UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

EDUARDO LOUREIRO CALAZANS

SISTEMAS DE ARMAS AUTÔNOMAS E O DIREITO: UMA ANÁLISE DO CENÁRIO REGULATÓRIO

BRASÍLIA

2025

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

EDUARDO LOUREIRO CALAZANS

SISTEMAS DE ARMAS AUTÔNOMAS E O DIREITO: UMA ANÁLISE DO CENÁRIO REGULATÓRIO

Trabalho de conclusão de curso de graduação apresentado à Faculdade de Direito da Universidade de Brasília, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientador: Evandro Piza Duarte

BRASÍLIA

2025

EDUARDO LOUREIRO CALAZANS

SISTEMAS DE ARMAS AUTÔNOMAS E O DIREITO: UMA ANÁLISE DO CENÁRIO REGULATÓRIO

Monografia apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília, campus Darcy Ribeiro, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Data da defesa: 13/02/2025.

Resultado: Aprovado.

BANCA EXAMINADORA

_____

Professor Doutor Evandro Piza Duarte (FD-UnB)

Orientador

_____

Professor Mestre Pedro Sousa (FD-UnB)

Coorientador

_____

Professor Mestre Thales Cassiano Silva (FD-UnB)

Examinador

_____

Professor Mestre Tiago Kalkmann (FD-UFRGS)

Examinador

BRASÍLIA

2025

RESUMO

O acirramento das tensões geopolíticas ao redor do Globo e a deflagração do status de guerra num retorno rompante por parte de várias das potências armamentistas tem gerado elevada preocupação da Comunidade Internacional, sobretudo em relação ao prognóstico de uso de novas armas de guerra, Sistemas Letais Autônomos dronificados, nesses teatros de combate nos anos vindouros.Essa dinâmica desperta uma grande inquietude, relacionada não só ao entendimento de seu funcionamento, ainda pouco disseminado para sociedade civil num geral, mas sobretudo, acerca da necessidade de regulação jurídica que envolva controle humano significativo desses dispositivos, antes que efetivamente se tornem uma grave realidade em desrespeito aos Direitos Internacionais Humanitários. Nesse contexto, o conteúdo desse trabalho busca investigar em ampla revisão bibliográfica os aspectos regulatórios e jurídico-dogmáticos no campo das lacunas ameaçadas pelo seu pleno desenvolvimento, ausente intervenção normativa da comunidade internacional, buscando adereçar o status da elaboração de políticas e de normas legislativas e de governança incidentes sobre a temática das inteligências artificiais e dos sistemas de armas autônomas .

Palavras-chave: Convenção de Certas Armas Adicionais, Direito Internacional Humanitário; Inteligências Artificiais, Sistemas de Armas Autônomas, Responsabilidade Criminal.

ABSTRACT

The worsening of geopolitical conflicts all around the Globe, and the outbreak of warfare by some of hawkish powerhouses has been creating great concern on the international Community. Mostly due to the forecast for the new artificial intelligence weapons spreading. The inclination on the forthcoming deployment of letal autonomous weapons at these war theaters in the next years, raise a deep inquietude, related not only to its usage, yet few enlarged to the civil society, but mainly according to the urge of its legal regulation and compelling of a significant human control. In this regard, this scientific work sums up the need to scrutinize pathways to develop already consecrated regulatory and dogmatic legal instruments that may offer at their improvement, clear and safe routes to settle the issues of the metajuridic gaps represented by their fully development, meaningful normative interventions by the international community.

Keywords: Autonomous weapon systems; Artificial Intelligence; The Convention on Certain Conventional Weapons; Criminal Responsibility, International Humanitarian Law, International Armed Conflicts

LISTA DE ABREVIATURAS E SIGLAS

AIA	*Artificial Intelligence Act*
ANAC	Agência Nacional de Aviação Civil
AWS	*Autonomous Weapon System*
CF	Constituição Federal
CAC	Convenção sobre certas Armas Convencionais
DECEA	Departamento de Controle do Espaço Aéreo
EUA	Estados Unidos da América
IA	Inteligência Artificial
LGPD	Lei Geral de Proteção de Dados
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
SKB	*Stop Killer Robots*
R.C	Responsabilidade Civil
UE	União Europeia
SAC	Sistema de Aviação Civil Brasileiro
ML	*Machine Learning*
PL	Projeto de Lei
VANT	Veículo Aéreo não Tripulado

LISTA DE FIGURAS

INTRODUÇÃO

O desenvolvimento de tecnologias dotadas de inteligência artificial tem desvelado um paradigma cada vez mais imprevisível em todos os campos da atividade humana. Ademais, a velocidade com que a indústria bélica tem desenvolvido novos artefatos, absolutamente incompatíveis com os modelos existentes de tutela jurídica, indica a urgência de estudo desses maquinários, com o objetivo de frear seu potencial destrutivo e, ainda, de buscar meios de responsabilização pelo uso abusivo ou inadequado desses dispositivos.

O acirramento das tensões geopolíticas ao redor do Globo e deflagração do status de guerra num retorno rompante por parte de várias das potências armamentistas, tem gerado elevada preocupação da comunidade internacional, sobretudo em relação ao prognóstico de uso de novas armas de guerra, Sistemas Letais Autônomos dronificados, nesses teatros de combate[1] nos anos vindouros. Realidade essa que desperta uma grande inquietude, relacionada não só ao entendimento de seu funcionamento, ainda pouco disseminado para sociedade civil num geral, mas sobretudo acerca da necessidade de regulação jurídica que envolva controle humano significativo desses dispositivos.

Contudo, dada a novidade que essas tecnologias representam até o momento, não é conhecido um regime próprio de seu tratamento no mundo jurídico. Assim, surge a necessidade de examinar alternativas de desenvolvimento de outros institutos já consagrados que ofereçam, na modernização de suas dinâmicas próprias, alternativas claras e seguras para dirimir as problemáticas de um futuro já inevitável, em que caçadores armados irão decidir quando, e como, ceifar vidas.

O reconhecimento dos conflitos éticos e tecnológicos suscitados pelo uso dessas tecnologias já mobilizou a sociedade civil global[2] a demandar das nações providências concretas que limitem a existência desses dispositivos.

A finalidade desta monografia, portanto, é de apresentar, por meio de revisão bibliográfica, um panorama geral acerca da origem, características e justificação do emprego

---

[1] Numa guerra, chama-se teatro de operações ou **teatro de guerra** uma área em que eventos militares importantes ocorrem ou estão em andamento.

[2] https://www.stopkillerrobots.org/ - Página Oficial da Campanha para Parem os Robôs Assassinos, movimento social que mobiliza diversas organizações não governamentais e especialistas que pugnam pelo banimento dos Sistemas Eletrônicos de Armas Autônomas.

das armas autônomas em situações de conflito. Além de oferecer essa visão geral, serão também discutidas possíveis vias de proibição ou regulamentação de tais dispositivos, delineadas pela doutrina majoritária do Direito Internacional Penal e pelas Convenções e Tratados Internacionais atualmente em vigor ao redor do mundo.

Metodologicamente, a pesquisa científica aqui investida possui caráter exploratório e de abordagem qualitativa, baseados no procedimento hipotético-dedutivo aliado a técnica de pesquisa bibliográfica e documental indireta, a partir de revisão literária e de análise crítica das referências utilizadas – livros, artigos científicos, legislação, relatórios de organismos nacionais, internacionais e grupos de trabalhos especializados na temática afeta, além de dados estatísticos disponibilizados em sítios especializados por instituições de monitoramento.

O trabalho está organizado em duas partes. A primeira trará o escrutínio dos desafios éticos envolvidos na presente insuficiência dos atuais parâmetros dogmáticos do Direito ao lidar com os sistemas letais automatizados, com fins de desvelar em que termos consistem nas lacunas afetadas por seu emprego dentro do campo do direito penal e da sujeição da responsabilidade civil. Serão também apresentadas algumas das principais propostas doutrinárias lançadas pelos estudiosos da área, para remediar os conflitos éticos e a ausência de vinculação do seu uso dentro dos contornos previstos na normatividade vigente das vias clássicas do direito internacional, possibilitando o levantamento das informações essenciais ao próximo capítulo, onde serão analisadas as legislações que tratam dos sistemas de inteligência artificial em caráter geral, a nível doméstico e internacional.

Na segunda parte do trabalho, além do exame da proposta do projeto de lei das Inteligências Artificiais no Brasil, será empregado um breve estudo de modelo comparado com a legislação da União Europeia, já mais avançada na temática. Esse objeto se justifica com o propósito de melhor compreender a convergência do modelo proposto no país com o estabelecido pela legislação internacional, bem como introduzir os dilemas que demonstram como o desenvolvimento dessa seara depende diretamente das formulações que vem se consolidando no contexto do Direito Internacional sob desiderato de estabelecer novas balizas à sua produção e manejo.

Por fim, cumprido esse objetivo, será realizada uma síntese histórica do desenvolvimento das regras internacionais do Direito Internacional dos Conflitos Armados e da linha temporal na qual a temática em discussão vem evoluindo nesse campo, prestando-se à finalidade de promover o estado da arte, e quais elementos constituem efetivamente a agenda

dos esforços da comunidade internacional no tratamento dos dispositivos armados telecomandados.

CAPÍTULO I - A DRONIFICAÇÃO DA VIDA E A INSEGURANÇA JURÍDICA DO DIREITO INTERNACIONAL HUMANITÁRIO

Os Sistemas de Armas Letais Autônomas dronificados nada mais são do que drones armados dotados de sistemas computacionais de inteligência artificial capazes de tomar decisões sem a necessidade de intervenção humana. Em verdade, ausente essa última característica, em nada se diferenciam de outros tipos de drones já existentes.

Drone é a palavra empregada para descrever uma terminologia leiga que faz menção a qualquer dispositivo remotamente tripulado. Desse modo, é essencialmente impossível elencar um rol de características que o definem, para além da possibilidade de controlá-lo remotamente. Aliás, essa é a definição exata apresentada por Gregóire Chamayou, segundo o qual: "qualquer veículo, qualquer máquina pilotada pode ser "dronizada" a partir do momento em que não há mais tripulação humana a bordo" (Chamayou, 2015, p.16).

No caso concreto, tal como tantas outras tecnologias concebidas com fins militares, a aplicação com finalidades distintas do emprego de força já se tornou uma realidade mais habitual que seu uso tático-estratégico, seja no Brasil, seja no resto do mundo.

Segundo levantamentos realizados pela Agência Nacional de Aviação Civil (ANAC)[3] junto ao Departamento de Controle do Espaço Aéreo - DECEA, já somos o principal mercado de aeronaves não tripuladas na América Latina, e já existem mais de cem mil aeronaves registradas no Brasil.

Hoje, a popularidade desses dispositivos é virtualmente infinita, estando presente na aplicação no agronegócio, no monitoramento do desmatamento, na construção civil, atividades de vigilância e delivery e, dada a criatividade com a qual podem ser projetados, seguirão cada vez ocupando os mais variados nichos em todos os setores da economia.

Com efeito, o estudo sobre a temática dos drones pode seguir em qualquer campo, afinal, são ferramentas cada vez mais consagradas, dada a otimização de tempo e recursos por eles propiciadas na execução de atividades até então absolutamente especializadas.

---

[3] A ANAC é a agência reguladora encarregada de disciplinar o uso de drones no Brasil.

Neste trabalho, no entanto, o objetivo essencial será de compreender sua atuação específica nos contextos em que o emprego de tais equipamentos representam risco à vida, especialmente com relação às novas interações que vem gerando robôs armados com fins bélicos.

I.1 – GUERRA 2.0: OS DILEMAS ÉTICOS DA VIOLÊNCIA ARMADA NÃO-HUMANA

Conforme se depreende da justificativa na corrida armamentista por itens de automação na seleção de alvos, a ideia central de evitar erros humanos – vez que os soldados seriam menos precisos, menos confiáveis e sujeitos ao cansaço e problemas psicológicos (Bedin, 2021, p.442), haveria na alternativa robótica uma demanda indispensável pela autorregulamentação dos algoritmos incorporados às inteligências artificiais que garantisse o respeito aos padrões internacionais de direito humanitário. A tendência, pelo contrário, é de encontrar algoritmos imprecisos e repletos de tendências racistas e discriminatórias.

Essa constatação advém do entendimento do processo de aprendizagem de máquinas e da base histórica que serve de partida das suas configurações iniciais. Segundo Sousa (2022, p. 27), a IA é um produto das decisões humanas passadas, que são suscetíveis ao viés humano, podendo ser distorcidas por preconceitos institucionais e históricos.

Em decorrência de tantas zonas cinzentas na confiabilidade conferida às máquinas, põem-se em xeque os limites das atividades em que seu uso deveria ser proibido ou, ao menos, regulado.

Christian Enemark (2023 p. 162), professor da Universidade de Edimburgo, inicia o sexto capítulo do livro Moralidades da Violência dos Drones rememorando um concurso realizado no ano de 2020, pela Agência de Pesquisa em Projetos Avançados de Defesa dos Estados Unidos, o AlphaDogFight, com fins de demonstrar o potencial das Inteligências Artificiais normalmente executados por seres-humanos. Na ocasião, durante simulação virtual, um algoritmo foi capaz de repetidamente destruir a aeronave de seu adversário, um piloto altamente especializado.

Logo em seguida, levanta-se o questionamento sobre os desafios éticos que são associados no exercício da violência promovido em contexto de distanciamento físico entre homem e máquina. O ponto de partida das reflexões surge da separação conferida na automação de funções consideradas menos importantes, “Por exemplo decolagem, pouso e manobras

aéreas" (Enemark, 2023 p. 162), e a perspectiva vindoura desses sistemas de decidir quando e como praticar atos violentos.

Existem grandes chances de a incorporação de plena automação com uso de IA se dar primeiro nos sistemas autônomos letais. Aqui, são defendidos dois elementos que justificam a priorização desse investimento.

O primeiro elemento é que a vantagem tática conferida pelo domínio do espaço aéreo não só evita a surpresa de receber novas ofensivas pelos céus, como também possibilita o desenvolvimento de outras atividades em que o poder aéreo representa papel central (ataques, transporte e vigilância) sem interferências externas. Nessa senda, a demanda imposta é de que os drones-armados sejam cada vez mais rápidos e eficientes em suas manobras nos espaços contestados. Tal desiderato certamente será mais eficiente sob operação de algoritmos, cuja capacidade de processamento supera em muito a de agentes humanos.

O segundo elemento é que o cenário aéreo representa um espaço menos propenso a ocorrência de danos imprevistos durante a experimentação dessas tecnologias, se comparados à sua implementação em veículos terrestres, dado o maior grau de liberdade – menor densidade de sujeitos em ar, e consequente mitigação de danos colaterais (Enemark, 2023, p. 164).

Até que seja produzida e implementada uma Inteligência Artificial Geral, capaz de isoladamente operacionalizar tais dispositivos, é descrito o processo de refinamento de modelos de IA mais restritos, voltados à execução de atividades específicas que operam em conjunto nos armamentos baseados em drones: mobilidade, gestão de saúde (aqui colocado como a capacidade de manutenção do sistema informático), interoperabilidade, inteligência (posto como a habilidade de coletar e processar dados) e uso da força (protocolos envolvidos na capacidade da máquina de operacionalizar uma cadeia de destruição).

A crescente capacidade de desenvolvimento autônomo de centros de controle específicos dessas atividades guarda relação central com o principal elemento que diferencia um armamento autônomo de qualquer outra modalidade de exercício da violência até então conhecida.

A falta de um norte específico que direcione seu manejo decorre também de uma ampla dificuldade em definir responsabilidades sobre os envolvidos no seu uso em campo, dada a dificuldade em determinar a responsabilidade direta, seja de um programador, seja de um comandante que decide enviar um dispositivo a determinada operação, visto que, como visitado anteriormente, é muito difícil determinar se uma ação maliciosa é resultante de *data poisoning*

– prática de inserção de dados maliciosos por programadores crackers ou resultado de falhas no design, ou de uma decisão consciente por parte dos operadores.

Essa incerteza pode levar a acusações injustas contra indivíduos inclusos na cadeia sem necessariamente possuírem controle significativo sobre o comportamento do sistema, demandando protocolos absolutamente estritos com relação à supervisão técnica, na regulamentação ou no controle ético dessas tecnologias. Elemento que possivelmente torna a atrair a responsabilidade estatal como um todo:

> Nesse Sentido, a lacuna constatada pela falta da responsabilização individual, deveria recair sobre o Estado que a tenha colocado em operação, a ver "os seres humanos têm direitos protegidos pelo Direito internacional e que a denegação desses direitos engaja a responsabilidade internacional dos Estados, independentemente da nacionalidade das vítimas de tais violações" (Piovesan, *apud* Buergenthal, 2022, p.34)

É o raciocínio retomado pela mesma autora na implicação do Direito costumeiro, em que os Estados são responsáveis pelas violações humanitárias perpetradas em seu território, ou por um de seus nacionais:

> Nessa toada, a resistência da comunidade internacional em adotar regime específico que puna os envolvidos numa operação com desfechos trágicos atrai a responsabilidade ao próprio Estado "Com esse raciocínio, perceber-se-á como a violação de uma obrigação internacional pelo Estado, seja em razão de ação ou omissão, implica responsabilização internacional. (Piovesan, 2022, p. 34)

Nesses termos se justifica o interesse transnacional de buscar a adoção de vias dogmáticas que regulem esses excessos – de forma desvinculada da responsabilização internacional, e que na atualidade não se coadunam com outros regimes próprios do Direito, seja no campo criminal, seja em outros institutos também já consagrados como o da responsabilidade civil, como passamos a ver.

I.2 – O *ACCOUNTABILITY GAP* E A REGULAÇÃO JURÍDICA NO MUNDO DIGITAL

Situados nas problemáticas levantadas no item anterior, passamos agora a desenvolver o clímax desse trabalho – quais são as respostas dogmáticas que podem oferecer respostas à crise dos princípios metajuridicos que norteiam a proteção à vida e à dignidade humana.

Seguimos permanentemente desenvolvendo novas tecnologias com o intuito de viver melhor. Sempre esperamos que suas capacidades, aquém das limitações humanas, cumpram o papel de otimizar nossas jornadas diárias, e de nos manter mais seguros e confortáveis, de

cometer menos erros e melhor desfrutar do tempo sobre a terra. Não obstante, em segundo momento, surge a seguinte indagação: E o que acontece quando essa tecnologia porventura vier a causar em contexto de conflito armado risco de vida a seres-humanos não envolvidos, ou mesmo em face da própria coletividade?

Nesse liame, vai se tornando diretamente cada vez mais imprescindível promover os elementos do que a doutrina tem enquadrado sob a perspectiva do constitucionalismo digital, cujo desiderato principal é de assegurar a proteção dos direitos fundamentais também no ambiente digital, balizando meios de governança justa e equilibrada, que acompanhem o desenvolvimento tecnológico do mundo computacional. E, para tanto, o surgimento de novas situações ainda não abarcadas pelas lacunas dos sistemas jurídicos "demandam uma resposta normativa, com o fito de manter seu equilíbrio" (Celeste, 2019, p. 12)

Até o presente momento, existem várias correntes doutrinárias que divergem sobre a necessidade de modernização de ramos próprios do Direito, com o fito de proporcionar essa resposta.

De forma não exaustiva, passemos a investigar algumas das principais propostas doutrinárias que alinham a necessária regulação das LAWS em meio aos contornos desejáveis do constitucionalismo digital, considerando o esgotamento dos modelos tradicionais por meio dos quais foram consagradas as tipificações próprias no campo do direito penal e do direito internacional humanitário.Passemos a analisar, em primeiro plano, os impasses contidos para atingir essa finalidade por meio do direito penal e da responsabilidade civil.

Da perspectiva do direito penal, Gomes (2001, *passim.*) descreve que o fato formal e materialmente típico compreende seis requisitos agrupados em três categorias. Os quatro primeiros são aspectos formais-objetivos, o quinto é normativo e o sexto é subjetivo. Assim, para que haja um fato típico, é necessário (i) uma conduta humana voluntária; (ii) um resultado naturalístico; (iii) um nexo de causalidade; (iv) uma relação de tipicidade; (v) um resultado jurídico desvalioso que implica numa ofensa: a) objetivamente imputável à conduta; b) concreta ou real; c) transcendental; d) grave; e) intolerável; e f) objetivamente imputável ao risco criado pelo agente; e (vi) uma imputação subjetiva nos casos de crimes dolosos.

Por conseguinte, dada a atual dogmática, já seria impossível no primeiro item punir um delito a um "ser" cibernético, sem que antes se considerasse a criação de uma personalidade jurídica para esses entes eletrônicos.

Inviabilizada a aplicação tradicional da Teoria da Culpa quando tratamos de tecnologias inteligentes, que nada mais são além de entes cibernéticos que atuam a partir da coleta de dados disponíveis para consolidar padrões, com base nos quais passam a realizar previsões e tomar decisões sem interferência humana (Gless *et al.*, 2016, p. 413-414).

Vimos em seção anterior, inclusive, que o processo de aprendizagem cibernética funciona diretamente vinculada ao repositório informacional previamente incluído nos dados históricos inseridos em suas primeiras iterações, tornando-as imprevisíveis e repletas de vieses discriminatórios, elevando de sobremaneira a desconfiança em torno de itens imbuídos de força letal.

Em se tratando da responsabilidade penal individual por crimes de guerra, por exemplo, essa surgiu de um profundo desejo de responsabilizar indivíduos por atrocidades e de desencorajar sua ocorrência futura. O direito penal é útil para criar e aplicar proibições, e, portanto, fornece um regime de responsabilidade apropriado para genocídio, escravidão, massacres, estupro sistemático e outros ultrajes semelhantes. Mas, embora os sistemas de armas autônomos sejam capazes de cometer graves violações do direito internacional humanitário com consequências trágicas, eles são úteis demais para serem criminalizados (Crootof, 2016, p. 1351).

A autoconsciência é outro dos elementos central dessa discussão, e para efeitos desse debate é válido suscitar o conceito do naturalismo biológico –segundo o qual a consciência humana, diferentemente das máquinas, possui características de subjetividade e estados de humor não replicáveis pelas IA - desprovidas de estados mentais, e até podendo ter conhecimento, mas não inteligência, e doravante, a consistente falta de *animus* que as torna essencialmente inimputáveis.

Por conseguinte, as respostas produzidas por algoritmos, que incluem condições ambientais, inserção de sugestões pelos usuários e o próprio processo de aprendizagem permanente da inteligência artificial, promovem o *standard* desses aparelhos como uma mescla, em parte produto de um engenheiro que o programou, e em parte o resultado infindo dos cálculos e iterações seguintes que põe em movimento por si mesmas, e cujas decisões passam a ser absolutamente imprevisíveis, mesmo aos seus criadores.

Uma vez constatado o rompimento do vínculo direto entre os agentes humanos e as realizações dos seus engenhos, faz-se necessário responder: seria possível incluir os próprios robôs como entes sujeitos à persecução criminal por seus atos?

Vários doutrinadores têm passado a advogar sobre a necessidade de estabelecer mecanismos próprios para responsabilizar aqueles que não tomam as medidas necessárias para controlar o risco derivado das atividades de seus robôs. Todavia, são os humanos que os produzem, programam, vendem e utilizam - os verdadeiros alvos das possíveis responsabilizações, seja na via criminal, seja por meio de institutos da responsabilização civil.

Nesse sentido, passaremos a examinar algumas produções literárias que cuidam da mesma temática, pela ótica de Rebecca Crootof, Sthéfano Divino, Pedro Sousa e de Gless; Silverman e Weigend.

O primeiro texto trata da responsabilidade incidente sobre o uso dos Sistemas de Armas Autônomas, tendo como objeto principal a lacuna jurídica existente no campo do direito internacional em relação ao uso desses itens. Decorre da característica *sui generis* dessa tecnologia, distinta das demais ferramentas bélicas que sempre serão acionadas ou programadas por um indivíduo, de forma dolosa, ainda que em virtude de dolo genérico.

Surge nesse liame a sugestão de que a evolução natural do Direito para abarcar tais situações envolve uma evolução do tratamento doutrinário que abarque novas dinâmicas de mundo e modernize institutos já consagrados. Com relação ao objeto em discussão, Rebecca Crootof apresenta afirma que "a responsabilidade civil, o regime legal governando aqueles delitos civis não-contratuais pelos quais um indivíduo pode compensá-los, não possui um sósia internacional" (Crootof, 2016, p. 1351) e prossegue atribuindo à escassez de desenvolvimento de um tratado internacional na qualidade da responsabilidade civil como elemento no qual subsiste a lacuna jurídica posta em discussão neste trabalho:

No entanto, essa lacuna de responsabilização é precisamente o tipo de problema que a responsabilidade civil é projetada para resolver. Pressões similares a essa sustentaram a transformação da lei doméstica da responsabilidade civil mais de um século atrás - a necessidade de se criar um sistema de responsabilização para os 'casos desconhecidos' da revolução industrial, relevantes, não intencionais e relativos aos danos de maquinários – estão presentes novamente, dessa vez na esfera internacional.[4] (Crootof, 2016, p. 1353)

[4] Trad nossa: no original "However, this accountability gap is precisely the kind of problem tort law is designed to solve. Pressures like those that fostered the transformation of domestic tort law over a hundred years ago – the need to create a liability regime for the 'stranger cases' resulting from Industrial Revolution's significant, unintended, machine-caused injuries – are at play again, now in the international sphere" - CROOTOF, Rebecca. *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV.
1347 (2016). (p.1353)

Segundo a autora, a perspectiva de desenvolvimento dessa modalidade de regulamentação oferece uma perspectiva muito mais vantajosa que o caminho do direito penal, que pugna por proibições absolutas. A responsabilidade civil, por sua vez, oferece meios de regrar atividades que possuem valores suficientemente elevados para que se considere seu descarte, pondo alternativas de compensação quando ocorrem os danos que lhes são inatos. Esse raciocínio inclusive já constitui a normatividade internacional em relação aos seus agentes quando ocorrem excessos ou são tomadas ações contrárias às instruções que lhes foram indicadas, de igual modo com relação aos particulares ou entidades reconhecidas como legítimas em seus próprios Estados.

Contudo, a principal discussão jurídica em torno das possíveis vias de responsabilização em torno da periculosidade conferida aos sistemas letais vai de encontro à lacuna de *accountability* que esses itens representam, ao desafiar a noção essencial que inclui a persecução dos responsáveis por alguma modalidade de lesão em torno da intencionalidade de algum agente humano (Crootof, 2016, p.1366).

Sobre o tema, Sthéfano Divino (2020, p. 162) descreve as possibilidades de impor a responsabilidade criminal das Inteligências Artificiais partindo da designação clássica da doutrina, que exige dois elementos prévios: i) o primeiro é o elemento externo ou de fato, expresso na tipificação de conduta criminal (*actus reus*); ii) o elemento interno ou mental designado pelo conhecimento ou intenção delituosa (*mens rea*). Nos termos já desenvolvidos até aqui, torna-se impossível a aplicação da responsabilidade criminal para as máquinas em face do último.

Pedro Sousa (2023, p. 37) sintetiza ainda, a produção de Gabriel Hallevy em três vias principais de possíveis responsabilizações penais vinculadas às AI:

- O primeiro desses modelos é o chamado *the perpetration-by-another liability model*, neste modelo, fatos típicos praticados por IA seriam de responsabilidade das pessoas envolvidas em sua produção e/ou operação, quando for o caso;
- O segundo modelo é o *the natural probable-consequence liability model*, segundo o qual não é necessário que haja o conhecimento dos atos praticados pela IA, mas os operadores de algoritmos estariam “obrigados a saber que esse delito é uma

consequência natural e provável" [5] de seus atos e assim, incorrendo em lesão, tanto a IA quanto as pessoas envolvidas em sua criação e operação seriam puníveis;

- O terceiro modelo apresentado é o *the direct liability model*, que separa a IA de seus desenvolvedores e usuários, fazendo com que tecnologias como machine learning e deep learning podem ser consideradas formas de conhecimento, possibilitando até mesmo, de acordo com Hallevy (2010, p. 28), "uma IA defender sua existência perante as excludentes de ilicitude, como legítima defesa" haja vista que as máquinas, incorporando fatos transformados em dados objetivos e experiências por meio do *machine learning* são capazes de preencher o *mens rea*.

Prosseguindo na investigação, Sousa discorre sobre uma série de produções que tratam da aplicação da Teoria da Ação Significativa - a qual limita o conceito de ação, de modo que só há caracterização da responsabilidade penal "quando caracterizada uma ação cujo sentido é socialmente indesejado, de forma que meros acontecimentos não merecem atenção do Direito penal" (Sousa, 2023, p. 39), tornando necessária para eventual julgamento de crimes praticados por IA, indagar se esse fato pode ser interpretado, no âmbito da causalidade, como manifestação objetiva da vontade do ser humano que a controla.

Cumpre destacar que, diferentemente de outros armamentos automáticos, como minas terrestres e armas sentinelas, cuja deflagração é meramente reativa ao acionamento de uma armadilha, os LAWS ativamente atuam por meio do processamento de dados para tomar decisões independentes, sem que haja qualquer tipo de interação humana no sistema ou sobre o sistema, tornando ainda mais obscuro um procedimento pelo qual possa ser mensurada a eventualidade de seu acionamento fora dos parâmetros desejáveis em caso de mau funcionamento.

É possível realizar uma conexão, por exemplo, do desenvolvimento de uma perspectiva de adoção de responsabilização da própria Inteligêncial Artificial como ente sujeito à persecução penal no modelo da *direct liability model* com a evolução da doutrina penal alemã, sob acepção do funcionalismo penal - segundo a qual a evolução da persecução penal tem evoluído para além do objetivo de punir faltas, e sim reestabelecer a confiabilidade social com relação à norma lesionada pelo ofensor (Gless *et al.*, 2016, p.421).

---

[5] "When an AI algorithm functions properly, there is no reason for it not to use all of its capabilities to analyze the factual data received through its receptors. However, an interesting legal question would be whether a defense of insanity might be raised in relation to a malfunctioning AI algorithm, when its analytical capabilities become corrupted as a result of that malfunction" (HALLEVY, 2010, p.28)

Ainda, dada a sensibilidade e incipiência da temática, é defendida também uma via dogmática mista, tal qual proposto por Fornasier (2020, p. 163):

> Punir criminalmente a AI pode implicar em custos significativos e requer mudanças legais drásticas. Doravante, mudanças modestas nas normas pré-existentes do direito penal que se direcionem aos indivíduos, conjuntamente com o potencial de expansão da responsabilidade civil poderiam constituir melhores soluções para os crimes cometidos com o uso de AI. Uma alternativa condizente poderia envolver a expansão do direito penal incluindo novas tipificações aos crimes de negligência centrados nos designs inapropriados, má operacionalização e ausência de testagem suficiente das aplicações de AI, e possivelmente penas para entes específicos que não cumpram com seus deveres legais, acrescentando-se, por óbvio, um patamar superior de relevância da sujeição civil de seus ofensores.[6]

Persiste ainda uma desconfiança em relação às práticas já implementadas nos ordenamentos jurídicos que fazem uso da tecnologia cibernética, como por exemplo, o uso da jurimetria, na qual são implementados conjuntos de softwares jurídicos para prever resultados e fornecer prováveis resultados de lides com base na probabilidade de manutenção dum precedente (*distinguishing*) ou sua superação (*overruling*). Aliás, a Resolução nº 332/2020, do Conselho Nacional de Justiça do (CNJ) demonstrou uma grande preocupação, em seu artigo 23, ao desencorajar sua utilização em matéria criminal, nos termos até aqui já desenvolvidos de que incorra possível viés discriminatório algorítmico que prejudicaria o réu.

Em verdade, a discussão, mesmo que puramente dogmática sobre as melhores alternativas de consolidação de um regramento que seja conferido de forma universal para os armamentos letais, ainda está absolutamente distante. Considerando uma das caraterísticas basilares do Direito, até que efetivamente esses itens cibernéticos provoquem os judiciários ao redor do mundo com casos concretos, pesquisas de cunho jurídico devem partir de questões universais, tanto política quanto filosoficamente. E por conseguinte, prosseguir fomentando pesquisas futuras que melhor desenvolvam a problemática das LAWS.

Nesse sentido, o exame aqui promovido não se encerra com respostas que adotem uma das alternativas propostas como sendo a ideal, e passaremos a buscar entender em que nível as atuais legislações doméstica e internacional tem se debruçado sobre a regulação das IAs.

---

[6] Trad. Nossa, no original: "The criminally punishing AI can carry significant costs and require radical legal changes. Therefore, modest changes in existing Criminal Law norms that target people, together with potentially expanded Law of Torts, would constitute better solutions for crimes committed with the use of AI. A suitable alternative would involve modest expansions to Criminal Law, including the typification of new crimes of negligence centered on inappropriate design, bad operation and insufficient testing of AI applications, and possible criminal penalties for designated parties that do not comply with legal duties – added, of course, to a greater degree of relevance given the civil liability for those offenses".

CAPÍTULO II. NORMATIVIDADE INCIDENTE SOBRE DRONES E IA, E AS PROPOSTAS DE SUA EVOLUÇÃO SOBRE LENTES JURÍDICAS E INTERNACIONALISTAS

II.1 – A REGULAMENTAÇÃO DE DRONES NO PAÍS: ESTRUTURA E LEGISLAÇÃO CORRELATA

O Sistema da Aviação Civil (SAC) brasileiro vem passando permanentemente por diversas transformações desde sua criação oficial, por intermédio do Decreto nº 65.144 em 12/09/1969. O SAC tem a finalidade de organizar as atividades necessárias ao funcionamento e ao desenvolvimento da aviação civil no país, envolvendo a devida regulação da atividade de Aviação Civil Pública, Privada e de operação dos Aeroportos Civis.

Já promulgada em setembro de 2005, a Lei nº 11.182/2005 criou a ANAC – Agência Nacional da Aviação Civil-, o que só se efetivou em março do ano seguinte, com a edição do Decreto nº 5.731/2006. Por força dos diplomas, a ANAC se consolidou como uma autarquia especial, vinculada à Secretaria de Aviação Civil da Presidência da República (SAC/PR) e dotada de independência administrativa, autonomia financeira, ausência de subordinação hierárquica e mandato fixo de seus dirigentes, com competência para regular e fiscalizar as atividades de aviação civil e de infraestrutura aeronáutica e aeroportuária (artigos 1º, 2º e 4º da Lei nº 11.182/2005). Para tal, o órgão deve observar e implementar as orientações, diretrizes e políticas estabelecidas pelo governo federal, adotando as medidas necessárias ao atendimento do interesse público e ao desenvolvimento da aviação.

Já as prerrogativas relacionadas ao controle do espaço aéreo, investigação e prevenção de acidentes, são respectivamente atribuídos ao Departamento de Controle do Tráfego Aéreo (DECEA), vinculada ao Ministério da Defesa ao Centro de Investigação e Prevenção de Acidentes Aeronáuticos (CENIPA), vinculado à Força Aérea Brasileira. Por fim, a Agência Nacional de Telecomunicações (ANATEL) é responsável pelas certificações dos equipamentos de enlace rádio e pela alocação de espectro. Os módulos transmissores de radiofrequências nos dos drones que incluam tais especificações como veículo aéreo, para a transmissão de imagens requerem certificação emitida pela Anatel.

A atividade regulatória da ANAC está dividida em duas facetas: a regulação técnica e a regulação econômica. A regulação técnica visa a garantia da segurança aos passageiros e usuários da Aviação Civil, confeccionando regulamentos que tratam sobre a certificação e fiscalização da indústria. Isto decorre da necessidade de que as operações aéreas cumpram

rígidos requisitos de segurança, já a regulação econômica diz respeito ao monitoramento permanente do custo de oportunidade de intervenção econômica por parte da agência.

A ANAC criou regras para as operações civis de aeronaves não tripuladas, que estão disciplinados no país por meio do Regulamento Brasileiro de Aviação Civil Especial nº 94/2017 (RBAC-E nº 94/2017) em conjunto com normas de operação de drones estabelecidas pela DECEA e pela Agência Nacional de Telecomunicações (ANATEL).

Pelo regulamento da ANAC, aeromodelos são as aeronaves não tripuladas remotamente, pilotadas para recreação e lazer, e as aeronaves remotamente pilotadas (RPA) são as aeronaves não tripuladas utilizadas para outros fins como experimentais, comerciais ou institucionais.

A ANAC é responsável no país pela regulação da operação da aviação civil. Todos os drones devem ser registrados na ANAC, sendo que atualmente a operação de equipamentos totalmente autônomos não é permitida - seja na legislação brasileira ou internacional. O DECEA, órgão do Comando da Aeronáutica, é responsável pelo controle do espaço aéreo e autorizações de voos. A Estratégia Nacional de Defesa, documento aprovado pelo Presidente da República em 2008, aponta para o emprego de VANTs para aperfeiçoar as capacidades de alerta, vigilância e monitoramento das Forças Armadas. Em particular, a Força Aérea recebeu a incumbência de absorver as implicações desse meio de vigilância e de combate para sua orientação tática e estratégica[7].

II.2 – ANÁLISE DO ARTIFICIAL INTELLIGENCE ACT DA U.E

Discutidas as lacunas jurídicas acerca da temática futura da existência de drones caçadores plenamente autônomos, surge uma segunda indagação. Como anda o processo regulatório pelos itens de automação baseados em IA? Dessa feita, passaremos agora a estudar

[7] As legislações atualizadas referente ao tema são a ICA 100-40 (Instrução sobre "Aeronaves não Tripuladas e o Acesso ao Espaço Aéreo Brasileiro"); ICA 100-12 (Instrução que dispõe sobre as Regras do Ar); MCA 56-5 (Manual que trata de "Aeronaves não tripuladas para uso exclusivo em operações aéreas especiais"); MCA 56-2 (Manual que trata de "Aeronaves não tripuladas para uso recreativo – aeromodelos); MCA 56-3 (Manual que trata de "Aeronaves não tripuladas para uso em proveito dos órgãos ligados aos governos federal, estadual e municipal"); MCA 56-4 (Aeronaves não tripuladas para uso em proveito dos órgãos de Segurança Pública, da Defesa Civil e de Fiscalização da Receita Federal") a RBAC-E94 (Contendo os requisitos gerais para aeronaves não tripuladas de uso civil); RBAC-45 (que trata das marcas de identificação, de nacionalidade e de matrícula de aeronaves no país); IS 94-003ª(contendo os procedimentos para elaboração e utilização de avaliação de risco operacional para operadores de aeronaves não tripuladas) e o Código Brasileiro da Aeronáutico (Lei 7565/1986).

sua normatização e os parâmetros éticos em que elas têm sido desenvolvidas, iniciando pelo Artificial Intelligence Act europeu, reconhecido até o momento como o procedimento mais moderno do mundo acerca desse tema.

Em 13 de março de 2024, foi aprovado no Parlamento Europeu, por ampla maioria, um conjunto de medidas com o fito de regrar a utilização de inteligência artificial na União Europeia. O AI Act, como ficou conhecido esse conjunto de normas, está norteado por sete princípios basilares. Estes incluem: iniciativa e supervisão por humanos; solidez técnica e segurança; privacidade e governação dos dados; transparência; diversidade, não discriminação e equidade; bem-estar social e ambiental e responsabilização. Sem prejuízo dos requisitos juridicamente vinculativos do presente regulamento e de quaisquer outras disposições aplicáveis do direito da União.

Aqui faz-se oportuno transcrever a informação promovida por Schlottfeldt,-no que traz as lições de Mittelstad:

> [...] é necessário ter cautela em torno de princípios, uma vez que eles não seriam suficientes para garantir uma IA confiável ou ética no futuro" O autor entende que sem uma regulamentação, a tradução dos princípios em prática continuará sendo um processo competitivo, não cooperativo. De fato, tem-se argumentado a insuficiência dos princípios como termos viabilizadores de equilíbrio entre proteção de direitos fundamentais e do desenvolvimento econômico-tecnológico, bem como a falta de mecanismos de fiscalização, coibição e mesmo sanções disponíveis aos operadores públicos ou privados dos itens cibernéticos. (Schlottfeldt, 2022, p. 9)

Nesses termos, o regramento do IA Act foi construído metodologicamente através da análise de riscos, classificando os sistemas como de riscos inaceitável ou elevado, dos limitados ou mínimos. Metodologia esta extremante próxima do implementado projeto de Lei nº 2.388/2023 que visa o mesmo objetivo de regulação das AI no país, e que visitaremos no subitem seguinte.

A produção europeia está alinhada com a tendência global de estabelecer uma legislação de inteligência artificial que assegure a transparência e proteja os direitos dos cidadãos, enquanto promove um ambiente de inovação tecnológica saudável e sustentável. O aperfeiçoamento de mecanismos protetivos dessa modalidade efetivamente consistirá em fator de destaque das práticas de governança em torno do desenvolvimento regional, com consequentes reflexos atinentes à soberania e à proteção da segurança nacional.

Nesse contexto, ainda que se considere nosso país em estágio tardio de desenvolvimento das inteligências artificiais, tornou-se imperativo que se desse início ao seu

próprio processo de formulação de estratégias nacionais e políticas públicas de controle da disseminação e operação de IAs, de forma que usualmente emprega-se o uso do modelo comparado como ferramenta que melhor responde sobre tendências e vias normativas de disciplinação de temática inovadora.

Questionamentos sobre como regulamentar algo inovador foram levantados por Baptista e Kellen (2016, p. 204):

> Que desenho e ferramentas regulatórias escolher? Mais ou menos interventiva? Tradicional, do tipo comando e controle, ou se inclinando para modelos regulatórios fracos ou policêntricos? Deve o legislador almejar uma normatização ampla e detalhada de cada inovação e, com isso, teoricamente, aumentar a segurança da sociedade? Ou, ao contrário, optar por uma proposta normativa flexível, de aspecto mais principiológico, permitindo uma capacidade maior de adaptação das normas diante de outras inovações, o que, como contrapartida, aumenta a incerteza quanto à sua incidência.

Autores como Demócrito Reinaldo Filho identificam o claro interesse econômico da Europa em ser vanguardista na produção da regulamentação:

> O objetivo é realmente alcançar uma posição de liderança como "global rulemaker" no processo de regulação de IA. Do mesmo modo como aconteceu com as políticas normativas de proteção de dados pessoais (com a edição do RGPD em 2018[5]), a Europa pretende assumir uma posição de vanguarda e liderança, induzindo a que outros países adotem legislação similar. Pode-se dizer que, sob esse prisma, a UE já alcançou o protagonismo desejado, pois a proposta apresentada é certamente um dos mais abrangentes conjuntos de normas regulatórias sobre IA.. (FILHO, 2021, *n.p*)

Há de se reconhecer que esse tipo de "pioneirismo" está diretamente vinculado ao fenômeno da "quarta revolução industrial" (FILHO, 2021, n.p), que já se encontra incorporada às discussões econômicas e tecnológicas do mundo moderno, nos termos cunhados por Klaus Schwab e defendidos pelo economista alemão-suíço no Fórum Econômico Mundial de 2016, no qual a essa revolução tem se desdobrado no que foi chamado de "transformação digital". Fenômeno em que os negócios, tradicionais ou não, são impactados pelas novas tecnologias com direcionamento em prol da digitalização de todos os setores, sejam públicos ou privados.

Fábio Ribeiro Porto (2016, *n.p.*) descreve ainda como esse fenômeno propicia a democratização do acesso e a eficiência da computação e dos serviços que se utilizam dela. Trazendo consigo novos desdobramentos em maior competitividade, universalização e melhoria de serviços, gerando novo referencial em segurança da informação, em que novos modelos econômicos e de negócios promovem a ruptura de formas de interação e interface com usuários antes homogêneos. Descrevendo como hoje somos simultaneamente espectadores e

protagonistas de uma das maiores transformações da história: o sepultamento da era analógica e o surgimento da era digital.

Nesse sentido, resgata que a: “sociedade evoluiu tanto que até as necessidades básicas dos seres humanos mudaram. Na base da famosa pirâmide de Maslow agora, mais do que as necessidades fisiológicas, estão a ansiedade por energia e wi-fi” (Picolli, 2021,p. 192).

Retornando ao diploma em questão, Schlottfeldt a enquadra dentro do contexto internacional, na superação anterior das iniciativas nacionais de regulação da IA que tradicionalmente vinham sido direcionadas para a elaboração de molduras éticas; salvaguarda de padrões técnicos e abordagens tecnológicas/proteção sistêmica; boas práticas e códigos de conduta, normalmente referidos como *soft law*. Considerando-a pioneira no sentido de propositura de regulamentações e de legislações (as chamadas *hard laws*), à medida que os formuladores de políticas e atores de IA em todo mundo que parte dos princípios à implementação de normativos sobretudo de forma a mitigar os riscos como a IA poderá avançar sem que seja regulada.

Muito embora a farta literatura descreva essa natureza de esforço regulatório como elemento que pode desencorajar o estímulo por inovações, na verdade, ao disciplinar padrões claros e esperáveis, pode-se, de fato, incentivar a inovação, ao definir-se “minimamente as regras do jogo” e com isso garantir segurança jurídica de entrantes e novos modelos de negócios. A inexistência de regulação favorece os grandes agentes que já implementaram seus modelos de negócio ou que podem suportar os custos de mudanças regulatórias no curso de suas atividades dificultando ou impedindo uma dinâmica de concorrência saudável entre agentes, como menciona Ana Frazão (2021, *n.p.*) em coluna publicada no ano de 2021.

Sob esse desiderato, a proposta de regulação da IA na UE foi se delineando e amadurecendo por mais de 5 anos, em idos de outubro de 2017, o Conselho Europeu destacou a premência em fazer frente às tendências emergentes, como a IA, “com a garantia simultânea de um elevado nível de proteção dos dados, direitos digitais e normas éticas”, instando a Comissão Europeia a apresentar uma abordagem europeia da IA (Conselho europeu, 2017, p. 8).

Em junho de 2018, foi proposta a criação de grupo de especialistas para fornecer conselhos sobre sua estratégia de IA, o Grupo de Peritos de Alto Nível sobre IA, encarregados da tarefa de coordenar um grupo de trabalho capaz de oferecer vias normativas que trouxessem:

(1) competitividade da Europa no panorama da IA; (2) preparo a UE para as mudanças socioeconômicas; (3) garantia um quadro ético e jurídico adequado.

Num período de dois anos, o Grupo trabalhou nos seguintes produtos: (1) Diretrizes Éticas para IA confiável: apresentando uma abordagem em IA centrada no ser humano e lista sete requisitos que os sistemas de IA deveriam atender para serem considerados confiáveis; (2) Recomendações de política e investimento para IA confiável: baseado no primeiro produto, o grupo apresentou 33 recomendações para sustentabilidade, crescimento, competitividade e inclusão; (3) Lista de Avaliação para IA confiável (Assessment List for Trustworthy AI – ALTAI): ferramenta que traduz as Diretrizes Éticas em um checklist de autoavaliação acessível e dinâmico; (4) Considerações Setoriais sobre a Política e Recomendações de Investimento: explora a possível implementação das recomendações publicadas anteriormente pelo Grupo em três áreas específicas: (i) setor público; (ii) saúde; (iii) fabricação & internet das coisas (SCHLOTTFELDT, 2022, p. 12).

Na sequência, foi criada a "Aliança Europeia para a IA", um fórum online com mais de 4 mil membros representando academia, empresas e indústrias, sociedade civil, cidadãos da UE e formuladores de políticas. O GPAN trabalhou em estreita colaboração com a Aliança Europeia para a IA, e seus produtos - documentos de políticas, trabalhos acadêmicos e discussões publicados no fórum, ajudaram a definir os produtos do GPAN. Por sua vez, as recomendações do GPAN serviram como subsídio para as iniciativas de formulação de políticas tomadas pela Comissão e seus Estados-Membros nas etapas subsequentes da definição do diploma.

As etapas seguintes contaram com a publicação de um *whitepaper*[8] contendo opções políticas para se alcançar o "duplo objetivo de promover a adoção da IA e de abordar os riscos associados a determinadas utilizações desta nova tecnologia", buscando o fomento de: (i) um "ecossistema de excelência", apto a apoiar o desenvolvimento e a utilização da IA na economia e na administração da UE; bem como (ii) um "ecossistema de confiança" calcado em um quadro regulamentar sólido, capaz de evitar uma fragmentação no mercado interno, mirando em objetivos de fiabilidade, segurança jurídica e aceitação pelo mercado (Comissão europeia, 2020, p. 1, 3, 5, 11). Nele, os principais riscos inicialmente identificados diziam respeito à aplicação de regras de proteção dos direitos fundamentais (e.g., dados pessoais; proteção da privacidade;

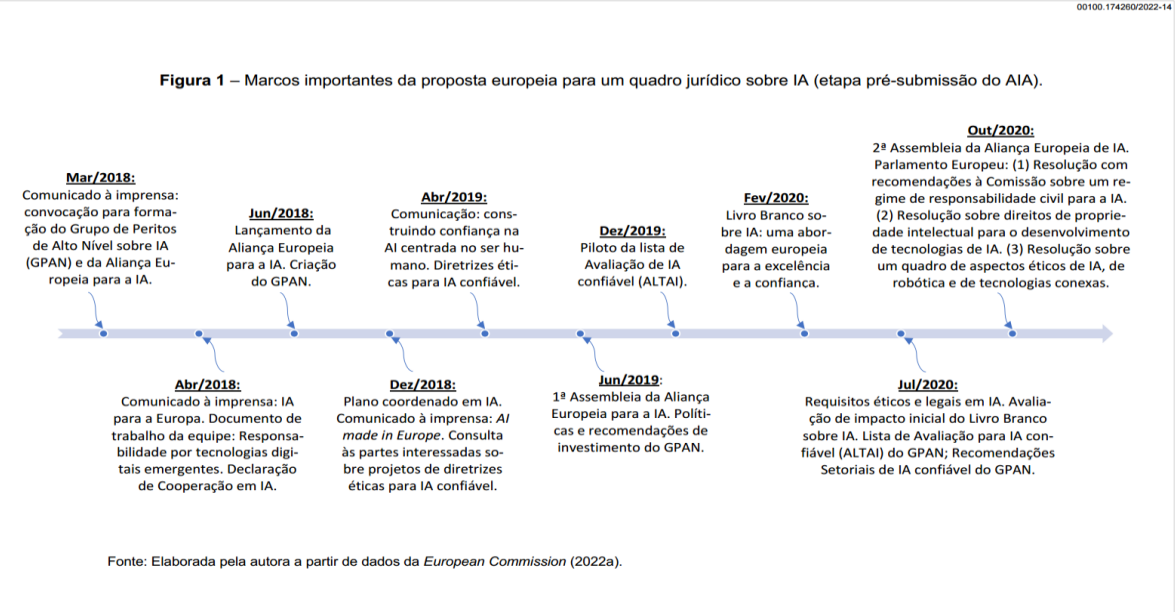
[8] Livros Brancos contêm propostas oficiais de medidas numa área específica, servindo como veículo para o debate da Comissão com o público, as partes interessadas, o Parlamento e o Conselho, a fim de facilitar um consenso político no desenvolvimento de uma proposta legislativa (Parlamento Europeu, 2020, p. 7).

liberdade de expressão; liberdades políticas; não discriminação), bem como questões de segurança e de responsabilidade (Council of europe, 2018; Comissão europeia, 2020, *n.p*).

Na sequência da publicação do livro branco, ocorreram por três anos diversas audiências públicas, tendo uma inclusive ocorrido de forma remota por força da epidemia mundial do Covid-19, todas voltadas a debater as principais conclusões da Consulta Pública sobre o Livro Branco e as perspectivas futuras na construção de uma abordagem europeia de excelência e confiança na IA.

Schlottfeldt (2022, p.14) elaborou uma linha cronológica que exprime os principais marcos preparatórios para apresentação da proposta de um quadro jurídico sobre IA na EU e está aqui reproduzida:

Figura 1 - Marcos importantes da proposta europeia para um quadro jur jurídico sobre IA (etapa pré-submissão do AIA)



Fonte: SCHLOTTFELDT (2022, p.16)

O AI Act busca construir um quadro jurídico europeu para a IA, com regras garantidoras dos direitos fundamentais, capazes de abordar os riscos gerados por utilizações específicas da IA através de um conjunto de regras complementares, proporcionadas e flexíveis. A Comissão vislumbra que essas regras têm o potencial de conferir à Europa um papel de liderança na definição do padrão-ouro global. Quanto a isso, pode-se dizer que o AIA é uma das medidas regulatórias mais influentes tomadas até agora internacionalmente, e preparada para abranger os desenvolvimentos tecnológicos de IA atuais e futuros.

Ainda de acordo com Schlottfeldt (2022, p.16), “[t]rês categorias de requisitos parecem particularmente pertinentes às principais preocupações da literatura em torno da IA na tomada de decisões que afetam os seres humanos,” a saber: (1) erro algorítmico, viés e discriminação; (2) tomada de decisão automatizada como contrária à dignidade humana; e (3) opacidade/falta de explicações.

Remediando essas preocupações: Os sistemas de risco limitado (Título IV, art. 52º, AIA) estarão sujeitos a um conjunto limitado de obrigações de transparência.

Por fim, sistemas de risco baixo (Título IX, art. 69º, AIA), categoria na qual a grande maioria dos sistemas de IA se enquadra, não serviriam ao desiderato de intervenção do AIA face a um risco mínimo ou nenhum risco para os direitos ou a segurança dos cidadãos.

Todavia, apesar de toda a robustez e seriedade até aqui descritas ao longo de toda a tramitação do AIA, próximos ao início de sua vigência, na data próxima de 2 de fevereiro de 2025, ainda persistem uma série de problemáticas não abarcadas pelo diploma, e pelas empresas que terão até meados do próximo ano para adaptarem as suas políticas internas à maioria das disposições da Lei da EU. Ocorre que a proibição de sistemas considerados de risco devido ao seu impacto negativo na sociedade também prevê algumas exceções quando o interesse público supera o risco potencial.

Caterina Rodelli, analista de políticas da UE na organização global de direitos humanos - Acess Now, é cética em relação a estas exceções: "se uma proibição contém exceções, deixa de ser uma proibição". (Paula Soler, 2025, *n.p)*

As principais exceções em comento versam principalmente em torno do uso de autoridades responsáveis pela aplicação da lei e pela migração, permitindo-lhes utilizar sistemas pouco fiáveis e perigosos, como detectores de mentiras, aplicações de policiamento preditivo ou sistemas de definição de perfis nos procedimentos de migração, incorrendo nas principais problemáticas descritas por Pedro Sousa (2022, *passim*) em torno da desconfiança de padrões discriminatórios por parte desses algoritmos.

Uma segunda problemática diz respeito à operacionalização da fiscalização do AI Act por parte dos Estados-membro da UE, que terão até agosto deste ano para criar as suas entidades reguladoras nacionais. Até então, pouco ou nada se sabe em vários países sobre as autoridades de fiscalização do mercado ou sobre os organismos notificados que irão supervisionar as regras a nível nacional.

Estabelecido o panorama da aprovação e da implementação do AI Act, seguiremos no próximo item buscando compreender as convergências que a proposta brasileira guarda com essa legislação.

II.3 – O projeto de Lei nº 2.388/2023 – que regulamenta a produção e operação de inteligências artificiais no Brasil foi aprovado pelo Senado Federal em votação simbólica no dia 10 de dezembro de 2023. Presentemente, o texto segue sua tramitação na Câmara dos Deputados. Sob autoria do Presidente da casa – Rodrigo Pacheco, sua implementação futura visa garantir segurança jurídica e ética no uso da tecnologia, além de proteger os direitos fundamentais, com destaque para os direitos autorais.

O PL apresenta a criação do Sistema Nacional de Regulação e Governança de Inteligência Artificial, incluindo o país na sistemática das melhores práticas internacionais em discussão. O texto substitutivo segue agora para análise na Câmara dos Deputados, onde será discutido, votado e, se aprovado, sancionado pelo presidente da República. Conforme expresso de seu Art. 1º:

> Esta Lei estabelece normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial (IA) no Brasil, com o objetivo de proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico. – PL nº 2338/2023. (BRASIL, 2023, *n.p.*)

Conforme documento da Autoridade Nacional de Proteção de Dados (2024, p. 3) contendo seu posicionamento em relação a proposta em tramitação da regulação das AI no Brasil, a perspectiva desde a propositura do PL nº 21/2020 evolui com a Comissão de Juristas no Senado Federal, tendo elaborado um substitutivo sobre inteligência artificial (CJSUBIA) em 2022 que já realizou diversas audiências públicas. Estas contaram com a participação de mais de 50 especialistas, em formato multissetorial, contando com a participação de representantes do poder público, setor empresarial, sociedade civil e da comunidade científico-acadêmica.

O resultado dessas discussões consolidou um relatório de 900 páginas, gestando um anteprojeto de lei que, em 03 de maio de 2023, foi convertido no PL nº 2338/2023 em comento. Nele, a avaliação dispõe a prerrogativa de interação com a Lei Geral de Proteção de Dados, já em vigência, sob desiderato de estabelecer mecanismos de governança sobre a IA, além de tutela de direitos, e trabalhar classificações de sistemas de IA de alto-risco, existe ainda

elemento interessantíssimo de fomento a implementação de *sanboxes regulatórios*[9] da qual se esperam ambientes experimentais voltados à inovação responsável.

O documento está fracionado em itens que serão aqui reproduzidos em nossos próprios termos para melhor delimitar o estado da arte da mencionada proposição legislativa.

Inicialmente, apresenta-se os postos de contato entre o projeto e a LGPD.

A justificativa do PL nº 2338/2023 propõe um modelo regulatório escorado em uma abordagem baseada na tutela de direitos e princípios fundamentais – o denominado *rights-based approach* – aliada a metodologia por meio do risco – *risk-based approach*, de forma complementar que delimita e proíbe a um só tempo o desenvolvimento de sistemas de IA de risco excessivo, resguardando direitos às pessoas mais afetadas pela implementação dessa natureza de programa.

O principal aproveitamento dessa metodologia regulatória é da constituição de mecanismos de governança – tal qual obrigação de que sejam elaborados relatórios de impacto à proteção de dados pessoais (RIPD) pelo controlador de dados nos termos do Art. 5º, XVII, da LGPD.

Em relação ao PL de uso das AI, cita-se a avaliação de impacto algorítmico possibilitando simultaneamente o controle da atividade e os pontos de convergência entre eventuais sobreposições e conflitos com as atribuições legais da própria entidade da ANPD quando sistemas de IA realizarem tratamento de dados pessoais, quais sejam "(i) direitos da pessoa afetada por sistema de IA e os direitos dos titulares; (ii) a correlação entre sistemas de IA de alto risco e o tratamento de dados pessoais; e (iii) mecanismos de governança". (ANPD, 2024, p. 3).

Novamente em alusão à LGPD, o PL de uso das IA guardou especial proximidade dos "direitos à informação, à explicação, e à contestação e de solicitar revisão", abrindo uma convergência bem como a possibilidade de conflito entre as normas. Desta feita, ao propor a obrigatoriedade de que haja contratualmente uma limitação de responsabilidade que informe ao usuário sobre (i) o caráter automatizado da interação com o sistema, (ii) sua descrição geral, e (iii) os tipos de decisões, recomendações ou previsões que se destina a fazer e consequências de sua utilização para a pessoa, com menção à identificação dos operadores do sistema de IA e

[9] Sandboxes regulatórios são ambientes regulatórios experimentais, funcionando como colaborações que reúnem reguladores e organizações que desenvolvem novas tecnologias e processos para testar as inovações em relação à estrutura regulatória.

informação sobre medidas de governança adotadas no desenvolvimento e emprego do sistema, a tutela do PL se esbarra no disposto no Art. 9º da LGPD que assegura aos seus titulares o acesso facilitado às informações sobre o tratamento de seus dados.

Há também o direito de contestação e de solicitar revisão, no qual o texto do PL possui direta correspondência com o direito de solicitar a revisão de decisões automatizadas previsto no Artigo 20º da LGPD. A tensão provocada vai de encontro a sobreposição entre a exigibilidade de "efeitos jurídicos relevantes" ou que "impactem de maneira significativa os interesses da pessoa" (Art. 9º, § 1 E §2 do PL). Já a previsão normativa da LGPD estabelece que o direito de revisão se aplica em hipóteses de "decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses", a exemplo do que ocorre nos casos de perfilamento.

Como depreende-se do texto, o projeto de lei estipula requisitos mais restritos que os da LGPD, sem mencionar razão pela qual a ANPD pugna pela menção de respeito às normas do último diploma como forma de restabelecer a compatibilidade jurídica entre os regramentos, ressalvando que o tema já lhe é afeto.

Já relativo ao princípio da não discriminação, considera-se que a despeito da menção deste mesmo como (art. 2º, V) e direito (art. 5º, V) do PL, no

> [...] contexto da revisão de decisões automatizadas, conforme o art. 20, §2º, da LGPD, a ANPD possui competência para realizar auditorias com o objetivo de verificar se existem aspectos discriminatórios no tratamento automatizado. (ANPD, 2024, p. 4)

Por fim, a redação dada pelo PL, ao discorrer sobre a discriminação, esbarra-se diretamente aos efeitos discriminatórios e aos usos ilegítimos e abusivos dos dados de pessoas sensíveis, definidos no Art. 5º, II da LGPD; Logo, a avaliação de riscos associados ao tratamento de dados de igual forma se esbarra na competência do ente.

Guardando larga similitude com as disposições presentes do AIA, pode-se encontrar no PL as delimitações de risco excessivo e risco alto, justificando diferentes níveis de restrições, garantias e balizas atinentes ao grau qualificado pela IA, podendo chegar ao patamar proibitório ao alcançar a categorização de riscos inaceitáveis. Há clara definição de um rol de finalidades de uso categorizadas de alto risco, delegando o processo ubíquo de sua atualização por meio de critérios específicos direcionados à autoridade competente. (Senado Federal, 2021, p.11).

Aqui estão categorizados os dados sensíveis como daqueles sistemas de IA que envolvem o tratamento de dados pessoais porque esses estão projetados para tomar decisões

automatizadas que podem ter impacto significativo em interesses de direito individual, dos quais se citam decisões relacionadas a crédito, emprego e segurança pública e de saúde. A ver:

> Salienta-se que dois dos critérios estabelecidos pelo PL para que a autoridade competente atualize as listas dos sistemas de IA de risco excessivo ou de alto risco envolvem expressamente a utilização de dados pessoais: (i) alto nível de identificabilidade dos titulares dos dados; e (ii) quando existirem expectativas razoáveis do afetado quanto ao uso de seus dados pessoais. (BIONI *et al.*, 2023, p.5)

Dessa forma, estabelecem que sejam monitorados ao longo dos ciclos de vida dos sistemas de IA para garantir a conformidade com os direitos humanos e direitos fundamentais, tanto no aspecto privado quanto nos direitos difusos, vez que grupos que eventualmente estejam sujeitos às decisões desses poderiam ter seu direito à não discriminação violados em termos de privacidade, proteção de dados pessoais e até mesmo o acesso a determinados benefícios sociais em decorrência de decisões automatizadas.

Comparando brevemente as referidas leis, é possível observar seu paralelismo acerca da instituição de programas de governança mediante códigos de conduta de agentes de IA (Art. 30º do PL), muito próximos ao programa de governança em privacidade da LGPD. Para ambos, se sobressai a clara escolha de política legislativa em favor da autorregulação regulada, funcionando em torno da adoção de padrões fixados pelo Estado, mas com flexibilidade das plataformas em materializá-los e implementá-los. A maior virtude desse modelo é de promover aos próprios agentes regulados a atitude preventiva e de antecipação de riscos de seus sistemas.

Além disso, outro instrumento análogo à LGPD é apresentado pelo PL das IAs: da **avaliação de impacto algoritmo (AIA),** cuja metodologia de funcionamento é descrita em quatro etapas: "(i) preparação; (ii) cognição do risco; (iii) mitigação dos riscos encontrados; e (iv) monitoramento. Como toda avaliação de impacto, trata-se de uma ferramenta que permite ao agente descrever características do sistema analisado, bem como identificar riscos e mecanismos para sua mitigação" (ANPD, 2024, p. 7).

Esse é o instrumento irmão do RIPD, e demanda a descrição dos tipos de dados coletados, da metodologia de coleta e análise do controlador incidente sobre a sistemática de anonimização da informação coletada. Mais uma vez são levantadas situações que demandaram a implementação simultânea dos institutos, a exemplo das tecnologias de reconhecimento facial e aplicações de IA na área da saúde.

Dessarte, resta nítido que, seja qual for a autoridade supervisora das IAs no país, ela deverá estar alinhada às atividades da ANPD, garantindo que os instrumentos de regulação estejam em plena consonância com os elementos já vigentes da LGPD.

Assim, resta imperativo que a implementação da Lei, caso aprovada na Câmara dos Deputados, zele da mesma preocupação sistêmica dos legislativos e regulatórios descritos no *AI Act* na jurisdição brasileira. Por consequência as sobreposições das regras propostas pelo PL nº 2338/2023 com a LGPD, demandaram ao mesmo tempo o fomento à inovação que passa a ser peça-chave do debate regulatório de novas tecnologias, desde que esse fomento promova o desenvolvimento de inovações responsáveis com limites bem margeados de respeito aos direitos fundamentais e coletivos.

De igual modo, espera-se aqui a adoção do modelo estrangeiro de fomento de *sandboxes* para testagem das regulações futuras, contendo as características mínimas de inovação no emprego de tecnologia ou uso alternativo daquelas já existentes e aprimoramentos de eficiência, redução de custos, aumento de segurança atrelado à diminuição de riscos e, sobretudo, de um plano de descontinuidade, com previsão de medidas que assegurem a viabilidade operacional do projeto, findo o período de autorização do *sandbox*.

Esse último elemento garante responsabilidade dos operadores por quaisquer danos infligidos a terceiros em resultado da experimentação que ocorra no ambiente de testagem.

Por fim, quanto à competência fiscalizatória prevista no Art 32º, VII, do PL, são preementes dois temas convergentes entre a proposta legislativa e a LGPD: (i) comunicação de incidentes de segurança e (ii) sanções administrativas. O primeiro impõe a obrigatoriedade de comunicação em caso da "ocorrência de graves incidentes de segurança, incluindo quando houver risco à vida e integridade física de pessoas, a interrupção de funcionamento de operações críticas de infraestrutura, graves danos à propriedade ou ao meio ambiente, bem como graves violações aos direitos fundamentais" (ANPD, 2024, p. 11) - (Art. 31º), submetidos ao regime de direito administrativo sancionador aplicáveis aos agentes infratores da normativa de proteção de dados ou dos preceitos do Projeto de Lei.

Por conseguinte, a eventual criação de um novo órgão regulador ou a atribuição de competências a entidade diversa da ANPD incorreria no risco de gestar uma fragmentação regulatória, suscitar questionamentos legais em casos concretos em que um agente possa ser sancionado por ambas as entidades regulatórias e urgência de convergência regulatória nos

elementos já objetos de proteção de dados pessoais cuja Autoridade Nacional de Proteção de Dados já é titular.

O final do parecer da ANPD sugere centralizar a garantia da proteção de dados e da privacidade com a governança em matéria de AI como sendo a melhor alternativa para a sustentação da segurança jurídica pelo diploma, assegurando a uniformidade regulatória entre temas fortemente entrelaçados, lembrando ainda o valor econômico de diminuir os custos de operação da adequação exigida pelo regramento, com efeitos de potencializar a confiança dos agentes regulados e da população geral no uso de sistemas de IA.

Nesses termos, citam nota conjunta pela Autoridade Europeia de Proteção de Dados (European Data Protection Supervisor – EDPS, no original) e pelo Comitê Europeu de Proteção de Dados (European Data Protection Board – EDPB, no original) em que

> Elas esclarecem que designar a autoridade de proteção de dados como autoridade supervisora de IA é uma estratégia que assegura não só harmonia na regulamentação, como também uma interpretação coerente das disposições perante os sujeitos regulados. Dessa forma, se posicionam no sentido de que é a melhor escolha a se fazer. (ANPD, 2024, p.13)

II.3 – UMA BREVE PONDERAÇÃO DE MODELO COMPARADO

Uma vez situados no corpo dos regramentos desenvolvidos nos dois itens anteriores, o penúltimo tópico deste trabalho cuidará de promover um modelo comparado com a finalidade de melhor desenvolver os elementos presentes nos mecanismos de avaliação de impacto algorítmico e risco contextual de IA dentro do campo regulatório assimétrico.

Como visto em seção anterior, o PL nº 2338/2023 foi elaborado após emissão de um relatório Final das atividades da CJSUBIA com mais de 900 páginas, o que incluiu, além do histórico de suas atividades e os processos de participação pública externalizados nas contribuições escritas, audiências públicas e seminário internacional, a minuta de substitutivo aos Projeto de Leis n.º 5.051/2019, 21/2020 e 872/2021.

Foi considerado um grande passo na evolução da discussão do tema, após grande crítica de seu predecessor, aprovado em tramitação em regime de urgência, o PL 21/20, especialmente pela comunidade acadêmica que considerou a falta de maior debate e participação pública sobre a referida proposta. Vez que o processo de aprovação do PL 21/20 na Câmara dos Deputados em 2021 deixou de aproveitar de ferramentas de participação pública disponíveis, que não apenas audiências públicas, como é o caso de consultas públicas,

permitindo maior colaboração para pessoas e grupos que não tiveram voz durante as audiências realizadas, dando maior legitimidade ao processo legislativo.

Após análise prévia do projeto de lei n º 2388/23, principalmente norteada por nossa própria lei pátria em torno dos mecanismos já consagrados pela LGPD, passamos a proceder numa análise de modelo comparado, com a finalidade de mapear o nível de convergência da proposta brasileira com a de outros países e organismos multilaterais e internacionais. Espera-se, com esse fito, desenvolver uma análise qualitativa que abarque a racionalidade regulatória de intersecção de um movimento global em governança de IA.

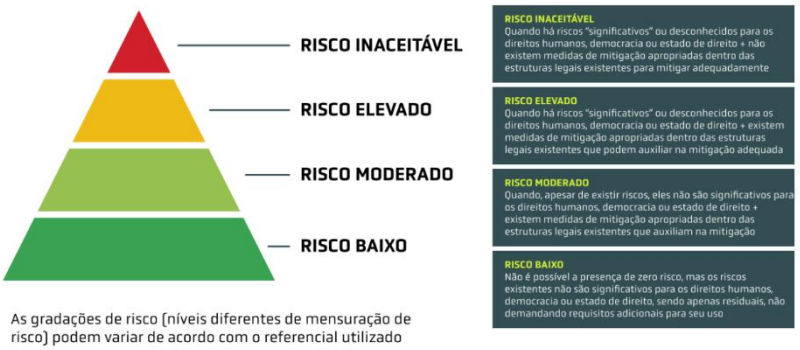
Cumpre destacar que a iminente aprovação da Lei geral dos AI não exclui a possibilidade concomitante de estabelecimento de regulação setorial a partir de fundações comuns a diferentes setores com potencial de catalisar o desenvolvimento tecnológico, econômico e social num modelo de inovação responsável.

Inicialmente, cita-se o modelo escolhido pelo PL nº 2338/2023 como sendo de regulação assimétrica baseada no risco, isso faz com que os "esforços regulatórios e as obrigações de governança não sejam iguais para todos os casos de uso, mesmo que em um mesmo setor, nem mesmo para todos os atores da cadeia de IA" (Bioni, 2023, p. 6). Grande parte desse estudo foi baseada nas notas técnicas confeccionadas pela associação Data Privacy Brasil de pesquisa, a qual passamos agora a visitar.

A pesquisa desenvolvida pela entidade buscou avaliar as propostas de regulamento de IA da União Europeia, da OCDE, UNESCO, Canadá, Conselho da União Europeia e até mesmo dos EUA, reconhecendo como em todas, e como tendência global, seus objetos mensuram proporcionalmente o grau de intervenção regulatória de acordo com o nível de risco de dada Inteligência Artificial aqui cunhado pelo conceito do – **Risco Contextual de IA.**

Por essa razão, a gradação de riscos pode ser atribuída à uma pirâmide, que vai desde os níveis de baixo risco – demandando menor grau de intervenção, de riscos moderados e elevados, demandando a imposição de uma série de deveres para que determinada tecnologia seja implementada, até a de riscos inaceitáveis, em que determinados itens de automação são peremptoriamente proibidos, em virtude do alto grau de comprometimento de direitos fundamentais ou de ameaças de corrosão do Estado de Direito. Conforme a imagem abaixo (Bioni *et al.*, 2023, p. 45):

Figura 2 - Graduações de risco



Fonte: Dataprivacy.org – Temas Centrais de Regulação de IA

Dos institutos analisados, o PL 2338/23 é o único que realiza tal divisão ao criar as categorias de risco excessivo e alto, sendo que tais denominações variam de forma contextual dado o escopo, nível de automação, grau de explicabilidade da AI, potencial de pessoas afetadas, quantidade de dados tratados, entre outros elementos da AI regulada. A importância desse modelo se dá ao proporcionar, por meio da definição de critérios, um consequente grau de segurança jurídica para os agentes regulados, ao evitar o excesso de generalismo regulatório.

Esse critério preenche de forma muito mais satisfatória, ainda que sem clara indicação de mecanismos de governança, ao menos uma indicação no tratamento da problemática de desenvolvimento de drones caçadores automáticos, que pela gravidade potencial de lesão de Direitos se enquadraria como de risco inaceitável.

II.4 – EIXO 1 – REGULAÇÃO BASEADA NO RISCO

Sobre a regulação de novas tecnologias, BIONI *et al.* (2023, p. 45) apresentam como premissas metodológicas do contexto de elaboração e supervisão continuada do modelo regulatório das IAs os três seguintes eixos: (i) regulação baseada no risco; (ii) avaliações de impacto algorítmico; (iii) IA Generativa.

A justificativa da escolha desses eixos temáticas é apresentada por centrarem os elementos fundantes do equilíbrio entre regulação baseada em riscos e em direitos. Neste trabalho serão analisados somente os dois primeiros eixos, conquanto a temática da IA

Generativa não tenha sido incluída das leituras prévias ou analisadas ao longo das seções anteriores.

Inicialmente é apresentado o conceito de risco como uma ferramenta que auxilia o processo de tomada de decisão, direcionando sua análise não para sua existência presumida, mas para o quanto de risco determinado agente é capaz ou está disposto a assumir e quanto é capaz de mitigar. (Gellert, 2020, pp. 245-271)

Desse corolário, conclui-se que nesse diapasão estão envolvidas "duas operações distintas, porém unidas: previsão do futuro (com a ajuda de números) e a tomada de decisões com base nisso. Assim, o risco, embora associado a algo mais quantificável, também pode ser entendido como um elemento qualitativo e valorativo que necessita ser avaliado considerando diferentes perspectivas" (Bioni *et al.*, 2023, p.25).

Apresenta-se, então, o modelo de regulação de risco originado no direito administrativo dos EUA nos anos 1960-1980, para regular questões de saúde, segurança e ambientais que tem como características a definição formal e quantitativa de risco e análises de custo-benefício, onde os potenciais danos deveriam ser conhecidos e medidos para que fossem ou regulados ou banidos.

Almejando a garantia do cumprimento das legislações de proteção de dados, o AI Act apresenta, por exemplo, no Art. 54º, o rol de requisitos para posterior tratamento de dados pessoais com finalidade diversa da original em *sandboxes* de IA. Além de limitar o tratamento do escopo com continuidade após o prazo de experimentação regulatória, estão previstas várias salvaguardas, como a existência de mecanismos de monitoramento eficazes para identificar riscos de direitos fundamentais dos titulares dos dados e isolamento dos ambientes de tratamento de dados pessoais durante a experimentação.

Ademais, a proposta europeia prevê no Art. 53º que as Autoridades de Proteção de Dados (APDs) devem estar envolvidas nos *sandboxes*, independentemente de serem designadas como autoridade competente da IA, quando a inovação em teste envolver o tratamento de dados pessoais. Essa proposta torna as APDs guardiãs dos *sandboxe*s regulatórios de IA na UE e é compatível com iniciativas que já vêm sendo realizadas no contexto europeu e já mencionadas em seção anterior, e aqui servem como exemplificativo do produto da probabilidade e da severidade de sua consequência para definir o quanto de risco é "aceitável" na prática em troca dos benefícios potencialmente gerados. Esse modelo demonstra a assertividade de vincular a

mitigação de riscos à estrutura muito rica de supervisão democrática de problemas que afetam toda a população.

As várias designações de modalidades de risco, trazem consigo diferentes modalidades de controle, e assim o "que se observa é que a análise de risco e mitigação pode ser realizada em um nível micro (da empresa e de um setor, por exemplo) ou no nível macro (como nos mercados em geral de forma mais transversal, com participação e intervenção do estado)." (BIONI *et. al.*, 2022, p.28).

No caso específico da proteção de dados pessoais, cita-se o Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection Regulation – GDPR) que prevê uma versão flexível da regulamentação responsiva às entidades reguladas e alocando os recursos de fiscalização dos reguladores por risco. Em outras palavras, a abordagem baseada em riscos afeta quais são as obrigações dos controladores em cada caso concreto, o que faz com que a lei de proteção de dados se aplique de forma diferente a depender do nível de risco de determinada atividade (BIONI *et. al.*, 2022, p.28).

Dessarte, a partir da mensuração do grau de risco, consideradas a severidade e probabilidade, as obrigações de cada um dos controladores são parametrizadas com mais ou menos obrigações, direitos e deveres – quanto maior o risco, maior a carga obrigacional. Essa avaliação, em situações de alto risco, é, por exemplo, consubstanciada na obrigação de elaboração de mecanismos de governança, como será descrito na análise promovida pelos autores no eixo 2.

O PL 2338/23 alia duas abordagens diferentes: baseada em direitos e em risco. A abordagem baseada em direitos permite a tutela dos direitos fundamentais do usuário que poderia ser impactada por sistemas de inteligência artificial, "ao mesmo tempo em que a abordagem baseada em risco, ao regulamentar a governança dos sistemas de inteligência artificial, garante previsibilidade e segurança jurídica para inovação e o desenvolvimento tecnológico". A ver:

> Estruturalmente, a proposição estabelece uma regulação baseada em riscos e uma modelagem regulatória fundada em direitos. Apresenta ainda instrumentos de governança para uma adequada prestação de contas dos agentes econômicos desenvolvedores e utilizadores da inteligência artificial, incentivando uma atuação de boa-fé e um eficaz gerenciamento de riscos.(Senado Federal, 2023,p.30)

É então descrito como o modelo adotado PL 2338/23 está em consonância com as iniciativas mais recentes de regulação de IA de *internacionais* para adaptar as obrigações dos agentes dos sistemas de IA. Existem direitos básicos que se aplicam a qualquer interação entre o sistema de IA e um ser humano (conforme Art.5, I, II, IV, V e VI, Art.7, Art.8, Art. 12) na toada de uma regulação baseada em direitos, como informação e transparência. Entretanto, há mais obrigações quando há um maior risco a direitos (Art. 5, III, Art. 9, Art. 10, Art. 11). Da mesma maneira, as medidas de governança dos sistemas de inteligência artificial também são divididas de acordo com o risco:

> Além de fixar direitos básicos e transversais para todo e qualquer contexto em que há interação entre máquina e ser humano, como informação e transparência, intensifica-se tal obrigação quando o sistema de IA produz efeitos jurídicos relevantes ou impactem os sujeitos de maneira significativa (ex: direito de contestação e intervenção humana). Assim, o peso da regulação é calibrado de acordo com os potenciais riscos do contexto de aplicação da tecnologia. Foram estabelecidas, de forma simétrica aos direitos, determinadas medidas gerais e específicas de governança para, respectivamente, sistemas de inteligência artificial com qualquer grau de risco e para os categorizados como de alto risco. (Senado Federal, 2023, p. 30-31)

A flexibilidade do enquadramento perante as medidas de governança de acordo com o risco de determinado sistema de IA, em um contexto específico, assemelha-se à regulamentação baseada em risco originada no Reino Unido e à abordagem do EU AI Act. É o que faz, por exemplo, o PL 2338/23 ao prever que, além de haver a necessária designação de uma autoridade competente (art. 32, caput) que este órgão regulador deverá cooperar com outros de competências correlatas para cognição e gerenciamento de riscos (Artigo 32, incisos V, VII e VIII).

Ainda, o PL 2338/23 diferencia-se qualitativamente das demais propostas regulatórias nacionais ao prever um capítulo para governança e boas práticas de modo a incentivar que os próprios agentes econômicos gerenciem os riscos das suas próprias atividades econômicas, na já mencionada modalidade de autorregulação regulada. Dessa forma, a partir dos documentos comparados, destaca-se o alinhamento do PL 2338/23 do Brasil às discussões internacionais, não apenas vindas do contexto europeu, mas de padrões globais, a exemplo da OCDE e UNESCO.

Essa estratégia de regulação e designação macro de faixas de risco foi adotada por diversas normativas regulando sistemas de inteligência artificial: o PL 2338/23 no Brasil, o EU AI Act, e o Proyecto de ley 15869/19 do Chile. De Igual forma, cita-se a ferramenta de avaliação

de impacto do Canadá (Canada's Algorithmic Impact Assessment tool no âmbito da Diretiva sob retomada de Decisão Automatizada do Canadá).

No PL das AI o risco é dividido em três faixas: excessivo, alto e moderado/baixo (categoria residual, não explicitada na legislação). Não há uma definição de cada categoria do risco, uma vez que o risco é classificado a partir de um rol exemplificativo, com previsão de elementos quantitativos e qualitativos para atualização do rol de sistemas de risco inaceitável e alto pela autoridade competente, conforme artigo 18.

Já na AIA, que também o divide em três faixas, o nível mais alto de risco é denominado inaceitável. A faixa de risco mais baixa da mesma maneira não é explicitada pela legislação, sendo uma categoria residual. O mesmo ocorre no projeto chileno 15869-19, que divide o risco em inaceitável e alto, além da categoria residual dos sistemas não classificados pelos dois níveis de risco

A ferramenta canadense se difere das anteriores, contendo em 4 níveis. Cada nível tem uma faixa percentual de impacto, a depender da reversibilidade das decisões automatizadas e da duração esperada da decisão tomada. Nesse sentido, decisões reversíveis e breves são de pouco impacto (nível I) e decisões irreversíveis e perpétuas são de muito alto impacto (nível IV).

Além do contexto, outros elementos podem ser utilizados como critério para definição do grau de risco, a exemplo do escopo, explicabilidade, quantidade de dados processados, nível de automação, dentre outros, o que deve ser minimamente explicitado nas regulações.

Os autores descrevem ainda em relação ao PL brasileiro, que a exceção quanto ao uso de IA de risco excessivo se dará em termos da seção de risco excessivo pelo poder público para o uso de sistemas de identificação biométrica à distância em atividades de segurança pública. Assim, consideram que:

> Na prática, o que o artigo **cria é uma moratória**, condicionando o uso de tais sistemas à dois fatores: (i) promulgação de lei federal específica, (ii) autorização judicial de utilização, que deve estar conectada à atividade de persecução penal individualizada, para crimes passíveis de pena máxima de reclusão superior a dois anos, busca de vítimas de crimes ou pessoas desaparecidas ou crime em flagrante. (BIONI *et. al.*, 2022, p.48, grifos no original.)

A lei federal deverá prever expressamente medidas proporcionais e estritamente necessárias ao atendimento do interesse público, além da necessidade de revisão por agente

público responsável pela inferência algorítmica antes da tomada de ação relativa à pessoa identificada.

Na regulamentação europeia, existem duas posições diferentes sobre a regulamentação da identificação biométrica. Seu uso está proibido em tempo real e em espaços públicos (por entes públicos ou privados), assim como o uso de sistemas para análise de gravações de espaços públicos com identificação biométrica remota. Consistindo a exceção, se houver autorização judicial prévia para o uso, que deve se dar no contexto da persecução penal, quando estritamente necessário, e ser relativo a um crime sério que já ocorreu.

Alguns documentos internacionais de referência não especificam nada em torno do uso de IAs de risco excessivo, mas preveem que, mediante certas condições, alguns sistemas de IA devem ser submetidos a moratória ou proibição prévias. A preocupação aqui levantada é com relação ao prognóstico futuro de desenvolvimento de sistemas letais plenamente autônomos – que se enquadrariam nessa denominação ao qual o PL restou silente, sobre os mecanismos incidentes no manejo AIs de risco inaceitável. A Recomendação sobre a Ética da Inteligência Artificial da UNESCO proíbe sistemas de IA que tenham efeitos negativos em impactos ambientais (Art. 86), de sistemas dotados do poder de tomar decisões de vida ou morte (Art. 36), e da recomendação de não utilização de IA para fins de vigilância em massa e crédito social (Art. 26).

II.5 – EIXO 2 – AVALIAÇÕES DE IMPACTO ALGORÍTMICO – AIA

O principal propósito das ferramentas aqui mencionadas é de servirem como efetiva ferramenta de *accountability*, dessa feita espera-se que haja uma procedimentalização mínima da AIA a partir de um tripé: (i) publicidade, prevendo a criação de uma base de dados pública sobre sistemas de IA de alto risco (ii) participação pública multissetorial significativa de indivíduos e comunidades potencialmente afetados, gerando legitimidade e supervisão significativa e democrática dos sistemas de IA e (iii) variedade dos riscos e benefícios a serem avaliados, promovendo uma regulação atenta aos aspectos sócio-técnicos-econômicos locais. Como exemplo, cita-se as definições do art. 4º, VI do PL 2.388/23, que adota os conceitos de discriminação direta e indireta da Convenção Interamericana contra o Racismo, adotada pelo Brasil em 2022 com status constitucional.

As avaliações de impacto como descritas em tópico anterior já são bem conhecidas na legislação pátria em termos de proteção de dados pessoais, em suas espécies de RIPD. Essas

ferramentas de governança possuem claro trabalho de controle em face da tutela de interesses sociais relevantes e por intermédio de sua análise sustentam processos decisórios informados das condições sob as quais poderão ser desenvolvidas determinadas iniciativas. Seu papal fulcral de elaboração de evidências se afasta, por exemplo, de avaliações de conformidade regulatórias produzidas *ex-post* e se sobressaem com relação às últimas dado seu caráter precaucionário/preventivo.

Assim, possuem caráter de aplicação de medidas de mitigação eficientes antes da implementação de uma determinada tecnologia, seguindo um escrutínio público que desengatilha um controle social e em rede de governança, tratando-se sobretudo, de medidas de justiça procedimental.

No cenário da aplicação de sistemas de inteligência artificial para automatização de decisões, isso se relaciona com o devido processo informacional, como:

> [...] forma de concretização do contraditório e da ampla defesa e, por conseguinte, de contenção sobre ações que interferem indevidamente em liberdades públicas - e.g., policiamento preditivo - e direitos individuais - e.g., liberdade de expressão no cenário de moderação de conteúdo, por meio de maior controle sobre os procedimentos que são realizados. (BIONI *et. al.*, 2022, p. 68)

Assim, a avaliação de impacto de AI cumpre ao papel desenvolver IA centrada no ser humano e eficaz, mesmo em contextos desafiadores, gerando maior confiabilidade não só da tecnologia em si, mas também das trocas econômicas que as envolve. Para tanto, exigem que seja feita uma clara definição de parâmetros mínimos de metodologia, critérios, etapas e, eventualmente, previsões sobre a necessidade de publicação e revisão periódica. Nesse ponto, o PL 2338/2023 avança em comparação aos demais, em similaridade com o que é feito no AI EU Act, Canadá e demais instrumentos internacionais, como veremos na sequência

Os autores citam um estudo preliminar sobre o AIA elaborado por um Comitê *Ad Hoc* de Inteligência Artificial do Conselho da Europa que constatou ao avaliar as estruturas gerais da avaliação de impacto dos direitos humanos, a tendência desses instrumentos se concentrarem em impactos adversos de determinada iniciativa sobre esses direitos, o que também acontece na maioria dos atuais modelos de avaliação de impacto de sistemas de IA. Defendem que avaliações de impacto de IA devem ser desenvolvidas de acordo com esta abordagem, haja vista não existirem apenas efeitos negativos já que a tecnologia tem muitas vantagens e pode criar um enorme impacto benéfico para a sociedade em geral. No entanto, esse valor deve estar restrito a detectar possíveis riscos de violação de direitos humanos, e não os contrabalancear com possíveis impactos benéficos.

Nesse diapasão, o equilíbrio entre benefícios e riscos não necessariamente se inclui na metodologia de avaliação de impacto, mas auxiliaria, posteriormente, no julgamento de oportunidade quanto à implantação (ou não) de sistemas de IA.

Já as recomendações da UNESCO sobre ética de sistemas de IA estabelece elementos que constituem uma boa prática para avaliação de impacto adaptáveis em diferentes áreas, quais sejam: "um método genérico para avaliação de impacto que consiste em 10 passos agrupados em 5 fases. São elas: (i) preparação; (ii) avaliação/análise; (iii) recomendações; (iv) etapas contínuas; (v) revisão". (Bioni *et al.*, 2023, p. 71)

Nesse sentido o CAHAI definiu quatro etapas mínimas para o desenvolvimento desta ferramenta, de forma a contemplar a identificação de direitos relevantes, avaliar os impactos nestes direitos – o que inclui critérios, o escopo e escala da aplicação e o potencial de pessoas impactadas), mecanismos de governança e avaliações constantes.

Esses elementos estão em consonância com a prestação de contas em IA oferecida pela OCDE em 2023, em suas orientações comuns para promover a interoperabilidade na gestão de riscos de IA, na qual confirma que os principais modelos e quadros de gestão de riscos se alinham a essas mesmas quatro etapas. Não obstante, o público-alvo, o âmbito do risco, o segmento do ciclo de vida de IA, a terminologia específica utilizada e a própria ordem das etapas possa variar entre os documentos existentes, os modelos geralmente procuram alcançar os mesmos resultados.

É o que acontece também no PL nº 2338/2023, que consagra as quatro etapas representadas pela preparação, cognição do risco, mitigação destes riscos e monitoramento em seu Art. 24.

Assim, a análise do risco formal geralmente envolve algum tipo de matemática que envolve elementos de probabilidade de um evento acontecer e a gravidade do dano potencialmente causado por esse evento, gerando a previsibilidade do impacto esperado pelos riscos identificáveis dentro da mesma classificação quaternária de baixo, moderado, elevado e altíssimo/inaceitável.

Nesse sentido, Mantalero sustenta que os sistemas de IA carregam consigo uma complexidade que exige que as avaliações de impacto sejam desenvolvidas a partir de um modelo misto de análise do seu impacto ético e social juntamente com as dimensões legais, como as dos direitos humanos (Mantalero, 2022, p.74) e, para tanto, defende a necessidade de uma abordagem *multistakeholder* centrada no ser humano.

Assim, a avaliação de impacto não é um processo trivial, tanto em sua realização quanto para análise, essa exigência fica geralmente restrita aos sistemas de IA de alto risco, sem prejuízo de sua realização como boa prática para os sistemas de IA de risco mais baixo.

É isso que está previsto no PL 2338/23 e no EU AI Act, assim como a AIDA canadense. Porém, além da classificação de alto risco como critério de destrave da obrigação de avaliações de impacto, há algumas iniciativas que associam outros critérios, como a natureza da organização, a exemplo de sistemas de IA utilizados pelo poder público, como reforçado pela Ferramenta de Avaliação de Impacto Ético de IA fornecida no âmbito das recomendações da UNESCO.

No caso do PL 2338/2023, há expressa previsão de atualizações periódicas da AIA, que deve fazer parte de todo o ciclo de vida dos sistemas de IA de alto risco (art. 25 e art. 24 parágrafo quarto). Assim, mesmo tratando-se de uma ferramenta preponderantemente realizada em momento anterior ao lançamento da tecnologia no mercado, a sua atualização ao longo do ciclo de vida da IA é indispensável, novamente rememoramos a obscuridade em torno do mecanismo de revisão via atualizações periódicas – o qual seria imprescindível na análise de tecnologias de alto risco.

Concluída nossa análise em torno dos modelos regulatórios adotados na prevenção e manejo dos riscos adotados ao desenvolver sistemas computacionais inteligentes, seguiremos agora para o último item deste trabalho, descrevendo brevemente o funcionamento do organismo escolhido pela comunidade internacional para discutir e elaborar enunciados que orientem os normativos regulatórios no campo das inteligências artificiais – O comitê de Certas Armas Convencionais.

II.6 – CAC – A Convenção sobre Certas Armas Adicionais e as discussões internacionais sobre proliferação das LAWS

Neste tópico, almeja-se desenhar uma descrição institucional e jurídica da Convenção sobre Certas Armas Convencionais e seu papel central na discussão internacional sobre a proliferação de sistemas letais de armas autônomas, abordando os principais enunciados formulados até a presente data pela entidade. Serão abordados sua sistemática, as principais distinções entre o modelo de regulamentação do direito costumeiro internacional em relação aos modelos do direito regulatório, e por fim, o atual estado da arte efetivamente debruçados na temática das LAWS.

Criada em 10 de outubro de 1980, a Convenção sobre Certas Armas Convencionais (CAC) surgiu do processo de negociação dos Protocolos Adicionais às convenções de Genebra, sobretudo durante os conflitos armados da Indochina da década de 60, que despertaram a necessidade de regulamentação do uso de armas incendiárias, minas antipessoais e outros itens que causassem danos indiscriminados e sofrimento excessivo, levando o governo da suíça a convocar as Conferências Diplomáticas sobre a Reafirmação e Desenvolvimento do Direito Internacional Humanitário Aplicável a Conflitos Armados ocorrida em Genebra entre 1974 e 1977 (NERY, 2022, p. 43). Como descreve o autor, determinadas delegações da conferência viam com bons olhos o estabelecimento de proibições e limitações concretas ao emprego desses tipos de artefato por via da criação de um comitê ou órgão específico capaz de formular uma lista de meios e métodos de combate cujas características fossem condizentes com o disposto no Art. 35 do Protocolo Adicional I do Comitê Internacional da Cruz Vermelha, conferindo-lhe um caráter mais substantivo.

Estabelecido o comitê *ad hoc* para discutir o tema, foi desenhado o comitê permanente em comento, com três objetivos primários: (i) O estabelecimento da conexão jurídica necessária entre o DIH contemporâneo e as futuras proibições e restrições ao uso de armamentos convencionais; (ii) a criação propriamente dita de um comitê para determinar quais armamentos e quais usos deveriam estar sujeito à sua limitação, promovendo acordos internacionais específicos sobre o tema e (iii) a consolidação institucional necessária para que os referidos acordos tivessem efeitos entre os Estados dentro dos quadros do DIH.

A despeito da falha inicial do rascunho do Artigo 86 da proposta inicial e não assinada de criação de um comitê permanente – em virtude da relutância de algumas nações que alegavam que conceber esse tipo de lista implicaria em desarmamento, estando, portanto, fora do escopo da conferência, foi acordada a resolução 22, que almejava a manutenção das tratativas envolvendo acordos sobre proibições ou restrições no uso de armas convencionais dentro do arcabouço institucional das Nações Unidas.

Como menciona Nery sobre o processo de institucionalização do CAC:

> A referida resolução e subsequente recomendação foram a pedra institucional fundamental para a realização dos debates preparatórios e eventual adoção da Convenção sobre Armas Convencionais. (NERY, 2022, p.45).

Nesse ponto o autor descreve como o histórico da CAC está intimamente entrelaçado com a relutância estatal na promoção de banimentos completos a determinados tipos de armamentos, estando mais propensos a estabelecer mecanismos de regulamentação diversos do

puro banimento no campo de armas autônomas e a outras aplicações em conflitos armados de inteligência artificial em virtude das vantagens estratégicas de seu uso na relação com outros Estados.

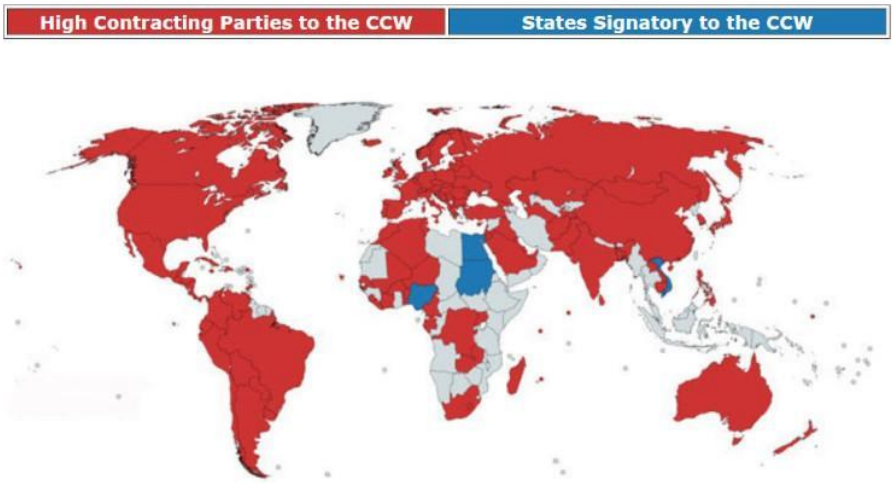
Não obstante, à partir da adoção da Resolução 22, adotada ao final da conferência diplomática, os Estados passaram a reconhecer que o alcance de uma paz duradoura no nível internacional só poderia ser assegurada por intermédio de mecanismos que efetivamente zelem pelo sistema de segurança previsto na Carta das Nações Unidas, finalmente rechaçando de forma direta as doutrinas de superioridade estratégica e das teorias de intimidação. Desse ponto em diante, o controle de armas passa a ser mecanismo indispensável do fortalecimento da segurança internacional e elemento de interesse da coletividade global.

Esse entendimento se fortaleceu no século XIX, com a concepção de que o desenho ou uso de certas armas convencionais poderiam acarretar perigos que consubstanciam elevadas preocupações humanitárias, estratégicas e de preservação de danos de conflitos armados, merecendo, portanto, normatividade própria que as tutelassem.

Dessa forma, a CAC representa um grande centro regulador da conduta em conflitos internacionais e não internacionais em relação ao uso de armas e dos meios e métodos de guerra em consonância ao Direito Internacional Humanitário (DIH). Anualmente, são convocadas reuniões do comitê no Escritório das Nações Unidas em Genebra, na Seção de Genebra do Escritório para Assuntos de Desarmamento, as reuniões e conferências são realizadas entre os Estados-partes para discutir sobre o surgimento de novas armas e da validade do uso de determinados meios e métodos de guerra para que não ocorram violações do DIH. O resultado dessas conferências é então disponibilizado nos idiomas oficiais admitidos pela ONU no banco de dados do Escritório das Nações Unidas para Assuntos de Desarmamento, o UNODA.

Funcionam com base em um mecanismo de monitoramento de suas disposições, conforme estabelecido em 2006, que é baseado no *compliance* de cooperação e consultas recíprocas, partilha de informações bem como implementando reuniões entre Altas Partes Contratantes (dispostas na imagem abaixo), conferências de análises das operações da Convenção, debates acerca de assuntos provenientes dessas informações e considerações de cooperação internacional.

Há de se citar que pesam duras críticas ao organismo, visto que o corpo normativo da CAC não estabelece uma obrigatoriedade do envio desses relatórios, tampouco estipula contramedidas em caso de sua não submissão.



Fonte: Escritório das Nações Unidas para Assuntos de Desarmamento – The convention on certain conventional weapons

Após cada reunião, é estabelecida nova agenda provisória e plano de trabalho para a próxima reunião, com pautas em voga a serem discutidas pelos grupos de especialistas.

O Artigo 36 do Protocolo Adicional I de 1977 às Convenções de Genebra de 1949 determina que todos os Estados-partes das Convenções de Genebra devem examinar a legalidade de toda nova arma, sistema de armas e métodos de guerra que produzem e adquirem. Portanto, a Convenção sobre Certas Armas Convencionais foi criada para restringir ou proibir o uso de certas armas, e pode, como na aplicação dos princípios adotados no Protocolo Adicional I de 1977, ser somada às proibições já existentes como menciona Sandoz (2009).

O mesmo autor caracteriza a estrutura institucional da CAC por meio dos 11 artigos de seu corpo normativo, que estabelece o escopo de aplicação, ratificação, entrada em vigor, relações com outros instrumentos jurídicos internacionais, mecanismos de análise e emenda, denúncia, depositários e textos autênticos, definindo-a como um arcabouço inteligente que estabelece um verdadeiro quadro geral das futuras proibições adotadas, sendo que sua função principal não é de definir proibições em si, e sim de promover apoio técnico aos respectivos protocolos que trarão normas substantivas no controle de armas.[10]

[10] SANDOZ, Yves. "Convention Of 10 October 1980 On Prohibitions Or Restrictions On The Use Of Certain Conventional Weapons Which May Be Deemed To Be Excessively Injurious Or To Have Indiscriminate Effects (Convention On Certain Conventional Weapons" Disponível em: < https://legal.un.org/avl/pdf/ha/cprccc/cprccc_e.pdf >

Outra crítica persistente quanto à estrutura da CAC está contida justamente nesse liame, em que sua estrutura geral não adota previsão específica de aferição do cumprimento de suas obrigações ou mecanismos normativos que assegurem a implementação das normativas por ela elaboradas. Esses dispositivos são elaborados a partir dos enunciados e protocolos formulados pelo comitê.

Até o momento, foram negociados 5 diferentes protocolos pelo CAC, disponíveis em seu sítio eletrônico: O Protocolo I sobre Fragmentos não Detectáveis, o Protocolo II sobre Minas, Armadilhas e Outros Dispositivos e o Protocolo III sobre Armas Incendiárias e os Protocolos IV e V sobre Armas Laser Cegantes e Restos Explosivos de Guerra, respectivamente, foram adotados pelos Estados-partes

Há dois tipos de reuniões implementadas no âmbito da CAC: as Reuniões de Altas Partes Contratantes e as Conferências de Análise.

A primeira ocorre anualmente com o fito de debater questões envolvendo temas de interesse do comitê e analisar os trabalhos desenvolvidos por grupos de peritos governamentais.

Já as conferências de análise, previstas do artigo 8 da convenção ocorre por ocasião de apresentação de uma emenda por parte de alguma das Altas Partes Contratantes, ou subsidiariamente, por força do § 3 se não apresentado nenhum acréscimo dessa natureza no prazo de 10 anos, qualquer parte contratante poderá convocar uma conferência de análise para discutir o funcionamento da Convenção e seus Protocolos Anexos, além de considerar qualquer proposta de emenda. Foi o ocorrido a partir da resolução 48/70 da Assembleia Geral das Nações Unidas que agendou a primeira dessa natureza entre 25 de setembro e 13 de outubro de 1995.

Nela, foi levantada a proposta de uma reunião periódica a cada 5 anos, que aprovada e em vigor, agora possui status e atribuições similares às Reuniões das Altas Partes, envolvendo a análise do estado e das operações da Convenção e seus Protocolos.

Outro ramo institucional de elevada importância dentro da sistemática da CAC, os Grupos de Peritos Governamentais são conjuntos de especialistas acadêmicos, militares, jurídicos e técnicos que se reúnem junto aos representantes estatais sob autoridade de mandato para promover debates e estudos sobre determinado tema ou arma, com competência inclusive para desenhar novo protocolo. Esses produzem relatórios, recomendações e rascunhos de documentos a serem aprovados pelos Estados membros.

Foi precisamente o trabalho de um Grupo de Peritos que resultou na formatação das regras procedimentais utilizadas na primeira conferência de análise, e replicadas para a segunda

ocorrida em 2001, na qual as decisões tomadas foram tomadas por consenso e não por contagem de votos.

II.7 – ESTRUTURAS DOS DEBATES PARA NOVAS TECNOLOGIAS EM ARMAMENTOS

Nery (2022, p. 56) narra como o tema de aplicação de autonomia dos sistemas de Inteligência Artificial começaram a ser tratados de forma específica em idos de 2013, quando a reunião das Altas Partes Contratantes desse ano decidiu agendar uma reunião informal para tratar das tecnologias emergentes dos LAWS em 2014. No triênio consecutivo, reuniões informais de grupos de peritos debateram acerca dos mecanismos para regulamentar a emergência dessas novas tecnologias e equipamentos militares.

Nelas, foram discutidos aspectos técnicos, éticos e jurídicos, contudo, para o autor é importante frisar o caráter *dual-use* da tecnologia discutida, isto é, o fato que os componentes técnicos que permitem autonomia em armamentos militares são os mesmos elementos que possibilitam o desenvolvimento de tecnologias no campo civil, bem como o papel das análises de armamentos previstas no Art. 36 do Protocolo Adicional I. a ver:

> Muitas intervenções mencionam o fato de componentes técnicos capacitadores de autonomia são similares em aplicações cíveis e militares em decorrência da natureza de duplo-uso dessas tecnologias. Também se menciona a importância de se preservara pesquisa e desenvolvimento de modalidades pacíficas de tais aplicações das robóticas, dada a previsibilidade positiva do seu impacto na saúde, por exemplo, ou da agricultura e atividades de resgate. Dessa forma, é considerado profícuo focar no uso crítico das LAWS relacionas ao uso da força[11]. (Nery, 2023, p. 57)

Já na 5ª Conferência do Grupo de Especialistas de 6 de março de 2024, decidiu-se pela criação de um grupo de peritos permanente para tratar do tema, decidindo também que o quadro normativo e de estrutura providos pelo CAC são fóruns apropriados para lidar com as questões dos sistemas de armas autônomos, em razão do caráter modular e evolucionário estabelecido pelo arcabouço geral da Convenção, sobretudo em virtude da busca por equilíbrio entre considerações humanitárias, de necessidade militar e a oportunidade de engajamento de

[11] Trad nossa; no original: "Many interventions mentioned the fact that the technical components enabling autonomy were similar for military and civil applications because of the dual-use nature of such technologies. It was also mentioned that it was important to preserve research and development on peaceful applications of robotics given their foreseeable positive impact, for instance on health care, agriculture or rescue operations. In this regard, it was mentioned that it could be useful to focus on the critical functions of LAWS related to the use of force" - CCW EXPERT MEETING ON LETHAL AUTONOMOUS WEAPON SYSTEMS. 2014. *Draft Report.* Disponível em: < https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2014/DraftReport.pdf >

múltiplos atores. Nesses termos, nota-se a estrutura institucional do organismo como potencialmente a mais adaptada não só para desenvolver conceitos e disposições sobre os LAWS, mas capaz de discutir impactos acerca das mais diversas aplicações de AI, incluindo modalidades de regulamento mais específicas (Nery, 2022, p. 61).

Por fim, Nery descreve a importância de ampliação da participação dos autores não-estatais no regime do CAC, sobretudo do setor de tecnologia em conflitos armados, incluindo não só a participação do terceiro setor como expressiva e valiosa da perspectiva teórica, como prática, com potencial de serem atores importantes dentro da estrutura do Comitê, propondo o envio de artigos e formulação de apresentações como algumas formas de costura de relações dentro da rede de governança tecnológica.

Nesse último item deste trabalho foi desenvolvida uma descrição da evolução do CAC, e apresentado um contraponto importantíssimo à futura discussão dos impactos das diversas aplicações de AI, esperando-se que pela inclusão de maior participação do terceiro setor, possam ser atingidos os objetivos conclamados pelo então Secretário-Geral das Nações Unidas, António Guterres, de que até o final de 2026 seja elaborado novo tratado internacional, que funcione como instrumento vinculativo que proíba os esforços de criação de sistemas autônomos de armas letais que desrespeitem o Direito Internacional Humanitário.

CONCLUSÃO

Este trabalho buscou apresentar, por meio de uma ampla revisão bibliográfica, um panorama geral acerca da origem, características e tentativas de justificação do emprego das armas autônomas. Essa visão geral foi lançada com o fito de possibilitar a discussão em torno das possíveis vias de proibição ou regulamentação de tais dispositivos, delineadas pela Doutrina Majoritária do Direito Internacional Penal e pelas Convenções e Tratados atualmente em vigor ou tratativas de implementação ao redor do mundo.

Nesse diapasão, concluímos pela dificuldade executiva de identificação clara de mecanismos de responsabilização de agentes envolvidos na cadeia de produção e operação dos sistemas letais autônomos, decorrente da incerteza quanto às várias possibilidades de violações ocorrerem por de falhas no design, atuação maliciosa de invasores dos sistemas informacionais ou efetivamente pela decisão consciente do controle significativo dos controladores – a qual inclusive dificilmente poderia ser mensurada em virtude do caráter de atuação automático da tecnologia.

Na sequência foi discutida a característica dogmática dos prováveis modelos de persecução penal que poderiam ser aplicáveis ao último elemento mencionado por intermédio de diferentes mecanismos que cuidam da *liability* em três vias principais de possíveis responsabilizações penais vinculadas às AI e seus operadores, levando ainda em consideração que além da necessária manifestação objetiva da vontade do ser humano que a controla, a evolução da persecução penal tem evoluído para além do objetivo de punir faltas, e sim reestabelecer a confiabilidade social com relação à norma lesionada pelo ofensor.

Já na segunda etapa deste trabalho, foi desenvolvida uma análise dos principais regramentos incidentes sobre tecnologias de Inteligência Artificial, buscando melhor compreender racionalidade regulatória de intersecção de um movimento global em governança de IA, atrelada principalmente a identificação de direitos relevantes, avaliação de impactos significativos nesses direitos e dos mecanismos de governança aplicáveis no seu manejo.

Por último em nosso recorte, foi apresentado o CAC – ente responsável pela discussão da proliferação de armas inteligentes no contexto internacional cujo o papel central e indissociável e elaborar termos de ajuste de condutas que freiem o uso de maquinários de guerra que desrespeitam os Direitos Humanitáriorios e causam sofrimento desnecessário, onde foi igualmente elencada a maior participação de participação de entidades privadas – atuantes no interesse social como força motriz importantíssima ao melhor êxito dessas discussões, sobretudo em virtude do caráter não mandatário de seus enunciados.

Segundo os modelos regulatórios revisados, como o AI Act e o Anteprojeto do Senado Federal para a regulação da IA no Brasil, formas de IA com possíveis resultados letais integrariam categorias de risco inaceitável/proibido, de modo que o modelo regulatório não parecer se o mais adequado para a responsabilidade penal relacionada a drones e outros equipamentos de guerra automatizados. Sugere-se, para a continuidade das pesquisas sobre o tema, a inclusão do debate sobre essas ferramentas militares no contexto do direito internacional de guerra, que se preocupa de forma mais ativa com tecnologias militares em contexto internacional, um uso presente e crescente dessas tecnologias.

Por fim, consideramos que essa pesquisa ainda possui várias dinâmicas que poderiam ter sido exploradas, com relação ao atual exercício do Poder Cinegético pelos Estados, dos recortes de doutrina militares a serem manejados no caráter de aumento dos gastos orçamentários de defesa nacional atrelados aprimoramento de itens de hardware e software, dada a impossibilidade de competição armamentista tendo unicamente o Estado como detentor e desenvolvedor das próximas tecnologias bélicas emergentes; e da importância participativa

de seres-humanos no controle de sistemas informáticos em cenários de *machine learning.* Esses elementos foram retirados do recorte inicial da pesquisa por não se vincularem à finalidade jurídica que buscamos desenvolver na presente pesquisa, mas muito dizem sobre as próximas sendas evolutivas que as tecnologias aqui examinadas terão nos próximos anos.

Nesses termos, há muito para se explorar em tema tão recente e de rápida evolução, mas acreditamos que os objetivos de apresentar um trabalho científico – acessível e informativo, foi uma missão efetivamente cumprida em nossos próprios termos, esperando que sirva de base para outras iterações que também desenvolvam os temas aqui propostos e que são de grande valia para a sociedade num geral.

REFERÊNCIAS

AGÊNCIA Nacional de Aviação Civil – ANAC – Regulamento Brasileiro de Aviação Civil Especial nº 94/2017 (RBAC-E nº 94/2017). Disponível em: < RBAC - Regulamentos

Brasileiros da Aviação Civil — Agência Nacional de Aviação Civil ANAC> Acesso em: 10 de Outubro de 2024.

AGÊNCIA Nacional de Proteção de Dados – ANPD – Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial – disponível em: < https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf >

BEDIN, G. A., Leves, A. M. P., & Marcht, L. M. (2022). Os Sistemas De Armas Autônomas E O Direito Internacional: Uma Análise Da Guerra E Das Implicações Do Uso Da Inteligência Artificial. Direito Público, 18(100). Disponível em: < https://doi.org/10.11117/rdp.v18i100.6000 >Acesso em: 26 out. 2023

BISPO, Christiano Carvalho. A Utilização do Veículo Aéreo Não Tripulado nas atividades de Segurança Pública em Minas Gerais. 2013. Especialização. Escola de Governo Professor Paulo Neves de Carvalho. Belo Horizonte/MG. 2013

BIONI, Bruno; GARROTE, Marina; GUEDES, Paula. Temas centrais na Regulação de IA: O local, o regional e o global na busca da interoperabilidade regulatória. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2023.

BORNE, Thiago. Tecnologias Militares Emergentes: digitalização e a *third offset strategy* estadunidense. Revista Brasil de Estudos de Defesa, v.6, nº1, jan/jun de 2019. p. 109-138. Doi. DOI: 10.26792/RBED.v6n1.2019.75118ISSN 2358-3932 Disponível em: <https://rbed.abedef.org/rbed/article/view/75118/42100 >Acesso em 04 de Nov. 2024

BRYNJOLFSSON, E., & MCAFEE, A. (2014). The second machine age. Work, progress, and prosperity in a time of brilliant technologies. W. W. Norton & Company.Disponível em:<https://edisciplinas.usp.br/pluginfile.php/4312922/mod_resource/content/2/Erik%20-%20The%20Second%20Machine%20Age.pdf >Acesso em: 26 out. 2023

CHAMAYOU, Grégoire. Teoria do Drone. Trad. Célia Euvaldo. São Paulo: Cosac Naify, 2015, 288 p.

CELESTE, E. Digital constitutionalism: a new systematic theorization. International Review of Law, Computers & Technology, v. 33, n. 1, p. 76–99, 2019.

CROOTOF, Rebecca. War Torts: Accountability for Autonomous Weapons, 164 U. PA. L. REV. 1347 (2016).

DEPARTAMENTO de Controle do Espaço Aéreo Brasileiro – DECEA – Aeronaves Não Tripuladas e o Acesso ao Espaço Aéreo Brasileiro – ICA 100-40. Disponível em: < Modelo de publicação (decea.mil.br)> Acesso em: 10 de Outubro de 2024.

DIVINO, S. Responsabilidade penal de Inteligência Artificial: uma análise sob a ótica do naturalismo biológico de John Searle. Revista Brasileira de Ciências Criminais, v. 171, p. 153–183, 2020

D. Tezza and M. Andujar, "The State-of-the-Art of Human–Drone Interaction: A Survey," in *IEEE Access*, vol. 7, pp. 167438-167454, 2019, doi: 10.1109/ACCESS.2019.2953900.

EAGLEN, Mackenzie. What is the Third Offset Strategy? Real Clear Defense[S.l.] (16 de fevereiro de 2016) Disponível em: <http://www.realcleardefense.com/articles/2016/02/16/what_is_the_third_offset_strategy_109034.html. > Acesso em 04 nov de 2023.

ENEMARK, Christian. Moralities of Drone Violence. Edinburgh University Press, 2023. Págs.161-199.

FARNOSIER, M. DE O. Criminal Liability and artificial intelligence. Revista Brasileira de Ciências Criminais, v. 187, n. 30, p. 153–170, 2022.

FRAZÃO, Ana. Marco da Inteligência Artificial em análise: Já não foram mapeados riscos suficientes para justificar uma regulação adequada e com efeitos práticos? - Parte I. Jota, 15 dez. 2021. Disponível em: https://www.jota.info/opiniao-eanalise/colunas/constituicao-empresa-e-mercado/marco-inteligencia-artificial-15122021. Acesso em: 27 jan 2025.

GARCIA, Rafael de Deus; DUARTE, Evandro Piza. *Compreendendo algoritmos aplicados aosistema de justiça criminal – ilegibilidade, acesso, compreensão, verdade e computabilidade no 'eu' identificado por algoritmos*.Revista Brasileira de Ciências Criminais. vol. 183. ano 29. p. 199-226. São Paulo: Ed. RT, setembro 2021.Disponivel em < https://bdjur.stj.jus.br/items/d53227a6-17bb-4f65-8657-5ae85bacebd5>. Acesso em 12/02/2025.

GLESS, Sabine, et al. "IF ROBOTS CAUSE HARM, WHO IS TO BLAME? SELF-DRIVING CARS AND CRIMINAL LIABILITY." *New Criminal Law Review: An International and Interdisciplinary Journal*, vol. 19, no. 3, 2016, pp. 412–36. *JSTOR*, https://www.jstor.org/stable/26417695. Acesso em 25 Jan. 2025.

HALLEVY, Gabriel (2010) "The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control," Akron Intellectual Property Journal: Vol. 4 : Iss. 2 , Article 1.

Available at: https://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1

International Human Rights Clinic & Human Rights Watch. (2012). Losing humanity. The case against killer robots. Human Rights Watch.

JORNAL Oficial da União Européia - Regulamento (Ue) 2024/1689 Do Parlamento Europeu E Do Conselho De 13 De Junho De 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689

KELSEN, Hans. Teoria Geral do Direito. 4. ed. São Paulo: Martins Fontes, 2005

MATÁRIC, M.J, Introdução à robótica. Tradução de Humberto Ferasoli Filho, José Reinaldo Silva, Silas Franco dos Reis Alves. – 1. Ed. São Paulo: Editora Unesp/Blucher, 2014. PIOVESAN, Flávia. Direitos Humanos e o Direito Constitucional Internacional. [Editora Saraiva, 2022. *E-book.* ISBN 9786553620476. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553620476/. Acesso em: 09 out. 2024.

MADEIRA, H. B., & Terron, L. L. S. (2024). INTELIGÊNCIA ARTIFICIAL NO DIREITO PENAL. *Revista Contemporânea*, *4*(9), e5802 . disponível em https://doi.org/10.56083/RCV4N9-130 Acesso em: 26/01/2025.

MITTELSTADT, Brent. Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, v. 1, p. 501-507, nov. 2019. Disponível em: https://doi.org/10.1038/s42256-019-0114-4 . Acesso em: 27 jan. 2025

NERY, Pedro Lyrio Verissimo. A Convenção sobre Certas Armas Convencionais e a fronteira entre conflitos armados e inteligência artificial: a construção de um arcabouço regulatório para equipamentos autônomos a partir de uma perspectiva produtiva e de governança internacional. 2023. 187 f. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023.

PORCELLI, A. M. (2021). La inteligencia artificial aplicada a la robótica en los conflictos armados. Debates sobre los sistemas de armas letales autónomas y la (in)suficiencia de los estándares del derecho internacional humanitario. Revista de Estudios Socio-Jurídicos, 23(1), 483-530. Disponível em: https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.9269 Acesso em: 26 out. 2024

PROJETO de relatório da reunião de especialistas de 2014 sobre Sistemas Letais de Armas Autônomas (LAWS) – CAC – disponível em : <https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2014/DraftReport.pdf >

SANDOZ, Yves. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (with Protocols), 1980. Audiovisual Library of International Law, 2009. Disponível em:< https://legal.un.org/avl/ha/cprccc/cprccc.html > Acesso em: 28 Jan. 2025

SENADO Federal, Brasil. Projeto de Lei nº 2338/2023. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF, 2023. Disponivel em:< https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1720545987618&disposition=inline> Acesso em 12 Fev 2025.

SOUSA, Pedro. Direito penal nos tempos da inteligência artificial: uma análise da responsabilidade dos agentes envolvidos no desenvolvimento e na operação de algoritmos de seleção e recrutamento em relação ao crime de racismo previsto no art. 4º da lei 7.716/1989. 2023. 123 f. Dissertação (Mestrado em Direito Constitucional). Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022.

SCHLOTTFELDT, Shana. Rebooting AI: a elaboração da proposta de regulação da inteligência artificial no Brasil em perspectiva comparada com a União Europeia. 2022. 60 f. Artigo científico apresentado ao Instituto Legislativo Brasileiro – ILB como pré-requisito para a obtenção de certificado de conclusão de Curso de Pós-Graduação Lato Sensu em Processo Legislativo e Direito Parlamentar.

WALSH, Toby. Robôs Assassinos – Inteligência artificial e armas autônomas. Revista IDEES. Disponível em: <https://revistaidees.cat/es/killer-robots/ >Acesso em 28 out. 2024