e como combatê-lo. **WELETRIC**. 22 de janeiro de 2019. Disponível em: <https://www.wattson.pt/2019/01/22/o-preconceito-na-inteligencia-artificial/> Acesso em 11 de fevereiro de 2023

PINA, Rute. Britânica que relatou estupro no metaverso: 'Foi real e perturbador'. **Uol.** 03 de junho de 2022. Disponível em: https://www.uol.com.br/universa/noticias/redacao/2022/06/03/estupro-no-metaverso-o-aconteceu-comigo-foi-real.htm

PIRES, Joel Machado; OLIVEIRA NETO, João Soares de. Realidade Aumentada no contexto de Computação Ubíqua: conceitos, características e ferramentas da

plataforma Android, Capítulo 6. 2021. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/76/326/582-1?inline=1 Acesso em: 25 de janeiro de 2023

PHILLIP, Abby. Robot grabs man, kills him in German car factory. **The Washington Post.** 02 de julho de 2015. Disponível em: <https://www.washingtonpost.com/news/morning-mix/wp/2015/07/02/robot-grabs-man-kills-him-in-ger Acesso em: 10 de outubro de 2022

Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN Acesso 06 de fevereiro de 2023.

QU, Tracy. China's algorithm law takes effect to curb Big Tech's sway in public opinion. **South Chine Morning Post.** Shanghai, 1 de março de 2022. Disponível em: https://www.scmp.com/tech/policy/article/3168816/chinas-algorithm-law-takes-effect-curb-big-techs-sway-public-opinion Acesso em 12 de fevereiro de 2023

RAGUÉS I VALLÈS, Ramon. La actuación en beneficio de la persona juridica como presupuesto de su responsabilidad penal. Madri; Barcelona; Buenos Aires; São Paulo: Marcial Pons, 2017.

REALE JR. Miguel. Teoria do Delito – 2ª ed. – São Paulo: Editora Revista dos Tribunais, 2000, p. 24/25.

REGULAMENTO CHINÊS, 2020. Disponível em: http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm Acesso em 12 de fevereiro de 2023

Robô agarra e mata trabalhador dentro de fábrica da Volkswagen. **G1**. São Paulo: 01 de junho de 2015 Disponível em: <https://g1.globo.com/mundo/noticia/2015/07/robo-agarra-e-mata-trabalhador-dentro-de-fabrica-da-volkswagen.html> Acesso em: 10 de outubro de 2022

Robot kills worker at Volkswagen plant in Germany. **The Guardian**. 02 de julho de 2015. Disponível em: <https://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany> Acesso em: 10 de outubro de 2022

ROCHA, Jhonny. Chat GPT: uso de ferramenta de inteligência artificial é analisada por TJMG. **JOTA**. Brasília, 08 de fevereiro de 2023. Disponível em: https://www.jota.info/justica/chat-gpt-tjmg-estuda-uso-de-ferramenta-de-inteligencia-artificial-08022023 Acesso em: 12 de fevereiro de 2023

RODOVALHO, Rodrigo Magalhães; MORAES, Rômulo Eduardo Garcia Moraes. 2017. Computação ubíqua e IHC. Disponível em: https://www.professores.uff.br/screspo/wp-

content/uploads/sites/127/2017/09/artigoIHC1.pdf Acesso em 10 de outubro de 2022

ROXIN, Claus. Derecho Penal. Parte General - Tomo I. Fundamentos. La estructura de la teoria del delito. Traducción de la 2 ed. Alemana. Madrid: Civitas.

____. A Teoria da imputação objetiva. *In:* Estudos de Direito Penal. Trad.: Luís Greco – Rio de Janeiro: Renovar, 2006

____. Sobre o recente debate em torno do bem jurídico. *In:* Novos Estudos de Direito Penal. Trad.: Luís Greco – São Paulo: Marcial Pons, 2014

____. Reflexões sobre a construção sistemática do direito penal. *In:* Novos Estudos de Direito Penal. Trad.: Luís Greco – São Paulo: Marcial Pons, 2014

Russia's Killer Drone in Ukraine Raises Fears About AI in Warfare. **Communications of the ACM**. 23 de março de 2022. Disponível em: https://cacm.acm.org/news/259529-russias-killer-drone-in-ukraine-raises-fears-about-ai-in-warfare/fulltext

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. *In:* Tratado de proteção de dados pessoais. Coord. Danilo Doneda ... et al.]. Rio de Janeiro: Forense, 2021.

SALVADOR NETTO, Alamiro Velludo. Responsabilidade penal da pessoa jurídica. São Paulo: Revista dos Tribunais, 2018.

SCHIETTI CRUZ, Rogerio. SANTOS, André Luiz Nogueira. ORTIZ. Mariana Fleming S. A responsabilidade penal omissiva imprópria e a posição de garante do dirigente de empresa na jurisprudência do Supremo Tribunal Federal. *In:* Direito econômico, os instrumentos de regulação e a empresa. Org.: SAYEG, Ricardo Hasson. SÉLLOS-KNOERR, Viviane Coêlho de, BENACCHIO, Marcelo. Coord.: HUDLER, Daniel Jacomelli. GARCEL, Adriane. São Paulo: Universidade Nove de Julho, 2021.

SCHÜNEMANN, Bernd. Sobre a posição de garantidor nos delitos de omissão imprópria - possibilidades histórico dogmáticas, materiais e de direito comparado para escapar de um caos. In: GRECO, Luís (Org.). Estudos de direito penal, direito processual penal e filosofia do direito. São Paulo: Marcial Pons, 2013, p. 159–181.

SILVA SANCHEZ, Jesús-María. Fundamentos del derecho penal de la Empresa. 2. ed. Buenos Aires: B de F, 2016.

____. A expansão do direito penal: aspectos da política criminal nas sociedades pós industriais. Trad.: Luiz Otávio de Almeida Rocha, 3ª ed. São Paulo: Editora Revista dos Tribunais, 2013.

SENADO FEDERAL, 2022. Relatório Final da Comissão de Juristas responsável por subsidiar a elaboração de substitutivo sobre inteligência artificial. Disponível em: <https://legis.senado.leg.br/diarios/ver/111533?sequencia=2> Acesso em 11 de fevereiro de 2023.

Superior Tribunal de Justiça - AgRg no RHC n. 164.698/PE, relator Ministro Olindo Menezes (Desembargador Convocado do TRF 1ª Região), Sexta Turma, julgado em 6/12/2022, DJe de 19/12/2022; HC n. 68.871/PR, relatora Ministra Maria Thereza de Assis Moura, relator para acórdão Ministro Og Fernandes, Sexta Turma, julgado em 6/8/2009, DJe de 5/10/2009; HC n. 46.525/MT, relator Ministro Arnaldo Esteves Lima, Quinta Turma, julgado em 21/3/2006, DJ de 10/4/2006 e REsp n. 822.517/DF, relator Ministro Gilson Dipp, Quinta Turma, julgado em 12/6/2007, DJ de 29/6/2007

TANGERMANN, Victor. Elon Musk promise self-driving cars “next year” every year since 2014. **Futurism.** 19 de janeiro de 2022. Disponível em: https://futurism.com/video-elon-musk-promising-self-driving-cars Acesso em 10 de fevereiro de 2023

TAVARES, Juarez. Fundamentos da teoria do delito – 1. ed. – Florianópolis: Tirant lo Blanch, 2018.

____. Teoria do crime culposo –5. ed. Florianópolis: Tirant lo Blanch, 2018.

____. Teoria do Injusto Penal – 4. ed. – São Paulo: Tirant lo Blanch, 2019.

TESLA. Disponível em: <https://www.tesla.com/support/autopilot> Acesso em 12 de janeiro de 2023

Tesla behind eight-vehicle crash was in ‘full self-driving’ mode, says driver. **The Guardian**. 22 de dezembro de 2022. Disponível em: <https://www.theguardian.com/technology/2022/dec/22/tesla-crash-full-self-driving-mode-san-francisco> Acesso em 25 de janeiro de 2023

The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems. Disponível em: <https://mail.intgovforum.org/multilingual/sites/default/files/webform/toronto-declaration-final.pdf> Acesso em 11 de fevereiro de 2023

THORBECKEDA, Catherine. Uber Eats dos EUA lança serviço de entrega feito por robôs. **CNN.** 15 de dezembro de 2022 Disponível em: <https://www.cnnbrasil.com.br/business/uber-eats-dos-eua-lanca-servico-de-entrega-feito-por-robos/> Acesso aos 25 de janeiro de 2023

Twitter: Ellon Musk. 24 de novembro de 2022. Disponível em: https://twitter.com/elonmusk/status/1595682322707267584?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1595682322707267584%7Ctwgr%5Ed2c6a0139310859c89fd4180579f01906908c1e2%7Ctwcon%5Es1_&ref

_url=https%3A%2F%2Ftheintercept.com%2F2023%2F01%2F10%2Ftesla-crash-footage-autopilot%2F

Twitter: Gerry (TayTweets). 23 e 24 de março de 2016. Disponível em: <https://twitter.com/geraldmellor/status/712880710328139776?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E712880710328139776%7Ctwgr%5Ed762487f856bcbdb1c7acb833dd9faa1140d9e51%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fwww.theverge.com%2F2016%2F3%2F24%2F11297050%2Ftay-microsoft-chatbot-racist> Acesso em: 22 de dezembro de 2022

Uber's self-driving operator charged over fatal crash. **BBC**. 16 de setembro de 2020 Disponível em: <https://www.bbc.com/news/technology-54175359> Acesso em: 10 de fevereiro de 2023.

U.S. Policy on Lethal Autonomous Weapon Systems. 14 de novembro de 2022. Disponível em: https://www.google.com/search?q=Defense+Primer%3A+U.S.+Policy+on+Lethal+Autonomous+Weapon+Systems&oq=Defense+Primer%3A+U.S.+Policy+on+Lethal+Autonomous+Weapon+Systems&aqs=chrome..69i57.278j0j7&sourceid=chrome&ie=UTF-8#:~:text=Resultados%20da%20pesquisa-,U.S.%20Policy%20on%20Lethal%20Autonomous%20Weapon%20Systems,https%3A//crsreports.congress.gov%20%E2%80%BA%20product%20%E2%80%BA%20pdf,-PDF Acesso em: 05 de fevereiro de 2023.

VERONESE, Alexandre. Os Direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. in Lei Geral de PROTEÇÃO DE DADOS PESSOAIS e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019.

VIANA, Eduardo. Dolo como compromisso cognitivo. São Paulo: Marcial Pons, 2017

VIEIRA, RACKEL. Prefeitura de Aparecida começa a levar internet gratuita a 200 cantos da cidade. **Prefeitura de Aparecida**. Aparecida, 30 de março de 2022. Disponível em: https://www.aparecida.go.gov.br/prefeitura-de-aparecida-comeca-a-levar-internet-gratuita-a-200-cantos-da-cidade/ Acesso em 25 de janeiro de 2023

WEISER, MARK. The computer for the 21st century (1991). Disponível em: <https://dl.acm.org/doi/pdf/10.1145/329124.329126 Acesso em: 22 de dezembro de 2022

WHYMAN, Robert. From the archive, 9 December 1981: Robot kills factory worker. The Guardian. 09 de dezembro de 2014. Disponível em: <https://www.theguardian.com/theguardian/2014/dec/09/robot-kills-factory-worker> Acesso em 22 de fevereiro de 2022

WIENS, Roger. Perseverance Now Selects its Own Targets to Zap. 31 de maio de 2022. **NASA.** Disponível em:

https://mars.nasa.gov/mars2020/mission/status/383/perseverance-now-selects-its-own-targets-to-zap/ Acesso em: 13 de janeiro de 2023

Youtube. Disponível em: https://www.youtube.com/watch?v=RDCbsn_5On4 Acesso em 10 de fevereiro de 2023