

#### ORGANIZADORES

FELIPE CHIARELLO DE SOUZA PINTO

SANDRA PASSINHAS

RICARDO LIBEL WALDMAN

JOÃO PINTO MONTEIRO

# ANAIS DO CONGRESSO SOCIEDADE DIGITAL E INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA DEMOCRACIA

#### AUTORES

ADELE MENDES WEINBERG

ANA CRISTINA CRESTANI

CELSO MARAN DE OLIVEIRA

DORIVALDO MANUEL "DORIVAL"

ELIEL VITOR DE SOUSA VITÓRIO

GUILHERME MORAES CARDOSO

ISADORA VALADARES ASSUNÇÃO

LUCAS GONÇALVES DA SILVA

MARCELO FONSECA SANTOS

MARINA CRIVELLI SIMÕES

REGINALDO FELIX NASCIMENTO

RENATA AKEMI OTAKE

RENATA BRAGA KLEVENHUSEN

TATIANA VIEIRA DE MORAES

**Coordenadores**

Felipe Chiarello de Souza Pinto

Sandra Passinhas

Ricardo Libel Waldman

João Pinto Monteiro

**ANAIS DO CONGRESSO SOCIEDADE  
DIGITAL E INTELIGÊNCIA ARTIFICIAL:  
DESAFIOS DA DEMOCRACIA**



**tirant**  
lo blanch

**Copyright**© Tirant lo Blanch Brasil

*Editor Responsável:* Aline Gostinski

*Capa e diagramação:* Analu Brettas

**CONSELHO EDITORIAL CIENTÍFICO:**

**EDUARDO FERRER MAC-GREGOR POISOT**

*Presidente da Corte Interamericana de Direitos Humanos. Investigador do Instituto de Investigações Jurídicas da UNAM - México*

**JUAREZ TAVARES**

*Catedrático de Direito Penal da Universidade do Estado do Rio de Janeiro - Brasil*

**LUIS LÓPEZ GUERRA**

*Ex Magistrado do Tribunal Europeu de Direitos Humanos. Catedrático de Direito Constitucional da Universidade Carlos III de Madrid - Espanha*

**OWEN M. FISS**

*Catedrático Emérito de Teoria de Direito da Universidade de Yale - EUA*

**TOMÁS S. VIVES ANTÓN**

*Catedrático de Direito Penal da Universidade de Valência - Espanha*

W443 Weinberg, Adele Mendes

Anais do congresso sociedade digital e inteligência artificial : desafios da democracia [livro eletrônico] / Adele Mendes Weinberg ... [et al.]; Felipe Chiarello de Souza Pinto, Sandra Passinhas, Ricardo Libel Waldman, João Pinto Monteiro (Coord.). - 1.ed. - São Paulo : Tirant lo Blanch, 2024.

2259 Kb; livro digital

ISBN: 978-65-5908-764-8.

1. Sociedade digital. 2. Inteligência artificial. 3. Democracia. 4. Direitos Humanos. I. Título.

CDU: 34:004

Biblioteca Elisabete Cândida da Silva CRB-8/6778

*É proibida a reprodução total ou parcial, por qualquer meio ou processo, inclusive quanto às características gráficas e/ou editoriais. A violação de direitos autorais constitui crime (Código Penal, art.184 e §§, Lei n° 10.695, de 01/07/2003), sujeitando-se à busca apreensão e indenizações diversas (Lei n°9.610/98).*



**tirant  
lo blanch**

**Todos os direitos desta edição reservados à Tirant lo Blanch.**

Fone: 11 2894 7330 / Email: [editora@tirant.com](mailto:editora@tirant.com) / [atendimento@tirant.com](mailto:atendimento@tirant.com)  
[tirant.com/br](http://tirant.com/br) - [editorial.tirant.com/br/](http://editorial.tirant.com/br/)

**Coordenadores**

Felipe Chiarello de Souza Pinto  
Sandra Passinhas  
Ricardo Libel Waldman  
João Pinto Monteiro

# ANAIS DO CONGRESSO SOCIEDADE DIGITAL E INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA DEMOCRACIA

**Autores**

Adele Mendes Weinberg  
Ana Cristina Crestani  
Celso Maran de Oliveira  
Dorivaldo Manuel “Dorival”  
Eliel Vitor de Sousa Vitorio  
Guilherme Moraes Cardoso  
Isadora Valadares Assunção  
Lucas Gonçalves da Silva  
Marcelo Fonseca Santos  
Marina Crivelli Simões  
Reginaldo Felix Nascimento  
Renata Akemi Otake  
Renata Braga Klevenhusen  
Tatiana Vieira de Moraes



# SUMÁRIO

|   |     |
|---|-----|
| APRESENTAÇÃO.....   | 7   |
| <i>Felipe Chiarello de Souza Pinto, Ricardo Libel Waldman, Sandra Passinhas e João Pinto Monteiro</i>   |     |
| DIREITO INTERNACIONAL DA ECONOMIA DIGITAL: RELAÇÕES CONTRATUAIS NA INTERNET E PROTEÇÃO JURÍDICA DO CONSUMIDOR .....   | 9   |
| <i>Lucas Gonçalves da Silva e Reginaldo Felix Nascimento</i>  |     |
| PROPRIETARY AND OPEN-SOURCE ARTIFICIAL INTELLIGENCE: THE REGULATORY CHALLENGES OF A JANUS-FACED TECHNOLOGY .....  | 19  |
| <i>Isadora Valadares Assunção</i>   |     |
| GUARDIÃO DA CONSTITUIÇÃO: UMA ANÁLISE DO CONTROLO DA CONSTITUCIONALIDADE ENTRE O CHEFE DO ESTADO E O TRIBUNAL CONSTITUCIONAL EM ANGOLA .....  | 43  |
| <i>Dorivaldo Manuel “Dorival”</i>   |     |
| DEMOCRACIA EM TEMPOS DE INTELIGÊNCIA ARTIFICIAL. DESAFIOS E OPORTUNIDADES .....   | 59  |
| <i>Guilherme Moraes Cardoso</i>   |     |
| O USO DA IA GENERATIVA EM CAMPANHAS POLÍTICAS E SEUS IMPACTOS NO PROCESSO ELEITORAL DEMOCRÁTICO.....  | 77  |
| <i>Adele Mendes Weinberg e Marina Crivelli Simões</i>   |     |
| A LGPD BRASILEIRA E O OBSTÁCULO À PESQUISA ACADÊMICA: O CASO DO ‘FÓRUM DE CIDADÃOS PARTICIPANTES’ .....   | 92  |
| <i>Tatiana Vieira de Moraes e Celso Maran de Oliveira</i>   |     |
| DIREITO PENAL E INTELIGÊNCIA ARTIFICIAL: ANÁLISE SOBRE A NECESSIDADE DE HAVER UMA REGULAMENTAÇÃO PARA GARANTIA DE DIREITOS FUNDAMENTAIS, SOB A ÓTICA DA PROPOSTA DE REGULAMENTO DA UNIÃO EUROPEIA SOBRE INTELIGÊNCIA ARTIFICIAL, DE 21 DE ABRIL DE 2021 ..... | 106 |
| <i>Ana Cristina Crestani</i>  |     |
| INTELIGÊNCIA ARTIFICIAL NOS PROCESSOS JUDICIAIS: ANÁLISE SOBRE A DISCRIMINAÇÃO ALGORÍTMICA .....  | 122 |
| <i>Renata Akemi Otake</i>   |     |
| GOVERNANÇA DE DADOS, AUDITORIA E DIREITOS FUNDAMENTAIS NO USO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL .....  | 133 |
| <i>Marcelo Fonseca Santos</i>   |     |

ARTIFICIAL INTELLIGENCE, DIGITAL RECREATION, AND THE ELIS REGINA CASE: AN ANALYSIS IN THE CONTEXT OF BILL 2,338/2023 AND PERSONALITY RIGHTS ..... 138

*Renata Braga Klevenhusen e Eliel Vitor de Sousa Vitorio*

# APRESENTAÇÃO

O Congresso Sociedade Digital e Inteligência Artificial : Desafios da Democracia foi organizado em conjunto pela Faculdade de Direito da Universidade de Coimbra – Portugal e pela Faculdade de Direito da Universidade Presbiteriana Mackenzie – Brasil, por meio de seu curso de Graduação em Direito e Programa de Pós-Graduação em Direito Político e Econômico com apoio das Subseções, Santo Amaro, Tatuapé, Jabaquara e Itaquera da Ordem dos Advogados do Brasil Seção de São Paulo, procura discutir os efeitos para o direito da inteligência artificial na sociedade digital. O principal tema discutido foram os desafios à democracia neste contexto. Para isso contamos com palestrantes de ambas as Universidades, experts na área, e com a apresentação de trabalhos de pesquisadores nos grupos de trabalho: GT1 Cidadania, democracia e inteligência artificial, GT2 Proteção de dados e democracia, GT3 Economia, democracia e inteligência artificial. Tais grupos se inserem nas investigações dos grupos de pesquisa Laboratório de Direito Digital e Democracia e Estado e Economia no Brasil, ambos registrados no Diretório de Grupos de Pesquisa Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq, do Brasil. Os trabalhos foram submetidos ao sistema duplo cego de avaliação, sendo que 60% dos avaliadores são mulheres. Os trabalhos vieram de Portugal, de Angola e de diversos Estados brasileiros, como São Paulo, Minas Gerais, Mato Grosso do Sul e Sergipe

O evento foi organizado para discutir estes temas a partir de uma perspectiva inclusiva quanto ao gênero, começando pelas comissões organizadoras e científica, paritárias entre homens e mulheres, do mesmo modo que os palestrantes. Também foi paritária a participação de brasileiros e portugueses em todos esses casos.

O tema da democracia foi abordado em diversas dimensões, tanto nas palestras quanto nos trabalhos apresentados, buscando mapear potencialidades e riscos da utilização das novas tecnologias para a efetivação dos direitos fundamentais. Esperamos que os leitores possam tirar proveito desses anais para suas próprias pesquisas.

*São Paulo/Coimbra, Janeiro de 2023*

**FELIPE CHIARELLO DE SOUZA PINTO**

**RICARDO LIBEL WALDMAN**

**SANDRA PASSINHAS**

**JOÃO PINTO MONTEIRO**

Os trabalhos vieram de Portugal, de Angola e de diversos Estados brasileiros, como São Paulo, Minas Gerais, Mato Grosso do Sul e Sergipe

O evento foi organizado para discutir estes temas a partir de uma perspectiva inclusiva quanto ao gênero, começando pelas comissões organizadoras e científica, paritárias entre homens e mulheres, do mesmo modo que os palestrantes. Também foi paritária a participação de brasileiros e portugueses em todos esses casos.

O tema da democracia foi abordado em diversas dimensões, tanto nas palestras quanto nos trabalhos apresentados, buscando mapear potencialidades e riscos da utilização das novas tecnologias para a efetivação dos direitos fundamentais. Esperamos que os leitores possam tirar proveito desses anais para suas próprias pesquisas.



# DIREITO INTERNACIONAL DA ECONOMIA DIGITAL: RELAÇÕES CONTRATUAIS NA INTERNET E PROTEÇÃO JURÍDICA DO CONSUMIDOR

LUCAS GONÇALVES DA SILVA<sup>1</sup>  
REGINALDO FELIX NASCIMENTO<sup>2</sup>

## 1. INTRODUÇÃO

Com o advento das tecnologias de informação e comunicação, a plataforma da vida opera um esvaziamento das práticas econômicas para o ambiente digital. Nesse contexto, as contratações na internet assumiram uma dimensão significativa nas relações econômicas transnacionais. A natureza anárquica da sociedade internacional e o Direito Internacional Privado, este considerado obsoleto com parâmetro na efervescência tecno-econômica, expõem um *status naturae* relativamente às contratações na internet e, em especial, uma vulnerabilização ainda mais hostil dos consumidores, sendo comum situações de violência financeira de consumo através das plataformas digitais.

A proposição de um Direito Internacional da Economia Digital, feita pelo professor Umberto Celli Junior, funciona como uma rosa dos ventos a fim de nortear a concentração dos estudos jurídicos entorno do estreitamento das relações econômicas por meio do recurso digital, facilitando o surgimento de uma iluminação epistemológica que dimensionaliza os desafios impostos pelas tecnologias de Informação e Comunicação. O crescimento exponencial do mercado digital justifica a relevância deste trabalho e do questionamento realizado, qual seja, compreender a proteção jurídica do consumidor na economia digital, esta que propõe ser imaterial e desterritorializada.

No campo do Direito Internacional da Econômica Digital, o presente trabalho tem como objetivo investigar: os impactos sofridos nas relações contratuais comerciais com o advento da internet; mensurar como o ciberespaço, na medida em que funciona como ambiente fértil para o exercício de direitos humanos e

---

1 Pós-doutor em Direito pela Università Degli Studi G. d'Annunzio (Itália). Doutor e Mestre em Direito do Estado pela Pontifícia Universidade Católica de São Paulo (PUC/SP). E-mail: [lucasgs@uol.com.br](mailto:lucasgs@uol.com.br).

2 Pós-graduando (*Lato Sensu*) em Direito Internacional (Universidade de São Paulo/USP). Mestrando em Constitucionalização do Direito (Universidade Federal de Sergipe/UFS). Taxa Capes. E-mail: [felixreginaldo84@gmail.com](mailto:felixreginaldo84@gmail.com).

fundamentais, funciona como violador de direitos; designar a flexão na vulnerabilidade do consumidor a partir do Direito Internacional Privado com amparo na realidade econômica digital; destrichar os aspectos da vulnerabilidade do consumidor nas relações consumeristas.

O trabalho é estruturado a partir da metodologia hipotético-dedutiva, através de uma abordagem temática histórico-evolutiva e dogmática, com recursos bibliográficos e documentais, tais como livros, periódicos, artigos e leis, de cunho nacional e internacional.

Na fase preliminar para o desenvolvimento das ideias traçadas neste artigo, utilizou-se as seguintes premissas hipotéticas: o Direito Internacional da Economia Digital é palpável e necessário para a compreensão das novas tecnologias e seus impactos na sociedade internacional; a alteração das práticas econômicas significou uma alteração nos padrões contratuais; o consumidor globalizado é hipervulnerável, porque sujeito a condições que os demais consumidores não estão expostos.

## **2. DIREITO INTERNACIONAL DA ECONOMIA DIGITAL E RELAÇÕES CONTRATUAIS NA INTERNET**

O Direito Internacional da Economia Digital é uma área ainda pouco explorada, porém demasiadamente importante para os contornos da globalização vivenciados na atualidade. O estudo do Direito Internacional da Economia Digital é proposto pelo Professor Umberto Celli Junior<sup>3</sup>, que inaugura uma discussão de extrema relevância no seio do Direito Internacional.

As tecnologias de informação e comunicação no cenário da economia mundial, ainda que não sofram influência mais “impositiva” de cunho jurídico nas relações internacionais, são tocadas por algumas propostas. À vista disso, pode-se observar, por exemplo, a Lei Modelo da UNCITRAL Sobre o Comércio Eletrônico que, segundo a professora Ana Amelia Menna Barreto de Castro Ferreira (2008, p. 262), “[...] aplica-se a qualquer tipo de informação na forma de mensagem de dados usada no contexto de atividades comerciais [...]”.

O aumento das transações internacionais com recursos tecnológicos tem inserido preocupações acerca dos novos contratos no âmbito do Direito Internacional Privado. Esse acontecimento levanta questionamentos acerca da necessidade de estudar, regulamentar e regular tópicos como Proteção e Dados Pessoais, noções jurídicas para os contratos e bens digitais, liberdade de expressão e a de-

---

3 CELLI JUNIOR, Umberto. Tecnologias digitais e o comércio de bens e serviços na OMC/Digital. Revista de Direito Internacional, v. 17, n. 1, 2020.

finição de outros padrões éticos para o uso da tecnologia. Isso porque, como afirmado por Cássio Bruno Castro Souza e Marta Luiza Leszczynski Salib, “com o mercado de consumo ampliado a níveis internacionais, a Internet surge como instrumento de marketing e vendas para as empresas transnacionais; e como meio de compra para os consumidores globais”.<sup>4</sup>

Recentes estudos acerca de como as tecnologias de informação e comunicação funcionam como ferramentas intensificadoras das assimetrias globais, o que Nick Couldry, Ulises Mejias e João Magalhães conceituam como sendo colonialismo de dados, escancaram o cunho geopolítico que o domínio de tais técnicas apresenta para o mundo. O capitalismo hoje funciona com ferramentas de controle mais invasivas, sofisticadas e silenciosas, apresentando a dominação por uma requintada força invisível que domina pela satisfação.

O Professor Umberto Celli Junior<sup>5</sup> conceitua o comércio digital como sendo aquele constituído pela “transmissão (transfronteiriça ou não) de bens e serviços por meios eletrônicos”. Esse breve conceito é muito interessante, porque internaliza relações nacionais virtuais de comércio, mas ao mesmo tempo provoca o que realmente existe de “nacional” nas relações domésticas conectadas ao anárquico ciberespaço. Talvez seja o momento de conjecturar o fim das relações domésticas em relação ao fenômeno da total internacionalização das relações contratuais através do ciberespaço.

Enquanto o encurtamento dos espaços através do ciberespaço continuar sendo visto como objeto de lucro, o esvaziamento das relações interpessoais e econômicas para o mundo virtual avançará substancialmente. A partir disso, “rompendo o paradigma de territorialidade, o desaparecimento no meio eletrônico dos limites estatais e territoriais, desafia a fixação da competência”<sup>6</sup>e, conseqüentemente, aplicação do direito e proteção dos sujeitos envolvidos.

Nesse aspecto, fulcral conceber a importância da proteção de dados pessoais no mundo contemporâneo. Umberto Celli Junior<sup>7</sup> assevera que as Leis Gerais de Proteção de Dados se ocupam com a localização de dados, o que compreende, nesse aspecto, a regulação dos fluxos transfronteiriços de dados pessoais. À vista disso, no Direito Internacional da Economia Digital, o controle dos fluxos transfronteiriços de dados pessoais deve ser entendido como novas barreiras co-

---

4 SOUZA, Cássio Bruno Castro; SALIB, Marta Luiza Leszczynski. A hipervulnerabilidade do consumidor no E-Commerce Cross Border: o desafio do mercado transnacional. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, v. 5, n. 2, p. 64-84, 2019, p. 05.

5 CELLI JUNIOR, Umberto. Tecnologias digitais e o comércio de bens e serviços na OMC/Digital. Revista de Direito Internacional, v. 17, n. 1, 2020, p. 393.

6 DE CASTRO, Ana Amelia Menna Barreto. Proteção do consumidor no comércio eletrônico sob a ótica da teoria da confiança. Revista da EMERJ, v. 11, n. 42, 2008, p. 168.

7 CELLI JUNIOR, Umberto. Tecnologias digitais e o comércio de bens e serviços na OMC/Digital. Revista de Direito Internacional, v. 17, n. 1, 2020.

merciais, porque as bases de dados são imprescindíveis em operações comerciais. Como descrito pelo Professor Umberto Celli Junior <sup>8</sup>:

A depender do entendimento da Comissão, no caso da União Europeia, e da Autoridade Nacional de Proteção de Dados, no caso do Brasil, a transferência poderá não ocorrer, interrompendo e impedindo o fluxo de dados essencial ao blockchain e às cadeias globais de suprimento do comércio internacional.

Na possibilidade de conflitos legais em função das limitações territoriais impostas pela formatação jurídica do Estado-nação, Umberto Celli Junior <sup>9</sup> demonstra como o GATS pode ser importante instrumento jurídico na resolução do conflito envolvendo *blockchain* e fluxos transfronteiriços de dados pessoais. Dessarte, Umberto Celli Junior<sup>10</sup> identifica que o Anexo para Telecomunicações do GATS veda o controle dos fluxos transfronteiriços de dados pessoais no âmbito da jurisdição da OMC, uma vez que os membros compromissados “[...] devem assegurar que os provedores de serviços estrangeiros possam usar redes de transportes de telecomunicações para o movimento transfronteiriço de informações e para o acesso de informações contidas em bases de dados”.

Todavia, ainda que se possa conjecturar sobre a adaptação do GATS ao cenário introduzido pelas TIC’S, o professor Umberto Celli Junior<sup>11</sup> salienta que não existe algo explícito na Organização Mundial de Comércio (OMC) que se refira diretamente as transações com recurso *blockchain*.

Nesse momento, a definição de uma subárea do Direito Internacional é de extrema relevância, porque insere no debate um campo de estudo sobre o qual os acadêmicos e profissionais podem depositar suas experiências. Existe uma proposta epistemológica muito rica e necessária, que abrange boa parte dos problemas enfrentados na interseção da globalização com as tecnologias, o Estado-nação e o Direito. Isso porque, a “[...] massificação do consumo e a transnacionalidade da produção ganhou novos contornos com a Internet (...) o acesso à produtos internacionais e serviços virtuais foi facilitado, pois aproximou consumidores, empresas, governos e entidades das mais variadas ordens”.<sup>12</sup> À vista disso, algumas preocupações apontadas por Lucas Gonçalves da Silva, Reginaldo Felix

---

8 CELLI JUNIOR, Umberto. Tecnologias digitais e o comércio de bens e serviços na OMC/Digital. Revista de Direito Internacional, v. 17, n. 1, 2020, p. 399.

9 CELLI JUNIOR, Umberto. Tecnologias digitais e o comércio de bens e serviços na OMC/Digital. Revista de Direito Internacional, v. 17, n. 1, 2020.

10 CELLI JUNIOR, Umberto. Tecnologias digitais e o comércio de bens e serviços na OMC/Digital. Revista de Direito Internacional, v. 17, n. 1, 2020, p. 400

11 CELLI JUNIOR, Umberto. Tecnologias digitais e o comércio de bens e serviços na OMC/Digital. Revista de Direito Internacional, v. 17, n. 1, 2020.

12 SOUZA, Cássio Bruno Castro; SALIB, Marta Luiza Leszczynski. A hipervulnerabilidade do consumidor no E-Commerce Cross Border: o desafio do mercado transnacional. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, v. 5, n. 2, p. 64-84, 2019, p. 65.

Nascimento e Camilla Ellen Aragão Costa<sup>13</sup>, relativamente a erosão orçamentária, regressividade tributária internacional e, conseqüentemente, fomento das assimetrias globais por meio da tributação internacional no ciberespaço, devem ser inseridas no âmbito do Direito Internacional da Economia Digital.

Outro aspecto que deve ser salientado e que reforça a necessidade de falar acerca de um Direito Internacional da Economia Digital, diz respeito ao fato de que o consumo direto nas plataformas tem deslocado produtos com imensidão considerável, de modo que a noção de um Estado-nação como agente importante para viabilizar grandes acordos de comércio para circulação de bens e serviços, tem ficado obsoleta nos últimos tempos. O consumidor poder ter acesso a qualquer serviço, sem depender da presteza política internacional do seu Estado, e outras nações podem encaminhar seus produtos para qualquer lugar do mundo, sem igualmente depender de grandes acordos comerciais para tanto, o que representa o surgimento de uma Economia indiferente ao Estado-nação e à geopolítica.

A natureza jurídica do objeto de estudo sempre é muito importante para entender os empregos das relações retratadas. No caso do Direito Internacional da Economia Digital, é possível perceber vertentes públicas e privatistas das relações jurídicas. Isto é, quando a análise diz respeito às relações contratuais de consumo, enquadra-se no Direito Internacional Privado, e quando às relações dizem respeito ao Direito Econômico, enquadra-se no Direito Internacional Público. Com efeito, o Direito Internacional da Economia Digital é imprescindível para a solidificação de uma epistemologia jurídica para o Estudo dos novos contornos conflituosos envolvendo uso das Tecnologias de Informação e Comunicação, que abrange tanto estudos publicistas quando privatistas do Direito.

Para o problema retratado neste artigo, algumas discussões são importantes no âmbito do Direito Internacional da Economia Digital. Isso porque, documentos internacionais levantam questionamentos polêmicos a esse respeito. A Lei Modelo da UNCITRAL para comércio eletrônico repercute que o comércio no ciberespaço não se daria num território, porque a internet seria um recurso de contratação e não exatamente um território. Todavia, perspectiva tal demonstra seus sinais de obsolescência quando empresas podem existir independente de qualquer endereço ou, ainda, a existência de produtos absolutamente digitais.

---

13 SILVA, Lucas Gonçalves da; NASCIMENTO, Reginaldo Felix; COSTA, Camilla Ellen Aragão. Tributação e Novas Tecnologias. In: PINTO, Danielle Jacon Ayres; SALEME, Edson Ricardo; AYUDA, Fernando Galindo (Org.). Direito, Governança e Novas Tecnologias. Anais do VI Encontro Virtual do CONPEDI, p. 418-439, 2023.

### 3. HIPERVULNERABILIDADE DO CONSUMIDOR NA ECONOMIA DIGITAL

Ana Amelia Menna Barreto de Castro Ferreira<sup>14</sup> destaca que “as tecnologias da informação e comunicação, por suas características intrínsecas de desmaterialização e desintermediação, agrava a posição de vulnerabilidade do consumidor, dificultando a efetividade das normas consagradas para seu abrigo”. Segundo Ana Amelia Menna Barreto de Castro Ferreira<sup>15</sup>, as redes sociais expõem o consumidor a uma violação intensa da privacidade. As escolhas podem ser impulsionadas, as pesquisas no buscador muitas vezes não correspondem aos reais interesses pressupostos pelo usuário, são corriqueiras propagandas e a publicidades abusivas ou enganosas, a popularização dos contratos de adesão (termos e condições), limitações cognitivo-decisórias do consentimento e a própria inteligência artificial que induz comportamentos, todos esses fatores contribuem para que a internet seja um ambiente de armadilhas, que pode a todo instante captar o usuário a firmar um contrato com prejuízos irreversíveis. Dessa forma, os contratos internacionais de consumo colocam o fornecedor e a cadeia de consumo muito distantes do usuário, amplificando ainda mais a vulnerabilidade do consumidor.

Cássio Bruno Castro Souza e Marta Luiza Leszczynski Salib<sup>16</sup> apontam para a concepção da hipervulnerabilidade do usuário da internet, defendida no artigo “Hipervulnerabilidade Digital Do consumidor Diante do Comércio Eletrônico, da Inteligência Artificial e da Internet das Coisas”. A abordagem feita pelos autores é de suma importância, tendo em vista que várias ocorrências apontam para o fato de que o consumidor globalizado está sujeito às condições que os consumidores tradicionais não estão submetidos, inclusive, é comum que o consumidor globalizado esteja posicionado numa terra de ninguém, em que suas relações não são protegidas por algum agente facilmente determinável.

Conforme preceituado por Cássio Bruno Castro Souza e Marta Luiza Leszczynski Salib<sup>17</sup>, “o Direito internacional historicamente desenvolveu-se para solucionar litígios entre partes que estavam no mesmo patamar, em condições de igualdade”. No caso do consumidor, a verticalidade da relação no ambiente digital é incomensurável, de modo que concebê-lo enquanto hipervulnerável é crucial na proteção dos seus direitos. A partir disso, urge imprescindível “[...]”

---

14 DE CASTRO, Ana Amelia Menna Barreto. Proteção do consumidor no comércio eletrônico sob a ótica da teoria da confiança. Revista da EMERJ, v. 11, n. 42, 2008, p. 168.

15 DE CASTRO, Ana Amelia Menna Barreto. Proteção do consumidor no comércio eletrônico sob a ótica da teoria da confiança. Revista da EMERJ, v. 11, n. 42, 2008.

16 SOUZA, Cássio Bruno Castro; SALIB, Marta Luiza Leszczynski. A hipervulnerabilidade do consumidor no E-Commerce Cross Border: o desafio do mercado transnacional. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, v. 5, n. 2, p. 64-84, 2019

17 SOUZA, Cássio Bruno Castro; SALIB, Marta Luiza Leszczynski. A hipervulnerabilidade do consumidor no E-Commerce Cross Border: o desafio do mercado transnacional. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, v. 5, n. 2, p. 64-84, 2019, p. 76.

equilibrar as relações entre a parte mais fraca da relação e a outra mais forte, entregando uma prestação jurisdicional mais justa possível”.<sup>18</sup>

Lucas de Souza Lehfeld, Alexandre Celio, Oniye Nashara Siqueira e Renato Britto Barufi<sup>19</sup>, categorizam a vulnerabilidade do consumidor nas plataformas digitais em vulnerabilidade fática, técnica e científica. Na perspectiva dos autores, a vulnerabilidade técnica diz respeito “[...] à condição do consumidor em não conter informações precisas acerca daquilo que compra, sendo presumido que o fornecedor detenha tais informações específicas sobre aquilo que comercializa”.<sup>20</sup> A vulnerabilidade técnica é vislumbrada em quaisquer ofertas na internet, considerando que o consumidor adquire um produto que será encaminhado de um outro país, com distância considerável, e o consumidor apenas consegue ter acesso ao produto quando o bem chega à sua residência.

Na vulnerabilidade fática, percebe-se a “[...] desigualdade financeira entre o consumidor e fornecedor, tendo em vista o poder econômico superior daquele que produz, principalmente se tratando de relação de consumo entre pessoa física e jurídica”<sup>21</sup>. Atualmente, algumas plataformas digitais chegam a concorrer poder com Estados. Esse mesmo poderio econômico figura em um dos polos da relação de consumo, estando de um lado a pessoa física (usuário da internet).

Na sequência, “[...] a vulnerabilidade jurídico-científica demonstra a ideia de que o consumidor nem sempre tem conhecimento de todos os seus direitos”<sup>22</sup>. Essa vulnerabilidade é intensificada quando o consumidor é exposto ao ambiente anárquico internacional, em que a dificuldade do entendimento do Direito Internacional Privado leva o consumidor a cometer equívocos, de modo a ter seus Direitos violados ou mesmo ter a reparação dificultada. Isso porque, “[...] o consumidor não tem informações suficientes para saber quais seus direitos, como funciona sua proteção contratual e quais órgãos contatar, no caso de descumprimento contratual ou acidente de consumo”, o que se intensifica, como recém afirmado, com a proposta do ciberespaço em ser um ambiente sem limitações.<sup>23</sup>

---

18 SOUZA, Cássio Bruno Castro; SALIB, Marta Luiza Leszczynski. A hipervulnerabilidade do consumidor no E-Commerce Cross Border: o desafio do mercado transnacional. *Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo*, v. 5, n. 2, p. 64-84, 2019, p. 76.

19 SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . *Revista Eletrônica Pesquiseduca*, [S. L.], v. 13, n. 29, p. 236–255, 2021

20 SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . *Revista Eletrônica Pesquiseduca*, [S. L.], v. 13, n. 29, p. 236–255, 2021, p. 243.

21 SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . *Revista Eletrônica Pesquiseduca*, [S. L.], v. 13, n. 29, p. 236–255, 2021, p. 243.

22 SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . *Revista Eletrônica Pesquiseduca*, [S. L.], v. 13, n. 29, p. 236–255, 2021, p. 243.

23 SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . *Revista Eletrônica Pesquiseduca*, [S. L.], v. 13, n. 29, p. 236–255, 2021, p. 243.

Num primeiro momento, Douglas Roberto Winkel Santin<sup>24</sup> expõe a Inteligência Artificial como agente significativo para a constituição da hipervulnerabilidade nas relações Digitais de Consumo. Sobre essa questão, Danilo Cesar Maganhoto Doneda, Laura Schertel Mendes, Carlos Affonso Pereira de Souza e Norberto Nuno Gomes de Andrade<sup>25</sup>, demonstram que as Inteligências Artificiais são capazes de controlar as decisões dos seres humanos, o que impõe questionamentos relativamente ao consentimento nos contratos firmados em plataformas digitais. Certamente, se de algum modo o consentimento é viciado pela inteligência artificial ou por algoritmos, os estatutos jurídicos devem reconhecer a imperfeição destas contratações, assegurando ao consumidor a possibilidade de reverter com segurança jurídica contratações equivocadas.

Laura Schertel Mendes e Gabriel C. Soares da Fonseca<sup>26</sup> demonstram a necessidade de que os contratos firmados na internet, especialmente o de adesão relativo ao consentimento para coleta de dados pessoais, encontre formas de proteção exteriores ao consentimento. Um dos argumentos mais emblemáticos dos referidos autores, diz respeito a relevância de pensar uma ética tecnológica e processos tecnológicos formados para proteger os usuários. Trazendo a discussão para os contratos de consumo, é imprescindível que os desenvolvedores de tecnologias se ocupem com a neutralização das tecnologias, no sentido de não produzirem violência financeira no mercado de consumo.

Carlos Mendes Monteiro da Silva, Luana Maria Martins e Elvis Gomes Marques Filho consideram a “[...] indispensabilidade de se estudar as peculiaridades do novo consumidor digital em comparação ao consumidor tradicional, bem como se tais peculiaridades são suficientes para justificar seu reconhecimento enquanto sujeito hipervulnerável”.<sup>27</sup> Logo, depois de analisadas as questões que intensificam a vulnerabilidade do consumidor no âmbito do Ciberespaço e no cenário do Direito Internacional da Economia Digital, é necessário conceber que as situações peculiares no ciberespaço constituem uma indubitável hipervulnerabilidade do consumidor nas relações de consumo plataformizadas e que não existe uma proteção consumerista sólida na sociedade internacional.

Portanto, a reunião dos fatores acima externados demonstram que o consumidor está exposto a situações peculiares e abusivas nas plataformas digitais, de

---

24 SANTIN, D. R. W. . A hipervulnerabilidade digital do consumidor diante do comércio eletrônico, da inteligência artificial e da internet das coisas. *Revista da Defensoria Pública do Estado do Rio Grande do Sul*, Porto Alegre, v. 2, n. 33, p. 22–43, 2023.

25 DONEDA, Danilo Cesar Maganhoto et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar-Revista de Ciências Jurídicas*, v. 23, n. 4, p. 1-17, 2018.

26 MENDES, Laura Schertel; DA FONSECA, Gabriel C. Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *REI-Revista Estudos Institucionais*, v. 6, n. 2, p. 507-533, 2020.

27 DA SILVA, Carlos Mendes Monteiro; MARTINS, Luana Maria; MARQUES FILHO, Elvis Gomes. O consumidor digital pode ser considerado um sujeito hipervulnerável?. *Ciências Sociais Aplicadas em Revista*, v. 22, n. 42, p. 17-31, 2022, p.18.



modo que nesses ambientes a sua vulnerabilidade é ainda maior, sendo inquestionável a configuração de uma hipervulnerabilidade nas relações de consumo intermediadas pela internet.

#### 4. CONSIDERAÇÕES FINAIS

O Direito Internacional da Economia Digital é uma proposta válida e importante para o direcionamento de estudos jurídicos que se prestam a diagnosticar os impactos das Tecnologias de Informação e Comunicação na sociedade internacional. Além disso, outro fator teórico que deve ser compreendido, diz respeito a possibilidade de o campo de estudo abordado ser útil tanto para análises publicistas do Direito quanto análises privatistas do Direito. O estreitamento das relações humanas e, conseqüentemente, relações econômicas, oferecem para o Direito desafios regulatórios, porque tais estreitamentos outrora incomuns, pressupõem e confirmam a existência e possibilidade de novos conflitos no seio da sociedade.

Nesse sentido, a mudança da sociedade e o impulsionamento da ideologia da globalização, através dos cenários supra externados, demonstra mudanças nas formas de contratação, sendo comum contratos imateriais e desterritorializados. O surgimento das novas contratações acompanha preocupações que gravitam a proteção do consumidor, tendo em vista que a sua vulnerabilidade é intensificada pelo ambiente virtual, por questões técnicas, científicas e fáticas.

Decerto, o consumidor deve ser compreendido como hipervulnerável, porque aparelham-se às suas práticas negociais situações incomuns, com relação as vulnerabilidades técnica, científica e fática, que são amplificadas com o surgimento do consumo mediado por Tecnologias de Informação e Comunicação.

#### REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Alix Aguirre; FERNÁNDEZ, Nelly Manasía. **Los principios Unidroit en las relaciones comerciales internacionales**. Revista de derecho, n. 25, p. 47-79, 2006.

ARAUJO, Nadia de. **Uma visão econômica do Direito Internacional Privado**. In: TIMM, Luciano Benetti. Direito e Economia no Brasil: estudos sobre a análise econômica do direito. 4ª ed. Indaiatuba: Editora Foco, 2021, p. 429-441.

CELLI JUNIOR, Umberto. **Tecnologias digitais e o comércio de bens e serviços na OMC/Digital**. Revista de Direito Internacional, v. 17, n. 1, 2020.

COASE, Ronald. **The problem of social cost**. Journal of Law and Economic, vol. 3, 1960, p. 1-44.

DA SILVA, Carlos Mendes Monteiro; MARTINS, Luana Maria; MARQUES FILHO, Elvis Gomes. **O consumidor digital pode ser considerado um sujeito hipervulnerável?**. Ciências Sociais Aplicadas em Revista, v. 22, n. 42, p. 17-31, 2022.

DE CASTRO, Ana Amelia Menna Barreto. **Proteção do consumidor no comércio eletrônico sob a ótica da teoria da confiança**. Revista da EMERJ, v. 11, n. 42, 2008.

DONEDA, Danilo Cesar Maganhoto et al. **Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal.** Pensar-Revista de Ciências Jurídicas, v. 23, n. 4, p. 1-17, 2018.

MORAES, Vitor Silva. **Contratos internacionais e os smart contracts: entre a tradição e a inovação.** Revista de Direito Internacional e Globalização Econômica, v. 5, n. 05, p. 104-114, 2019.

OLIVEIRA, Thiago Barcik Lucas de. **A economia dos custos de transação e o novo modelo proposto pelos smart contracts.** Revista Jurídica Luso-brasileira, nº 3, 1651-1679, 2022.

SILVA, Lucas Gonçalves da; NASCIMENTO, Reginaldo Felix; COSTA, Camilla Ellen Aragão. **Tributação e Novas Tecnologias.** In: PINTO, Danielle Jacon Ayres; SALEME, Edson Ricardo; AYUDA, Fernando Galindo (Org.). Direito, Governança e Novas Tecnologias. Anais do VI Encontro Virtual do CONPEDI, p. 418-439, 2023.

SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S. **A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD.** Revista Eletrônica Pesquiseduca, [S. l.], v. 13, n. 29, p. 236-255, 2021

SIQUEIRA, Oniye Nashara et al. **A (hiper) vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD.** Revista Eletrônica Pesquiseduca, v. 13, n. 29, p. 236-255, 2021.

SOUZA, Cássio Bruno Castro; SALIB, Marta Luiza Leszczynski. **A hipervulnerabilidade do consumidor no E-Commerce Cross Border: o desafio do mercado transnacional.** Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, v. 5, n. 2, p. 64-84, 2019.

# PROPRIETARY AND OPEN-SOURCE ARTIFICIAL INTELLIGENCE: THE REGULATORY CHALLENGES OF A JANUS- FACED TECHNOLOGY

ISADORA VALADARES ASSUNÇÃO<sup>1</sup>

## 1. INTRODUCTION

In Roman mythology, Janus is represented as having two faces, one looking to the past and one overseeing the future<sup>2</sup>. Since then, Janus became a symbol for areas that involve intrinsic dichotomies, such as Artificial Intelligence, which is both a dual-use technology and an area in which both proprietary and open-source systems are being developed.

AI systems are not new, although only recently has AI become a buzzword<sup>3</sup>. The idea of an intelligent machine can be traced back to Turing's seminal paper in 1950<sup>4</sup>, followed by the birth of a somewhat structured research field at the 1956 Dartmouth Summer Project<sup>5</sup>. However, hardware limitations prevented research directions that are nowadays widely diffused (*v.g.*, machine learning in general and, more specifically, Deep Neural Networks) from being recognised as having increased potential for solving complex problems<sup>6</sup>. Almost ironically, the increase in data collection and in available computational power led these very techniques to currently become a *quasi*-standard in the industry.

In this context, for many years, proprietary AI systems, many of which were developed by R&D departments of large companies were the rule in the AI field, partly due to the computational resources requirements and to the need of large databases, which were more readily available to these companies as they are

- 
- 1 Undergraduate Law student at the University of São Paulo. Mentored by Prof. Dr. Bernardo Bissoto Queiroz de Moraes in the Scientific Initiation Program of the Department of Civil Law. Lattes Curriculum: <http://lattes.cnpq.br/0274069896671094>. E-mail: [isadoravaladares@usp.br](mailto:isadoravaladares@usp.br)
  - 2 WASSEN, Donald L. Janus definition. World History Encyclopedia, 2015. Available at: <https://www.worldhistory.org/Janus/>. Accessed on 15 oct. 2023.
  - 3 ARTIFICIAL INTELLIGENCE. Google Trends, 2023. Available at: <https://trends.google.com.br/trends/explore?date=today%205-y&q=ai&hl=pt>. Accessed on 15 oct. 2023.
  - 4 TURING, Alan M. Computing Machinery and Intelligence. **Creative Computing**, v. 6, n. 1, p. 44-53, 1980.
  - 5 MCCARTHY, John et al. A proposal for the Dartmouth summer research project on artificial intelligence, August 31, 1955. **AI magazine**, v. 27, n. 4, p. 12-12, 2006.
  - 6 HOOKER, Sara. The hardware lottery. **Communications of the ACM**, v. 64, n. 12, p. 58-65, 2021.

significant players in the infosphere<sup>7</sup>. However, a different movement seems to be gaining momentum: open-source AI models.

One recent example of the opposition between these paradigms reached the public in May 2023: a leaked internal memorandum from a Google employee that stated that “We [Google] have no moat, and neither does OpenAI”<sup>8</sup>. In essence, the author of the document voiced his concern that, while Google and OpenAI were competing, a third group - open-source AI developers - had been catching up with the companies, which were doomed to be overtaken.

While open-source software has existed for quite some time, existing or proposed regulations for AI systems do not adequately address the dichotomy of proprietary and open-source AI, which will be analysed in the first section. In sequence, the dual-use attribute of each of these technological frameworks will be examined. In the end, general principles for a regulation that is compatible with the Janus-faced nature of AI will be proposed.

## 2. THE DICHOTOMY OF PROPRIETARY AND OPEN-SOURCE ARTIFICIAL INTELLIGENCE

Innovation should not be seen as a static and well-defined spot in time, but rather as a process that depends on a multi-agent effort, be it in a centralised or dispersed manner<sup>9</sup>.

In the beginning of the 20th century, innovation was carried out mainly in closed-door environments, partly due to an existing rivalry between basic research – seen as science by excellence – and applied research, seen as subsidiary<sup>10</sup>. In this model, industry was the leading actor of innovation, with their internal research and development (R&D) departments being responsible both for basic and applied research. A great example of this can be seen in the Bell Labs experience, which was responsible for the invention of the transistors, a technology that revolutionised computation<sup>11</sup>. The vertical integration in the closed innovation paradigm encompassed from the raw materials to the final products and knowledge was internally siloed in each company<sup>12</sup>.

---

7 VIPRA, Jai; KORINEK, Anton. Market concentration implications of foundation models. Brookings, 2023. Available at: <https://www.brookings.edu/articles/market-concentration-implications-of-foundation-models-the-invisible-hand-of-chatgpt/>. Accessed on 15 oct. 2023.

8 PATEL, Dylan; AHMAD, Afzal. Google “We have no moat, and neither does OpenAI”. Semianalysis, 2023. Available at: <https://www.semianalysis.com/p/google-we-have-no-moat-and-neither>. Accessed on 15 oct. 2023.

9 ROGERS, Everett M. Diffusion of innovations. New York: Simon and Schuster, 2010.

10 CHESBROUGH, Henry William. **Open innovation: The new imperative for creating and profiting from technology**. Cambridge: Harvard Business Press, 2003.

11 WU, Tim. **The master switch: The rise and fall of information empires**. New York: Vintage, 2011.

12 CHESBROUGH, Henry William. **Open innovation: The new imperative for creating and profiting from technology**. Cambridge: Harvard Business Press, 2003.

Nonetheless, as the exchange between R&D specialists intensified, innovation started to flourish in a more open paradigm, which values cooperation and interdisciplinary knowledge<sup>13</sup>. Firstly, with the erosion of employment stability, it became harder to maintain internal information secret as researchers moved from one company to the other. This was amplified by the improvement of communication networks, that allowed for researchers to exchange information outside of their siloed R&D departments. Finally, even incipient ideas now had incentives to be developed outside of traditional industrial players, with the advent of Venture Capital firms<sup>14</sup>.

The open paradigm of innovation is not to be confused with open source itself, as it can also lead to proprietary inventions. However, it is certain that the same advantages that the open innovation paradigm brought to the research area are some of the most distinguishable characteristics of open-source software: the promotion of iterative interactions between developers from multiple backgrounds.

In this sense, as research that leads to proprietary innovation is typically done in a more centralised and isolated manner, it has been compared to the method of building a mediaeval cathedral. Quite oppositely, open-source research is compared to a bazaar, as its distributed structure is similar to a fair of ideas. What warrants further examination are the impacts of each of these structures - “the cathedral and the bazaar”<sup>15</sup> - on the development and application of an idiosyncratic technology: AI.

## *2.1. PROPRIETARY ARTIFICIAL INTELLIGENCE AND ECONOMIC POWER*

Google (Alphabet), Apple, Facebook (Meta), Amazon and Microsoft - usually called by the acronym GAFAM or the expressions “Big Five” and “big tech”<sup>16</sup> - are some of the technology companies that most have far-reaching impacts in digital space and, consequently, in society. One example of this is the market capitalization of the GAFAM companies, which totals more than 8.7 trillion dollars<sup>17</sup>.

The pre-eminent position of these companies in the tech industry can be attributed to their dominance in the Big Data industry. Further examination of

---

13 CHESBROUGH, Henry William. **Open innovation: The new imperative for creating and profiting from technology**. Cambridge: Harvard Business Press, 2003.

14 Idem, *ibidem*.

15 RAYMOND, Eric. The cathedral and the bazaar. **Knowledge, Technology & Policy**, v. 12, n. 3, p. 23-49, 1999.

16 AN Exploration of acquisitions by big tech companies. The GAFAM Empire, 2023. Available at: <https://gafam.theglassroom.org/-timelines-of-expansion>. Accessed on 15 oct. 2023.

17 FENTON, Susan. Apple, Microsoft remain world's top 2 companies by market cap. Reuters, 2023. Available at: <https://www.reuters.com/technology/global-markets-marketcap-2023-08-01/>. Accessed on 15 oct. 2023.

the collected data, using AI models in the process of Knowledge Discovery in Databases, provides insights into user behaviour and informs commercial and organisational strategies<sup>18</sup>. Given these insights, big tech companies can improve their products and services, which, in turn, attracts more users. With more users, there is more data generation, in a feedback loop characterised by network externalities and lock-in effects<sup>19</sup>.

The omnipresence of big tech companies and their AI algorithms in society have become a truism. What is not incontrovertible are the effects of this dominance. From one perspective, big tech companies offer great advantages. To cite some: (i) they greatly financially influence some countries' GDPs, with Apple accounting for about 10% of the United States' GDP<sup>20</sup>; (ii) they are responsible for creating new labour opportunities, such as Amazon's Mechanical Turk; (iii) these companies have been leaders in many initiatives to bridge the digital divide, for example, with Facebook's Free Basics program; (iv) they offer optimised services in a wide-range of fields, from accurate navigation systems such as Google Maps to personalised services like Instagram's feed; (v) they offer access to independent sources of information in areas with media control, for instance, the Facebook platform was a major agent in the Arab Spring<sup>21</sup>; (vi) they are able to positively nudge users' behaviour, for example, with the Apple Watch experiment that increased users' probability of standing after periods of prolonged sitting by approximately 44%<sup>22</sup>.

However, for each of these potential benefits, a countervailing critique can be made: (i) financial power correlates with political power, which makes big tech influential stakeholders in many countries through well-financed lobbying<sup>23</sup>; (ii) work conditions of platform labour have been extensively questioned<sup>24</sup>; (iii) the initiatives to bridge the digital divide lead to concerns of data colonialism<sup>25</sup>; (iv)

---

18 GU, Hongfei. Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese Political Science*, p. 1-22, 2023.

19 FARRELL, Joseph; KLEMPERER, Paul. Coordination and lock-in: Competition with switching costs and network effects. *Handbook of industrial organization*, v. 3, p. 1967-2072, 2007.

20 POPKEN, Ben. Apple is now worth \$2 trillion, making it the most valuable company in the world. NBC News, 2020. Available at: <https://www.nbcnews.com/business/business-news/apple-now-worth-2-trillion-making-it-most-valuable-company-n1237287>. Accessed on 15 oct. 2023.

21 ARAFA, Mohamed; ARMSTRONG, Crystal. "Facebook to Mobilize, Twitter to Coordinate Protests, and YouTube to Tell the World": New Media, Cyberactivism, and the Arab Spring. *Journal of Global Initiatives: Policy, Pedagogy, Perspective*, v. 10, n. 1, p. 6, 2016.

22 NAZARET, Achille; SAPIRO, Guillermo. A large-scale observational study of the causal effects of a behavioral health nudge. *Science Advances*, v. 9, n. 38, p. eadi1752, 2023.

23 TAYLOR, Jack. Big Tech turns its lobbyists loose on Europe, alarming regulators. The New York Times, 2020. Available at: <https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html>. Accessed on 15 oct. 2023.

24 WILLIAMS, Adrienne et al. The exploited labor behind Artificial Intelligence. Noema, 2022. Available at: <https://www.noemamag.com/the-exploited-labor-behind-artificial-intelligence/>. Accessed on 15 oct. 2023.

25 THATCHER, Jim; O'SULLIVAN, David; MAHMOUDI, Dillon. Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, v. 34, n. 6, p. 990-1006, 2016.

their wide range of services create relevant data privacy issues<sup>26</sup>; (v) platforms for information dissemination have also been involved in the diffusion of hate speech, such as the role of Facebook in the *rohingya* genocide in Myanmar<sup>27</sup>; (vi) venues that allow for positive behavioural modification can also be used maliciously, such as in the Cambridge Analytica episode<sup>28</sup>.

This has even led scholars to propose that big tech companies' recent acknowledgment of some of these problems (such as the diffusion of hate speech) is a regulatory-capture strategy, as it was their algorithms themselves that created these problems<sup>29</sup>. If companies were to effectively solve the issues, their business models would be severely threatened.

The concerns about big tech dominance have already surpassed academia walls, leading to regulatory proposals. In the EU, recent regulations have imposed obligations to digital platforms, such as the Digital Markets Act (DMA) and the Digital Services Act (DSA)<sup>30</sup>, and to AI providers, with the EU AI Act<sup>31</sup>. In the US, a Blueprint for an AI Bill of Rights has been published by the White House<sup>32</sup> and antitrust investigations have been opened by the FTC<sup>33</sup>.

What is evident is that big tech dominance is being questioned. Another threat is economic recession in the tech sector: big tech companies lost 2.5 trillion dollars in combined market value in 2022, leading to hiring freezes and cost-cutting measures<sup>34</sup>. Perhaps the most significant vulnerability is the dispute over these companies' technological superiority<sup>35</sup>, as open-source AI systems are proliferating and reaching ever-increasing metrics of performance.

---

26 RUBINSTEIN, Ira. *Big data: The end of privacy or a new beginning?*. International Data Privacy Law (2013 Forthcoming), NYU School of Law, Public Law Research Paper, n. 12-56, 2012

27 MYANMAR: Facebook's systems promoted violence against Rohingya; Meta owes reparations. Amnesty International, 2022. Available at: <https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebook-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/>. Accessed on 15 oct. 2023.

28 WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. The Guardian, 2019. Available at: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Accessed on 15 oct. 2023.

29 SLEE, Tom. The incompatible incentives of private-sector AI. *The Oxford Handbook of Ethics of AI*, p. 106-123, 2020.

30 THE DIGITAL Services Act package. European Commission, 2023. Available at: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. Accessed on 15 oct. 2023.

31 EU AI ACT: first regulation on artificial intelligence. European Parliament, 2023. Available at: <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>. Accessed on 15 oct. 2023.

32 WHAT is the Blueprint for an AI Bill of Rights? White House, 2023. Available at: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>. Accessed on 15 oct. 2023.

33 KHAN, Lina. The new Brandeis movement: America's antimonopoly debate. *Journal of European Competition Law & Practice*, v. 9, n. 3, p. 131-132, 2018.

34 THE FUTURE of Big Tech. J.P. Morgan, 2022. Available at: <https://www.jpmorgan.com/insights/global-research/technology/future-of-big-tech>. Accessed on 15 oct. 2023.

35 BEARD, Alison. Can Big Tech be disrupted? Available at: <https://hbr.org/2022/01/can-big-tech-be-disrupted>. Accessed on 15 oct. 2023.

## 2.2. THE OPEN-SOURCE ARTIFICIAL INTELLIGENCE MOVEMENT

In the beginning of the 1970s, ARPAnet was developed by the Department of Defense in conjunction with universities, helping connect research groups across the US<sup>36</sup>. Around the same time, engineers at Bell Labs created a software environment called Unix. The operating system was initially shared quite extensively among academic institutions. However, the scenario shifted, and commercially licensed versions of Unix – such as SunOS - started to proliferate, limiting the access and modifications to its source code<sup>37</sup>. Frustrated by what was perceived as a loss in freedom, Richard Stallman developed the GNU project (a recursive acronym - Gnu's Not Unix), aiming to develop a free software based on Unix<sup>38</sup>.

Free software was not a disagreement with the price of proprietary software. Instead, the movement was based on a moral argument about the need to preserve freedom through the promotion of solidarity and cooperation between programmers<sup>39</sup>. One of the most significant advances in the movement was the development of a licence that made free software protected by copyright law (renamed copyleft): the General Public License (GPL)<sup>40</sup>.

However, a growing number of programmers that also believed software should be made openly accessible started to see Stallman's moral arguments – seen as too confrontational - as an obstacle to their idea becoming more widely accepted. Thus, a more pragmatist approach arose, coining the term open-source software (OSS).

For the OSS movement, access to the source code was a means to an end: the advancement of the state-of-the-art in the technological field. This came from the perception that more people tamed the complexity of software development<sup>41</sup>. What is attributed by some as the largest accomplishment of OSS was the development of Linux by the programmer Linus Torvalds, proving that decentralised, iterative development of complex software is possible<sup>42</sup>.

The OSS movement founded the Open-Source Initiative, responsible for upholding the OSS definition. OSS licences must comply with ten guiding prin-

---

36 RAYMOND, E. A brief history of hackerdom. *Open Sources: Voices from the Open Source Revolution*. 1999.

37 Idem, *ibidem*.

38 LEVY, Steven. **Hackers: Heroes of the computer revolution**. Garden City, NY: Anchor Press/Doubleday, 1984.

39 STALLMAN, Richard. The GNU manifesto. 1985. Available at: [gnu.org/philosophy/fsfs/rms-essays.pdf](http://gnu.org/philosophy/fsfs/rms-essays.pdf). Accessed on 15 oct. 2023.

40 STALLMAN, Richard. Copyleft: pragmatic idealism. Available at: [gnu.org/philosophy/fsfs/rms-essays.pdf](http://gnu.org/philosophy/fsfs/rms-essays.pdf). Accessed on 15 oct. 2023.

41 Idem, *ibidem*.

42 TORVALDS, Linus. The linux edge. **Communications of the ACM**, v. 42, n. 4, p. 38-39, 1999.



ciples. The licence needs to allow for (i) free redistribution and (ii) access to the source code, ensuring that derived programs (iii) are also licensed as OSS and (iv) that integrity of the initial source code authorship is maintained. There is a prohibition of (v) discrimination against people or (vi) fields of endeavour. Furthermore, OSS must (vii) be redistributed independently of the execution of additional licences. The licences must (viii) not be product-specific and must (ix) not restrict the distribution of other software. Lastly, licences must (x) be technologically neutral<sup>43</sup>.

Regarding the impact of the open-source movement in AI, it is important to note that artificial intelligence is significantly different from traditional software. Thus, the definition of open-source AI does not involve a mere extension of the concept of OSS for a new technology<sup>44</sup>. In part, this happens because AI development involves many different steps - such as data curation, model training and fine-tuning. Open sourcing a pre-trained model does not mean that critical design choices such as data labelling and Reinforcement Learning from Human Feedback (RLHF) documentation is made auditable or even publicly accessible. In this sense, three ideas can be associated with the application of the term “open” in the AI field: open as transparent, open as reusable and open as extensible (as in the allowance of modifications)<sup>45</sup>.

Open-source strategies are present since the core of AI development, providing basic frameworks - such as TensorFlow and Pytorch. Both applications can be traced back to big tech: TensorFlow was developed by Google<sup>46</sup> and Pytorch by Meta<sup>47</sup>. This pattern - software developed by big tech companies becoming publicly available with traditional OSS licences - is repeated many times in the AI industry.

For big tech companies, owning the infrastructure and becoming the leader of setting *de facto* standards is valuable, as it provides for easier integration of research developments into their proprietary products and services. Thus, the term open-source in the AI field is, at least to an extent, being captured by big tech companies not for the principles associated with the OSS movement - those

---

43 THE Open Source Definition (Annotated). Open Source Initiative, 2023. Available at: <https://opensource.org/definition-annotated/>. Accessed on 15 oct. 2023.

44 DEEP Dive: AI Webinar Series. Open Source Initiative, 2023. Available at: <https://opensource.org/events/deep-dive-ai-webinar-series-2023/>. Accessed on 15 oct. 2023.

45 WIDDER, David Gray; WEST, Sarah; WHITTAKER, Meredith. Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI. 2023. Available at: <https://ssrn.com/abstract=4543807>. Accessed on 15 oct. 2023.

46 CHINTALA, Soumith. Pytorch strengthens its governance by joining the Linux Foundation. Pytorch, 2022. Available at: <https://pytorch.org/blog/PyTorchfoundation/>. Accessed on 15 oct. 2023.

47 ABADI, Martín et al. Tensorflow: Large-scale machine learning on heterogeneous distributed systems. **arXiv preprint arXiv:1603.04467**, 2016.

of decentralisation and technological democratisation - but for the competitive value it promotes<sup>48</sup>.

Open-source initiatives are also relevant in the creation of datasets that can later be used to train AI models, such as The Pile or the Common Crawl dataset. Although databases that are publicly available and auditable are extremely relevant for open-source AI development, they do not solve the problems associated with extensive data collection, such as privacy concerns. Moreover, to effectively be used to train an AI model, these datasets usually need further curation, mainly through human labour-intensive processes<sup>49</sup>.

The development of open-source AI systems has escalated after Meta made the source code of their model LLaMA, available to the public, but with the model weights subject to access control. Within a week, they were leaked<sup>50</sup>. Many open-source developments arose, and Stanford released Alpaca, fine tuning LLaMA with costs as low as U\$600<sup>51</sup>. Much was said about the possibility of average people fine tuning pre-trained open-sourced AI models for their personalised goals with no need for specialised hardware. The extent of the accuracy of this information is questionable<sup>52</sup>. One illuminating example is that running a single chatbot based on Stanford Alpaca has been deemed so resource-intensive, due to the inference costs, that the initiative was discontinued<sup>53</sup>.

Given this context, whether open-source AI is independent from big tech can be challenged on many grounds<sup>54</sup>. From TensorFlow and Pytorch to LLaMA, open-source AI has been building on the shoulders of big tech-led initiatives. However, modifying and building upon a model is quite different from developing one from scratch, and it is yet to be proved that AI systems could be developed completely outside of the big tech infrastructure, both due to *de facto* standards and due to computational costs. Even those open-source AI models that were developed more independently, such as GPTNeo from EleutherAI, do

---

48 WIDDER, David Gray; WEST, Sarah; WHITTAKER, Meredith. Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI. 2023. Available at: <https://ssrn.com/abstract=4543807>. Accessed on 15 oct. 2023.

49 LUCCIONI, Alexandra Sasha; VIVIANO, Joseph D. What's in the Box? A Preliminary Analysis of Undesirable Content in the Common Crawl Corpus. **arXiv preprint arXiv:2105.02732**, 2021.

50 VINCENT, James. Meta's powerful AI language model has leaked online – what happens now? The Verge, 2023. Available at: <https://www.theverge.com/2023/3/8/23629362/meta-ai-language-model-llama-leak-online-misuse>. Accessed on 15 oct. 2023.

51 INSTRUCT-TUNE LLaMA on consumer hardware. GitHub, 2023. Available at: <https://github.com/tloen/alpaca-lora>. Accessed on 15 oct. 2023.

52 EDWARDS, Benj. You can now run a GPT-3-level AI model on your laptop, phone, and Raspberry Pi. Ars Technica, 2023. Available at: <https://arstechnica.com/information-technology/2023/03/you-can-now-run-a-gpt-3-level-ai-model-on-your-laptop-phone-and-raspberry-pi/>. Accessed on 15 oct. 2023.

53 [https://www.theregister.com/2023/03/21/stanford\\_ai\\_alpaca\\_taken\\_offline/](https://www.theregister.com/2023/03/21/stanford_ai_alpaca_taken_offline/). Accessed on 15 oct. 2023.

54 WIDDER, David Gray; WEST, Sarah; WHITTAKER, Meredith. Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI. 2023. Available at: <https://ssrn.com/abstract=4543807>. Accessed on 15 oct. 2023.

not automatically solve the problems associated with AI systems, such as data privacy and others.

Since the traditional OSS movement, open source was never a “pixie dust” for solving problems that arose from technological progress<sup>55</sup>. The same is true for AI. On the one hand, some stakeholders propose that open-source AI models will democratise the technology and, thus, need to be exempt from regulation<sup>56</sup>. On the contrary, other players argue that openness is intrinsically inconvenient in the AI domain, as it amplifies the potential for malicious use<sup>57</sup>. To what extent each of these sides are correct demands further examination of the dual-use character of AI.

### 3. POTENTIAL AND RISKS OF ARTIFICIAL INTELLIGENCE AS A DUAL-USE TECHNOLOGY

For the sake of clarity, the societal impacts of artificial intelligence can be grouped into five overarching categories: (i) development of a sense of autonomy; (ii) power structure; (iii) public safety; (iv) ownership; (v) availability and exploitation of resources.

#### 3.1. AI AND PERSONAL AUTONOMY

The philosophical understanding of autonomy has long been debated, notably by consequentialists and deontologists. Although consequentialism and deontology focus each on different aspects, valuing, respectively, outcomes<sup>58</sup> and internal motivations<sup>59</sup>, both theoretical currents are based on the consideration that humans are rational.

This unbounded rationality paradigm has been questioned by many areas of study, including behavioural economists, that argue that cognitive biases can be leveraged for behavioural interventions<sup>60</sup>. The advent of AI systems widens the scale of these possible modifications, for better or worse. For instance, social

---

55 RAYMOND, Eric. The cathedral and the bazaar. **Knowledge, Technology & Policy**, v. 12, n. 3, p. 23-49, 1999.  
56 PERSPECTIVES on Open Source Regulation in the upcoming EU AI Act. Open Source Initiative, 2023. Available at: <https://opensource.org/perspectives-on-open-source-regulation-in-the-upcoming-eu-ai-act/>. Accessed on 15 oct. 2023.  
57 GOODING, Matthew. Open Source LLMs could make artificial intelligence more dangerous, says ‘godfather’ of AI. Available at: <https://techmonitor.ai/technology/ai-and-automation/open-source-chatgpt-ai-llm-geoffrey-hinton>. Accessed on 15 oct. 2023.  
58 BENTHAM, Jeremy; MILL, John Stuart. **Utilitarianism and other essays**. Penguin UK, 2004.  
59 KANT, Immanuel et al. **Critique of pure reason**. London: JM Dent, 1934.  
60 THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: Improving decisions about health, wealth, and happiness**. Penguin, 2009.

networks algorithms can be used to improve voters' attendance rate<sup>61</sup>, but also to politically manipulate them<sup>62</sup>.

Another concern is that the extensive data collection and algorithmic analysis can lead to chilling effects. For example, LGBTQIA+ people might express themselves differently for fear of being identified as such, being outed in countries that criminalise certain sexual orientations or gender identities<sup>63</sup>. AI can also incentivise behaviours that are not seen as authentic. One example of this was the rise of the so-called NPC lives in social media platforms in Brazil, especially on Tiktok<sup>64</sup>. Repetitive and inauthentic actions were reinforced by the algorithm, as content creators gained views, likes and even monetary compensations, until Tiktok restricted NPC lives' reach as they were seen as degrading.

Finally, an additional remark is that personal autonomy is shaped by the way each person experiences the world through a different lens. This perception of reality *per se* can be influenced by the advent of generative AI models. Ultimately, they may cause disinformation to spread, altering the weight people attribute to some communication channels<sup>65</sup>. Even the reliance of modals of information by themselves might be questioned<sup>66</sup>. For example, deepfakes could alter the examination of documentary proof in judicial. Conversely, synthetic media can also have a range of positive applications, with recognised educational and artistic uses<sup>67</sup>.

### 3.2. AI AND POWER STRUCTURES

AI is a human-created concept. As such, it is influenced by the power structures that underlie society. However, algorithms are not static. Rather, they shape these same structures that fostered or hindered their creation. They are

---

61 HAENSCHEN, Katherine. Social pressure on social media: Using Facebook status updates to increase voter turnout. **Journal of Communication**, v. 66, n. 4, p. 542-563, 2016.

62 WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. *The Guardian*, 2019. Available at: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Accessed on 15 oct. 2023.

63 ASSUNÇÃO, Isadora; FICO, Bernardo. A case for regulation: impacts of Artificial Intelligence on the LGBTQIA+ Community. Available at: [https://legaltechcenter.net/files/sites/159/2022/06/Assuncao\\_Fico\\_A\\_Case\\_for\\_Regulation\\_Impacts\\_of\\_AI\\_on\\_the\\_LGBTQIA\\_Community.pdf](https://legaltechcenter.net/files/sites/159/2022/06/Assuncao_Fico_A_Case_for_Regulation_Impacts_of_AI_on_the_LGBTQIA_Community.pdf). WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. *The Guardian*, 2019. Available at: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Accessed on 15 oct. 2023.

64 HOFF, Nicole. Dancers and video game characters merge in the uncanny valley. *The NY Times*, 2023. Available at: <https://www.nytimes.com/2023/10/06/arts/dance/tiktok-dancers-imitating-video-game-characters.html>. Accessed on 15 oct. 2023.

65 CHESNEY, Bobby; CITRON, Danielle. Deep fakes: A looming challenge for privacy, democracy, and national security. **Calif. L. Rev.**, v. 107, p. 1753, 2019.

66 KERNER, Catherine; RISSE, Mathias. Beyond porn and discreditation: Epistemic promises and perils of deepfake technology in digital lifeworlds. **Moral Philosophy and Politics**, v. 8, n. 1, p. 81-108, 2021.

67 JAIMAN, Ashish. Positive use cases of synthetic media. *Towards Data Science*, 2020. Available at: <https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387>. Accessed on 15 oct. 2023.

engines of transformation, not observational tools<sup>68</sup>. These modifications can be perceived on various levels. At first, it is notable that AI systems embed social biases both due to training data and to the choice of models *per se*<sup>69</sup>. As an increasing number of crucial decisions - from immigration to criminal justice - involve AI systems, these biases can lead to discriminatory unfavourable outcomes for protected groups, having been compared to algorithms of oppression<sup>70</sup>.

Furthermore, AI systems might cause the marginalisation of social groups - especially of minorities - both by exclusion and inclusion. The digital divide causes sectors of population to live in the outside of the realms of highly digitised lives. Situated on the margins of Big Data, they are less accurately represented in datasets. Models trained on these datasets perform differently for these excluded groups, which might lessen their access to services and opportunities, with a loop of further exclusion<sup>71</sup>.

On the opposite side, if sectors are over-represented, such as what happens with black people in datasets used to train predictive policing systems, they may also be subject to unfavourable outcomes, such as increased police contacts<sup>72</sup>. Over-inclusion can also be seen by certain communities as a new form of acculturation and colonialism<sup>73</sup>.

Finally, AI has a significant role of normalising certain values, especially in a world dominated by digital platforms. Par excellence, content moderation AI systems involve trade-offs between essential values - such as freedom of expression and the protection against hate speech<sup>74</sup>. Sometimes, these trade-offs do not reflect practices from minority groups. For example, Twitter's algorithmic content-moderation system banned several drag queens accounts in Brazil, as the words they used to interact with each other was classified as a form of hate speech<sup>75</sup>. Instead, they were just giving new meaning to terms that traditionally were used to oppress them, as an integral part of the socialisation processes in that group.

- 
- 68 SLEE, Tom. The incompatible incentives of private-sector AI. **The Oxford Handbook of Ethics of AI**, p. 106-123, 2020.
- 69 BAROCAS, Solon; SELBST, Andrew D. Big data's disparate impact. **California law review**, p. 671-732, 2016; HOOKER, Sara. Moving beyond "algorithmic bias is a data problem". **Patterns**, v. 2, n. 4, 2021.
- 70 NOBLE, Safiya Umoja. Algorithms of oppression. In: **Algorithms of oppression**. New York university press, 2018.
- 71 LERMAN, Jonas. *Big data and its exclusions*. Stan. L. Rev. Online, v. 66, p. 55, 2013.
- 72 FERGUSON, Andrew Guthrie. *The rise of Big Data policing: surveillance, race and the future of law enforcement*. 1<sup>o</sup> ed. Nova York: New York University, 2017, pp. 9-14.
- 73 COULDRY, Nick; MEJIAS, Ulises A. Data colonialism: Rethinking big data's relation to the contemporary subject. **Television & New Media**, v. 20, n. 4, p. 336-349, 2019.
- 74 CITRON, Danielle Keats. Extremist speech, compelled conformity, and censorship creep. **Notre Dame L. Rev.**, v. 93, p. 1035, 2017.
- 75 GOMES, Alessandra *et al.* Drag queens and artificial intelligence: should computers decide what is 'toxic' on the internet? InternetLab, 2019. Available at: <https://internetlab.org.br/en/news/drag-queens-and-artificial-intelligence-should-computers-decide-what-is-toxic-on-the-internet/>. Accessed on 15 oct. 2023.

As seen, AI systems may lead to discrimination and marginalisation of certain societal sectors. However, they can also reshape power structures for good, democratising access to information and providing platforms for voices traditionally unheard of. This has even led Meta to be considered as an extremist organisation in Russia, as its platforms have the potential to empower opposition<sup>76</sup>. The ambivalence is notable.

### 3.3. AI AND PUBLIC SAFETY

AI systems are used in several public security initiatives. One of the most significant uses is in investigative and policing efforts, effectively helping in crime prevention<sup>77</sup>. Nonetheless, several scholars have voiced their concerns that these uses might be a pretext for the creation of an unparalleled and biased surveillance structure<sup>78</sup>.

Furthermore, AI military applications are noteworthy, ranging from autonomous weapons to tools that foster intelligence operations<sup>79</sup>. As many of the existing or proposed regulations provide exemptions for military AI systems<sup>80</sup>, their use occurs outside of public oversight. AI systems can also be applied to other critical areas, such as energy and transportation infrastructure or biotechnology developments. This makes AI systems prone to suffer cyber-attacks from agents that wish to disturb public order, especially in areas of increased geopolitical importance<sup>81</sup>.

Finally, another relevant area is what is called the existential risk of AI systems. The existential risk derives from the potential development of an artificial general intelligence - able to meet human performance in several domains - or even a superintelligence that outperforms humans. Scholars argue that these developments could eventually lead to the demeaning or even to the extinction of humanity if efforts are not carried out to align these systems with human intent<sup>82</sup>. The degree of realism of this proposition has been the object of several discussions, with some positing that the existential risk discourse is no more than

---

76 PERRETT, Connor; CANALES, Katie. A Russian court has declared Meta guilty of extremist activity but will still allow access to Whatsapp. *Insider*, 2022. Available at: <https://www.businessinsider.com/russia-declares-meta-facebook-an-extremist-organization-2022-3>. Accessed on 15 oct. 2023.

77 FERGUSON, Andrew Guthrie. *The rise of Big Data policing: surveillance, race and the future of law enforcement*. 1<sup>o</sup> ed. Nova York: New York University, 2017, pp. 9-14.

78 BRAYNE, Sarah. **Predict and Surveil: Data, discretion, and the future of policing**. Oxford University Press, USA, 2020.

79 SVENMARCK, Peter et al. Possibilities and challenges for artificial intelligence in military applications. In: **Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting**. 2018. p. 1-16.

80 SCOPE of the EU Artificial Intelligence Act. European Center for Not-for-Profit Law, 2023. Available at: [https://ecnl.org/sites/default/files/2022-03/ECNL\\_Pagers\\_on\\_scope\\_of\\_AIA\\_ECNL\\_FINAL.pdf](https://ecnl.org/sites/default/files/2022-03/ECNL_Pagers_on_scope_of_AIA_ECNL_FINAL.pdf). Accessed on 15 oct. 2023.

81 BRUNDAGE, Miles et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. **arXiv preprint arXiv:1802.07228**, 2018.

82 BOSTROM, Nick. Existential risk prevention as global priority. **Global Policy**, v. 4, n. 1, p. 15-31, 2013.

a strategy to shift focus from the already proven concerns, such as algorithmic discrimination and data privacy<sup>83</sup>.

It is notable that safety is the main area that opponents of open-source AI use to claim for the imposition of strict restrictions of these open initiatives. This comes from the perception that, as AI systems are dual-use, and public order is a critical domain to national sovereignty or even to human existence, open-sourcing AI will make these systems more widely available for hostile agents and, thus, it will increase the probability of malicious uses<sup>84</sup>.

### 3.4. AI AND OWNERSHIP

Regarding ownership, AI deeply affects intellectual property rights, as uncertainty exists about the weight that should be attributed to the systems contributions in the process of invention<sup>85</sup>. For example, Dr. Stephen Thaler filed patent applications in several jurisdictions, indicating the DABUS AI system as the sole inventor. Most of them were rejected as it was considered mandatory that inventors are humans<sup>86</sup>. In turn, copyright and AI has been the centre of the debate on the United States Copyright Office (USCO) *Zarya of the Dawn* case. After it was discovered that the images from the comic book had all been created using the generative AI system Midjourney, the USCO considered that these images could not be the subject of copyright protection because the artist did not effectively control the creation process, as “the information in the prompt may ‘influence’ generated image, but prompt text does not dictate a specific result”<sup>87</sup>.

Additionally, AI also impacts workers’ ownership of their labour power. First, some scholars consider that the data extraction structure that underpins AI development is a form of unpaid labour expropriation<sup>88</sup>. Another relevant aspect is that the whole life cycle of an AI system - from its training to its public diffusion - is based on invisible human labour. From the activities of data labelling to that of giving feedback to provide for reinforcement learning, human efforts are involved<sup>89</sup>. After an AI system is deployed to the public, moderation structures

---

83 FEARS about AI’s existential risk are overdone, says a group of experts. *The Economist*, 2023. Available at: [Fears about AI’s existential risk are overdone, says a group of experts \(economist.com\)](https://www.economist.com/technology-and-science/2023/10/15/fears-about-ais-existential-risk-are-overdone-says-a-group-of-experts). Accessed on 15 oct. 2023.

84 BRUNDAGE, Miles et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*, 2018.

85 ABBOTT, RYAN. I Think, Therefore I Invent: Creative Computers and the Future of Patent Law, 57 B.C. L. Ver. 1079 (2016). Pp. 1092 – 1099; 1103 – 1113.

86 DI IULIO, Marco Fioravante Villela. Parecer nº 00024/2022/CGPI/PFE-INPI/PGF/AGU. *Revista Rede de Direito Digital, Intelectual & Sociedade*, v. 2, n. 4, p. 303-314, 2022.

87 UNITED STATES COPYRIGHT OFFICE. *Zarya of the Dawn* Letter, 2023.

88 POSNER, Eric; WEYL, Eric. *Radical markets: Uprooting capitalism and democracy for a just society*. Princeton University Press, 2018.

89 STEPHENS, Elizabeth. The mechanical Turk: A short history of ‘artificial artificial intelligence’. *Cultural Studies*, v. 37, n. 1, p. 65-87, 2023.

may need to be established, with humans making the behind-the-scenes decisions of whether an information (for example, content generated from AI tools) is abusive or not<sup>90</sup>.

### 3.5. AI AND RESOURCES' AVAILABILITY AND EXPLOITATION

The computational costs associated with AI development and deployment contribute to a concentrated structure, with wide gaps between industrial and research stakeholders, between for-profit and non-profit organisations and even between countries. Thus, AI can generate a new form of technological dependence. One example of this is the role of *de facto* and *de jure* standardisation<sup>91</sup>. Both commercial and geopolitical dispute can be seen in the standardisation process, *v.g.*, Meta's efforts to determine the *de facto* standard for AI development environments with PyTorch and China's incorporation of international standardisation organisations as a central part of their external geopolitical strategies<sup>92</sup>. However, the same phenomena that generates dependency can be incorporated into a strategy to further emergent countries' positions in the geopolitical scene, both by national initiatives that promote AI innovation and by leveraging mineral and natural resources' availability, from which AI deeply depends on<sup>93</sup>.

With computational costs, comes the exploitation of environmental resources, many of them finite and non-renewable. Training a single BERT model, without fine-tuning, is estimated to require the energy of a trans-continental flight<sup>94</sup>. That is not to mention the resource consumption of running a widely used interface, such as ChatGPT, which surpasses the training cost of the GPT-4 model on a weekly basis due to the cost of inferences<sup>95</sup>. This makes balancing AI and environmental protection a pressing need.

Based on an exploration of the potential benefits and risks associated with AI systems, a foundation is set to provide for a more well-informed consideration about the regulation of an intrinsically dichotomic technology.

---

90 KLONICK, Kate. The new governors: The people, rules, and processes governing online speech. *Harv. L. Rev.*, v. 131, p. 1598, 2017.

91 EBERS, Martin. Standardizing AI-The Case of the European Commission's Proposal for an Artificial Intelligence Act. **The Cambridge handbook of artificial intelligence: global perspectives on law and ethics**, 2021.

92 RÜHLIG, Tim. Chinese influence through technical standardization power. **Journal of Contemporary China**, v. 32, n. 139, p. 54-72, 2023.

93 FATIMA, Samar; DESOUZA, Kevin C.; DAWSON, Gregory S. National strategic artificial intelligence plans: A multi-dimensional analysis. **Economic Analysis and Policy**, v. 67, p. 178-194, 2020.

94 STRUBELL, Emma; GANESH, Ananya; MCCALLUM, Andrew. Energy and policy considerations for deep learning in NLP. **arXiv preprint arXiv:1906.02243**, 2019.

95 PATEL, Dylan; AHMAD, Afzal. The Inference Cost Of Search Disruption—Large Language Model Cost Analysis. 2023.



## 4. A PROPOSAL FOR A REGULATORY FRAME ACCORDANT TO A JANUS-FACED ARTIFICIAL INTELLIGENCE

The dichotomies that pervade AI from its development to its applications imply significant challenges for the proposition of an overarching regulatory framework. In this section, a tentative effort to establish general directives will be made. The setting of a foundation entails, by itself, significant limitations: there is need for further work to be centred around the specificities of implementing this suggestion in each different legal order.

### **Principle 1. A combination of *ex ante* and *ex post* regulatory mechanisms is required.**

*Ex ante* regulations are essential to prevent the occurrence of systemic harms and to mitigate the likelihood of these events, especially those with outstanding consequences<sup>96</sup>. These mechanisms could involve mandatory documentation of the whole life cycle of an AI system, from its development to its deployment and eventual discontinuation. These records might have various formats and could involve from data provenance information to the registration of statistical tests carried out to assess the existence of algorithmic bias<sup>97</sup>. Further on, disclosure and transparency obligations are relevant, so regulators are aware of the initiatives occurring in any given moment, which makes efficient monitoring and enforcement possible. It is even possible that regulators establish pre-market approval structures for the AI applications deemed critical, similar to what happens in the pharmaceutical domain<sup>98</sup>.

However, as mentioned, rationality is bounded. Moreover, there is an inherent information asymmetry between regulators and the agents subject to regulation, including due to divergent aims<sup>99</sup>. Thus, no regulator - as well equipped as it could be - is able to address all possible events. With regards to AI systems, apart from the risks outlined above, the models could also develop emergent unexpected capabilities, which might be able to propagate in scale and be deployed across different scopes<sup>100</sup>. It is not only a question of risk, but of uncertainty.

---

96 SCHWARCZ, Steven L. Keynote Address: "Ex Ante versus Ex Post Approaches to Financial Regulation"-Friday, January 28, 2011. **Chap. L. Rev.**, v. 15, p. 257, 2011.

97 MITCHELL, Margaret et al. Model cards for model reporting. In: **Proceedings of the conference on fairness, accountability, and transparency**. 2019. p. 220-229.

98 TUTT, Andrew. An FDA for algorithms. **Admin. L. Rev.**, v. 69, p. 83, 2017.

99 SIMON, Herbert A. Bounded rationality. **Utility and probability**, p. 15-18, 1990.

100 ANDERLJUNG, Markus et al. Frontier AI regulation: Managing emerging risks to public safety. **arXiv preprint arXiv:2307.03718**, 2023.

In this context, a combination with *ex post* mechanisms, centred on liability regimes, becomes essential, much like in the regulation of financial markets. Civil and administrative sanctions can lead to effective reparations, and pose a preventive role, such as with the punitive damages in the Common Law framework. To advance both reparative and preventative objectives, it is crucial to institute procedural rights so people adversely impacted by AI systems can seek redress through both collective and individual legal actions.

**Principle 2. There is no universal regime adequate for the wide range AI applications.**

The potential AI applications encompass a broad range of domains and are diverse even on a given domain. Just as different transactions are assigned to different governance structures so as to economise<sup>101</sup>, an adequate regulatory framework must set forth distinct regimes for AI systems. Considerations must be based on the general field of endeavour (for example, education, infrastructure, etc.) and on the risks associated with a particular system.

Thus, to define the categories that will be associated with stricter or more flexible regimes, it is necessary to balance the costs and benefits of a given AI system, identifying risk categories that will need different mitigation strategies to achieve risk levels deemed technically and socially acceptable<sup>102</sup>. This leads to less burdensome regulations, with reduced compliance costs, that are less prone to stifle innovation.

**Principle 3. Regulatory hybridism is necessary, but not sufficient: the State maintains a substantial role.**

State-centric regulation has come to several shortcomings in the contemporary era. In summary, the domains to be regulated are characterised by increasing causal complexity and involve interdependencies between multiple agents. Due to the fragmentation of power in several fronts, there has been a shift from national hierarchical regulations to transnational heterarchical ones, some of them parallel to any governmental involvement. Furthermore, the static view of command-and-control regulation shifted to a more realistic recognition that agents are autonomous and reactive, acting upon regulation, sometimes to comply with it, but also to circumvent it<sup>103</sup>.

---

101 WILLIAMSON, Oliver E. Transaction cost economics. **Handbook of industrial organization**, v. 1, p. 135-182, 1989.

102 SUNSTEIN, Cass. Risk and Reason: Safety, Law and the Environment. Nova York: Cambridge University Press, 2002, pp. 4-8.

103 BLACK, Julia. Decentring regulation: Understanding the role of regulation and self-regulation in a 'post-regulatory' world. **Current legal problems**, v. 54, n. 1, p. 103-146, 2001.

Initially, this led many to affirm the “hollowing out” of the State. However, it has been noted that regulations have not decreased. Instead, they have been growing both in scale and in scope, through what is called hybrid regulation<sup>104</sup>. Hybridism involves regulation with the participation of different agents, sometimes on rule-making, others in rule-monitoring and some even in rule-enforcement. What is common between the many stakeholder combinations is that States still maintain a substantial role, with direct and indirect influence on regulation<sup>105</sup>.

With the advent of cyberspace, utopian libertarianism affirmed that States not only *should not* regulate the new digital technologies, but that they *could not* do so<sup>106</sup>. An empiric examination shows otherwise. For example, several regulations arised centred around data processing<sup>107</sup>, encryption techniques<sup>108</sup> and digital piracy<sup>109</sup>. It may be that complete state control is not possible, but efficient control is achievable, especially by regulations that involve inputs coming from multiple stakeholders.

The same holds true for AI systems. Especially due to the highly technical attributes of the AI field, academia and industry agents must participate in the regulatory process. Users and other people affected by the technology will be the ones to bear the negative consequences in the end, so it is of paramount importance that civil society should be consulted as well. Not every technological aspect can or should be regulated, but it is essential to identify areas that involve not only technical divergences, but also trade-offs between important social values, so they can be subjected to a deliberative rule-making process, instead of being delegated to private stakeholders located outside of public hindsight.

#### **Principle 4. Regulation should prioritise the underlying structural elements, not merely the substantial conduct.**

One of the central aspects that made hybrid regulations effective in the initial development of cyberspace was the focus on indirect and structural regula-

---

104 LEVI-FAUR, David. From “big government” to “big governance?”. *In*: LEVI-FAUR, David [org.]. *The Oxford Handbook on Governance*. Oxford University Press: 2012.

105 LEVI-FAUR, David. Regulation and regulatory governance. **Handbook on the Politics of Regulation**, v. 1, n. 1, p. 1-25, 2011.

106 LESSIG, Lawrence. **Code: And other laws of cyberspace**. 2009.

107 EUROPEAN PARLIAMENT. General Data Protection Regulation. Available at: <https://gdpr-info.eu/>. Accessed on 15 oct. 2023.

108 KARSTEN, Jack; WEST, Darrell. A brief history f US encryption policy. Brookings, 2016. Available at: <https://www.brookings.edu/articles/a-brief-history-of-u-s-encryption-policy/>. Accessed on 15 oct. 2023.

109 UNITED STATES OF AMERICA. Digital Millenium Copyright Act. Available at: <https://www.copyright.gov/dmca/>. Accessed on 15 oct. 2023.

tion<sup>110</sup>. The architecture of digital technologies is different from other regulatory domains and might pose obstacles to the regulation of specific behaviours. With regards to AI, developers and users might not always be immediately identifiable, which turns command-and-control regulations, centred on sanctioning undesirable conducts, not ideal in terms of effectiveness. With the increase of open-source AI, this can be an even more prevalent concern.

Instead, States should focus on regulating the structure that underlies the development of AI systems and the provision of public or commercial applications. For example, regulating the architecture of AI technologies might involve mandating that AI systems available to the public promote identification and authentication of the users, so that *ex post* enforcement mechanisms can be effective at acting upon eventual illicit behaviours. In sum, structure builds substance<sup>111</sup>. Thus, regulating AI systems' architecture can be used indirectly to favour further substantial actions, if needed be.

### **Principle 5. Diversity in regulatory mechanisms is imperative to counter variability in development and application.**

Aligned with the need for hybrid regulations focused on structure rather than substance is the importance of non-monolithic regulations. Diverse regulatory mechanisms should be established, and combinations between different instruments should be prioritised<sup>112</sup>. When possible, regulation should also be redundant, so that if one mechanism fails, there are others to prevent troublesome consequences.

Some noteworthy strategies are proceduralization and collibration. Proceduralization involves regulating the process, instead of the outcome, which is accordant to a structural regulatory framework<sup>113</sup>. Procedural rules, such as those centred around data handling, statistical testing of the models, human oversight mechanisms, etc., might be effective to promote intended outcomes (such as the absence of algorithmic discrimination). Another relevant procedural mechanism is the obligation to perform an algorithmic impact assessment periodically or to be subject to auditing by notified bodies from time to time.

In turn, collibration involves identifying antagonistic forces in a field, examining the current relation between them, and steering this relation to a

---

110 LESSIG, Lawrence. **Code: And other laws of cyberspace**. 2009.

111 LESSIG, Lawrence. **Code: And other laws of cyberspace**. 2009.

112 BLACK, Julia. Decentring regulation: Understanding the role of regulation and self-regulation in a 'post-regulatory' world. **Current legal problems**, v. 54, n. 1, p. 103-146, 2001.

113 BLACK, Julia. Proceduralizing regulation: part I. **Oxford journal of legal studies**, v. 20, n. 4, p. 597-614, 2000.

different and more favourable configuration<sup>114</sup>. This influence can be done in various ways, using sanctions or incentives. For example, one could make the largest players in a field be subject to a stricter and more burdensome regulatory regime to promote newcomers. For example, this is what is done by the Digital Markets Act in the European Union. Alternatively, one could use tax incentives to promote redistribution of the resources needed to develop some initiative. Regarding the AI field, collibration can be a useful mechanism to disrupt big tech's dominance, promoting open-source development. The incentives could be conditioned on following a set of procedural rules, such as ones that focus on identifiability and traceability, in order to address the risks that are specific to open-source AI models.

**Principle 6. The pace of regulatory adaptation must align with the rapid rate of technological innovation.**

A usual problem that is associated with regulation is that legal rule-making is a lengthy process. This might lead to the enactment of regulations that come to exist in an already outdated manner. In the technological field, this has been a pervasive problem, due to fast-paced innovation. To mitigate this pace incompatibility, regulation should be as technologically neutral as possible, avoiding definitions related strictly to currently available techniques.

In addition to that, regulators can also proceed in innovative manners<sup>115</sup>. One suggestion is to combine experimental regulations to regulatory sandboxes. For example, one can devise a controlled trial to examine the impacts of a new proposed regulation. To proceed with the trial, a regulatory sandbox can be established, in which participants are not subject to the full range of obligations or sanctions that they would if the regulation was enacted in a traditional way. Other than that, sunset clauses might impose the need for periodic review of the regulation by a specific commission, to evaluate if it is still adequate to the current technological scenario.

Retrospective reviews of the implementation of all these principles can lead to iterative improvements in regulatory processes<sup>116</sup>, striking a balance between the mitigation of risks and the promotion of technological progress.

---

114 DUNSIRE, Andrew. **Manipulating social tensions: Collibration as an alternative mode of government intervention**. MPIFG discussion paper, 1993.

115 RANCHORDAS, Sofia. Innovation-friendly regulation: The sunset of regulation, the sunrise of innovation. *Jurimetrics*, v. 55, p. 201, 2014.

116 SUNSTEIN, Cass R. **The cost-benefit revolution**. Cambridge: MIT press, 2018.

## 5. CONCLUSION

The article identifies a double dichotomy pervasive to AI: it is a dual-use technology being developed by antagonistic forces. It proceeds to analyse the relation of proprietary AI models to the dominance of large technological companies - the big tech industry. Further, the opposition that the movement of open-source AI poses to the big tech companies is contrasted to the intricate ties open-source happens to have with the dominant industry players by themselves. Moving to the dual-use nature of the technology, a taxonomy of the societal impacts AI poses is made, highlighting five areas of both great potential and significant risks: personhood, dominance structures, public safety, ownership, and financial and environmental resources.

Based on these foundations, a proposal for an adequate regulation is made, centred on the combination of *ex ante* and *ex post* mechanisms. Different regimes for different risk categories are deemed necessary, with the proposition of hybrid and diverse regulatory strategies to counter variety in AI development and application. The focus is shifted from a command-and-control direct regulation to an indirect process that prioritises structure instead of substance. Additionally, mechanisms to make regulation compatible with fast-paced innovations are suggested, such as regulatory sandboxes, experimental regulation, and sunset clauses. Given the foregoing, it is imperative to adapt regulation to the dynamic and Janus-faced nature of the technology they aim to govern.

## REFERENCES

- ABADI, Martín et al. Tensorflow: Large-scale machine learning on heterogeneous distributed systems. arXiv preprint arXiv:1603.04467, 2016.
- ABBOTT, RYAN. I Think, Therefore I Invent: Creative Computers and the Future of Patent Law, 57 B.C. L. Ver. 1079 (2016). Pp. 1092 – 1099; 1103 – 1113.
- AN EXPLORATION of acquisitions by big tech companies. The GAFAM Empire, 2023. Available at: <https://gafam.theglassroom.org/-/timelines-of-expansion>. Accessed on 15 oct. 2023.
- ANDERLJUNG, Markus et al. Frontier AI regulation: Managing emerging risks to public safety. arXiv preprint arXiv:2307.03718, 2023.
- ARAFI, Mohamed; ARMSTRONG, Crystal. “ Facebook to Mobilize, Twitter to Coordinate Protests, and YouTube to Tell the World”: New Media, Cyberactivism, and the Arab Spring. Journal of Global Initiatives: Policy, Pedagogy, Perspective, v. 10, n. 1, p. 6, 2016.
- ARTIFICIAL INTELLIGENCE. Google Trends, 2023. Available at: <https://trends.google.com.br/trends/explore?date=today%205-y&q=ai&chl=pt>. Accessed on 15 oct. 2023.
- ASSUNÇÃO, Isadora; FICO, Bernardo. A case for regulation: impacts of Artificial Intelligence on the LGBTQIA+ Community. Available at: [https://legaltechcenter.net/files/sites/159/2022/06/Assuncao\\_Fico\\_A\\_Case\\_for\\_Regulation\\_Impacts\\_of\\_AI\\_on\\_the\\_LGBTQIA\\_Community.pdf](https://legaltechcenter.net/files/sites/159/2022/06/Assuncao_Fico_A_Case_for_Regulation_Impacts_of_AI_on_the_LGBTQIA_Community.pdf).
- WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. The Guardian, 2019. Available at: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Accessed on 15 oct. 2023.

BAROCAS, Solon; SELBST, Andrew D. Big data's disparate impact. *California law review*, p. 671-732, 2016;

HOOKE, Sara. Moving beyond "algorithmic bias is a data problem". *Patterns*, v. 2, n. 4, 2021.

BEARD, Alison. Can Big Tech be disrupted? Available at: <https://hbr.org/2022/01/can-big-tech-be-disrupted>. Accessed on 15 oct. 2023.

BENTHAM, Jeremy; MILL, John Stuart. *Utilitarianism and other essays*. Penguin UK, 2004.

BLACK, Julia. Decentering regulation: Understanding the role of regulation and self-regulation in a 'post-regulatory' world. *Current legal problems*, v. 54, n. 1, p. 103-146, 2001.

\_\_\_\_\_. Proceduralizing regulation: part I. *Oxford journal of legal studies*, v. 20, n. 4, p. 597-614, 2000.

BOSTROM, Nick. Existential risk prevention as global priority. *Global Policy*, v. 4, n. 1, p. 15-31, 2013.

BRAYNE, Sarah. *Predict and Surveil: Data, discretion, and the future of policing*. Oxford University Press, USA, 2020.

BRUNDAGE, Miles et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228, 2018.

CHESBROUGH, Henry William. *Open innovation: The new imperative for creating and profiting from technology*. Cambridge: Harvard Business Press, 2003.

CHESNEY, Bobby; CITRON, Danielle. Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif. L. Rev.*, v. 107, p. 1753, 2019.

CHINTALA, Soumith. Pytorch strengthens its governance by joining the Linux Foundation. Pytorch, 2022. Available at: <https://pytorch.org/blog/PyTorchfoundation/>. Accessed on 15 oct. 2023.

CITRON, Danielle Keats. Extremist speech, compelled conformity, and censorship creep. *Notre Dame L. Rev.*, v. 93, p. 1035, 2017.

COULDRY, Nick; MEJIAS, Ulises A. Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, v. 20, n. 4, p. 336-349, 2019.

DEEP Dive: AI Webinar Series. Open Source Initiative, 2023. Available at: <https://opensource.org/events/deep-dive-ai-webinar-series-2023/>. Accessed on 15 oct. 2023.

DI IULIO, Marco Fioravante Villela. Parecer nº 00024/2022/CGPI/PFE-INPI/PGF/AGU. *Revista Rede de Direito Digital, Intelectual & Sociedade*, v. 2, n. 4, p. 303-314, 2022.

DUNSIRE, Andrew. *Manipulating social tensions: Collibration as an alternative mode of government intervention*. MPIfG discussion paper, 1993.

EBERS, Martin. Standardizing AI-The Case of the European Commission's Proposal for an Artificial Intelligence Act. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*, 2021.

EDWARDS, Benj. You can now run a GPT-3-level AI model on your laptop, phone, and Raspberry Pi. *Ars Technica*, 2023. Available at: <https://arstechnica.com/information-technology/2023/03/you-can-now-run-a-gpt-3-level-ai-model-on-your-laptop-phone-and-raspberry-pi/>. Accessed on 15 oct. 2023.

EU AI ACT: first regulation on artificial intelligence. European Parliament, 2023. Available at: <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>. Accessed on 15 oct. 2023.

EUROPEAN PARLIAMENT. *General Data Protection Regulation*. Available at: <https://gdpr-info.eu/>. Accessed on 15 oct. 2023.

FARRELL, Joseph; KLEMPERER, Paul. Coordination and lock-in: Competition with switching costs and network effects. *Handbook of industrial organization*, v. 3, p. 1967-2072, 2007.

FATIMA, Samar; DESOUZA, Kevin C.; DAWSON, Gregory S. National strategic artificial intelligence plans: A multi-dimensional analysis. *Economic Analysis and Policy*, v. 67, p. 178-194, 2020.

FEARS about AI's existential risk are overdone, says a group of experts. *The Economist*, 2023. Available at: <https://www.economist.com/news/2023/10/15/fears-about-ai-existential-risk-are-overdone>. Accessed on 15 oct. 2023.

FENTON, Susan. Apple, Microsoft remain world's top 2 companies by market cap. Reuters, 2023. Available at: <https://www.reuters.com/technology/global-markets-marketcap-2023-08-01/>. Accessed on 15 oct. 2023.

FERGUSON, Andrew Guthrie. The rise of Big Data policing: surveillance, race and the future of law enforcement. 1<sup>o</sup> ed. Nova York: New York University, 2017, pp. 9-14.

GILMAN, Nils; CERVENY, Ben. Tomorrow's democracy is open source. Noema, 2023. Available at: <https://www.noemamag.com/tomorrows-democracy-is-open-source/>. Accessed on 15 oct. 2023.

GOMES, Alessandra et al. Drag queens and artificial intelligence: should computers decide what is 'toxic' on the internet? InternetLab, 2019. Available at: <https://internetlab.org.br/en/news/drag-queens-and-artificial-intelligence-should-computers-decide-what-is-toxic-on-the-internet/>. Accessed on 15 oct. 2023.

GOODING, Matthew. Open Source LLMs could make artificial intelligence more dangerous, says 'god-father' of AI. Available at: <https://techmonitor.ai/technology/ai-and-automation/open-source-chatgpt-ai-llm-geoffrey-hinton>. Accessed on 15 oct. 2023.

GU, Hongfei. Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese Political Science*, p. 1-22, 2023.

HAENSCHEN, Katherine. Social pressure on social media: Using Facebook status updates to increase voter turnout. *Journal of Communication*, v. 66, n. 4, p. 542-563, 2016.

HOFF, Nicole. Dancers and video game characters merge in the uncanny valley. *The NY Times*, 2023. Available at: <https://www.nytimes.com/2023/10/06/arts/dance/tiktok-dancers-imitating-video-game-characters.html>. Accessed on 15 oct. 2023.

HOOKER, Sara. The hardware lottery. *Communications of the ACM*, v. 64, n. 12, p. 58-65, 2021.

INSTRUCT-TUNE LLaMA on consumer hardware. GitHub, 2023. Available at: <https://github.com/tloen/alpaca-lora>. Accessed on 15 oct. 2023.

JAIMAN, Ashish. Positive use cases of synthetic media. *Towards Data Science*, 2020. Available at: <https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387>. Accessed on 15 oct. 2023.

KANT, Immanuel et al. *Critique of pure reason*. London: JM Dent, 1934.

KARSTEN, Jack; WEST, Darrell. A brief history of US encryption policy. Brookings, 2016. Available at: <https://www.brookings.edu/articles/a-brief-history-of-u-s-encryption-policy/>. Accessed on 15 oct. 2023.

KERNER, Catherine; RISSE, Mathias. Beyond porn and discreditation: Epistemic promises and perils of deepfake technology in digital lifeworlds. *Moral Philosophy and Politics*, v. 8, n. 1, p. 81-108, 2021.

KHAN, Lina. The new Brandeis movement: America's antimonopoly debate. *Journal of European Competition Law & Practice*, v. 9, n. 3, p. 131-132, 2018.

KLONICK, Kate. The new governors: The people, rules, and processes governing online speech. *Harv. L. Rev.*, v. 131, p. 1598, 2017.

LERMAN, Jonas. Big data and its exclusions. *Stan. L. Rev. Online*, v. 66, p. 55, 2013.

LESSIG, Lawrence. *Code: And other laws of cyberspace*. 2009.

LEVI-FAUR, David. From "big government" to "big governance"?. In: LEVI-FAUR, David [org.]. *The Oxford Handbook on Governance*. Oxford University Press: 2012.

LEVI-FAUR, David. Regulation and regulatory governance. *Handbook on the Politics of Regulation*, v. 1, n. 1, p. 1-25, 2011.

LEVY, Steven. *Hackers: Heroes of the computer revolution*. Garden City, NY: Anchor Press/Doubleday, 1984.

LUCCIONI, Alexandra Sasha; VIVIANO, Joseph D. What's in the Box? A Preliminary Analysis of Undesirable Content in the Common Crawl Corpus. arXiv preprint arXiv:2105.02732, 2021.

MAFFULLI, Stefano. Meta's LLaMa 2 license is not Open Source. *Voices of Open Source*, 2023. Available at: <https://blog.opensource.org/metals-llama-2-license-is-not-open-source/>. Accessed on 15 oct. 2023.

MCCARTHY, John et al. A proposal for the Dartmouth summer research project on artificial intelligence, August 31, 1955. *AI magazine*, v. 27, n. 4, p. 12-12, 2006.

MITCHELL, Margaret et al. Model cards for model reporting. In: *Proceedings of the conference on fairness, accountability, and transparency*. 2019. p. 220-229.



MYANMAR: Facebook's systems promoted violence against Rohingya; Meta owes reparations. Amnesty International, 2022. Available at: <https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebook-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/>. Accessed on 15 oct. 2023.

NAZARET, Achille; SAPIRO, Guillermo. A large-scale observational study of the causal effects of a behavioral health nudge. *Science Advances*, v. 9, n. 38, p. eadi1752, 2023.

NOBLE, Safiya Umoja. Algorithms of oppression. In: *Algorithms of oppression*. New York university press, 2018.

PATEL, Dylan; AHMAD, Afzal. Google "We have no moat, and neither does OpenAI". *Semianalysis*, 2023. Available at: <https://www.semianalysis.com/p/google-we-have-no-moat-and-neither>. Accessed on 15 oct. 2023.

\_\_\_\_\_. The Inference Cost Of Search Disruption—Large Language Model Cost Analysis. 2023.

PERRRETT, Connor; CANALES, Katie. A Russian court has declared Meta guilty of extremist activity but will still allow access to Whatsapp. *Insider*, 2022. Available at: <https://www.businessinsider.com/russia-declares-meta-facebook-an-extremist-organization-2022-3>. Accessed on 15 oct. 2023.

PERSPECTIVES on Open Source Regulation in the upcoming EU AI Act. Open Source Initiative, 2023. Available at: <https://opensource.org/perspectives-on-open-source-regulation-in-the-upcoming-eu-ai-act/>. Accessed on 15 oct. 2023.

POPKEN, Ben. Apple is now worth \$2 trillion, making it the most valuable company in the world. *NBC News*, 2020. Available at: <https://www.nbcnews.com/business/business-news/apple-now-worth-2-trillion-making-it-most-valuable-company-n1237287>. Accessed on 15 oct. 2023.

POSNER, Eric; WEYL, Eric. *Radical markets: Uprooting capitalism and democracy for a just society*. Princeton University Press, 2018.

RANCHORDAS, Sofia. Innovation-friendly regulation: The sunset of regulation, the sunrise of innovation. *Jurimetrics*, v. 55, p. 201, 2014.

RAYMOND, Eric. A brief history of hackerdom. *Voices from the Open Source Revolution*. 1999.

\_\_\_\_\_. The cathedral and the bazaar. *Knowledge, Technology & Policy*, v. 12, n. 3, p. 23-49, 1999.

ROGERS, Everett M. *Diffusion of innovations*. New York: Simon and Schuster, 2010.

RUBINSTEIN, Ira. Big data: The end of privacy or a new beginning?. *International Data Privacy Law (2013 Forthcoming)*, NYU School of Law, Public Law Research Paper, n. 12-56, 2012

RÜHLIG, Tim. Chinese influence through technical standardization power. *Journal of Contemporary China*, v. 32, n. 139, p. 54-72, 2023.

SCHWARCZ, Steven L. Keynote Address: "Ex Ante versus Ex Post Approaches to Financial Regulation"-Friday, January 28, 2011. *Chap. L. Rev.*, v. 15, p. 257, 2011.

SCOPE of the EU Artificial Intelligence Act. European Center for Not-for-Profit Law, 2023. Available at: [https://ecn.org/sites/default/files/2022-03/ECNL\\_Pagers\\_on\\_scope\\_of\\_AIA\\_ECNL\\_FINAL.pdf](https://ecn.org/sites/default/files/2022-03/ECNL_Pagers_on_scope_of_AIA_ECNL_FINAL.pdf). Accessed on 15 oct. 2023.

SIMON, Herbert A. Bounded rationality. *Utility and probability*, p. 15-18, 1990.

SLEE, Tom. The incompatible incentives of private-sector AI. *The Oxford Handbook of Ethics of AI*, p. 106-123, 2020.

STALLMAN, Richard. Copyleft: pragmatic idealism. Available at: [gnu.org/philosophy/fsfs/rms-essays.pdf](http://gnu.org/philosophy/fsfs/rms-essays.pdf). Accessed on 15 oct. 2023.

\_\_\_\_\_. The GNU manifesto. 1985. Available at: [gnu.org/philosophy/fsfs/rms-essays.pdf](http://gnu.org/philosophy/fsfs/rms-essays.pdf). Accessed on 15 oct. 2023.

STEPHENS, Elizabeth. The mechanical Turk: A short history of 'artificial artificial intelligence'. *Cultural Studies*, v. 37, n. 1, p. 65-87, 2023.

STRUBELL, Emma; GANESH, Ananya; MCCALLUM, Andrew. Energy and policy considerations for deep learning in NLP. *arXiv preprint arXiv:1906.02243*, 2019.

SUNSTEIN, Cass R. *The cost-benefit revolution*. Cambridge: MIT press, 2018.

\_\_\_\_\_. *Risk and Reason: Safety, Law and the Environment*. Nova York: Cambridge University Press, 2002, pp. 4-8.

SVENMARCK, Peter et al. Possibilities and challenges for artificial intelligence in military applications. In: *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*. 2018. p. 1-16.

TAYLOR, Jack. Big Tech turns its lobbyists loose on Europe, alarming regulators. *The New York Times*, 2020. Available at: <https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html>. Accessed on 15 oct. 2023.

THALER, Richard H.; SUNSTEIN, Cass R. *Nudge: Improving decisions about health, wealth, and happiness*. Penguin, 2009.

THATCHER, Jim; O'SULLIVAN, David; MAHMOUDI, Dillon. Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, v. 34, n. 6, p. 990-1006, 2016.

THE DIGITAL Services Act package. European Commission, 2023. Available at: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. Accessed on 15 oct. 2023.

THE FUTURE of Big Tech. J.P. Morgan, 2022. Available at: <https://www.jpmorgan.com/insights/global-research/technology/future-of-big-tech>. Accessed on 15 oct. 2023.

THE Open Source Definition (Annotated). Open Source Initiative, 2023. Available at: <https://opensource.org/definition-annotated/>. Accessed on 15 oct. 2023.

TORVALDS, Linus. The linux edge. *Communications of the ACM*, v. 42, n. 4, p. 38-39, 1999.

TURING, Alan M. *Computing Machinery and Intelligence*. *Creative Computing*, v. 6, n. 1, p. 44-53, 1980.

TUTT, Andrew. An FDA for algorithms. *Admin. L. Rev.*, v. 69, p. 83, 2017.

UNITED STATES COPYRIGHT OFFICE. *Zarya of the Dawn Letter*, 2023.

UNITED STATES OF AMERICA. *Digital Millenium Copyright Act*. Available at: <https://www.copyright.gov/dmca/>. Accessed on 15 oct. 2023.

VINCENT, James. Meta's powerful AI language model has leaked online – what happens now? *The Verge*, 2023. Available at: <https://www.theverge.com/2023/3/8/23629362/meta-ai-language-model-llama-leak-online-misuse>. Accessed on 15 oct. 2023.

VIPRA, Jai; KORINEK, Anton. Market concentration implications of foundation models. *Brookings*, 2023. Available at: <https://www.brookings.edu/articles/market-concentration-implications-of-foundation-models-the-invisible-hand-of-chatgpt/>. Accessed on 15 oct. 2023.

WASSEN, Donald L. *Janus definition*. *World History Encyclopedia*, 2015. Available at: <https://www.world-history.org/Janus/>. Accessed on 15 oct. 2023.

WHAT is the Blueprint for an AI Bill of Rights? *White House*, 2023. Available at: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>. Accessed on 15 oct. 2023.

WIDDER, David Gray; WEST, Sarah; WHITTAKER, Meredith. *Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI*. 2023. Available at: <https://ssrn.com/abstract=4543807>. Accessed on 15 oct. 2023.

WILLIAMS, Adrienne et al. *The exploited labor behind Artificial Intelligence*. *Noema*, 2022. Available at: <https://www.noemamag.com/the-exploited-labor-behind-artificial-intelligence/>. Accessed on 15 oct. 2023.

WILLIAMSON, Oliver E. *Transaction cost economics*. *Handbook of industrial organization*, v. 1, p. 135-182, 1989.

WONG, Julia Carrie. *The Cambridge Analytica scandal changed the world – but it didn't change Facebook*. *The Guardian*, 2019. Available at: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Accessed on 15 oct. 2023.

WU, Tim. *The master switch: The rise and fall of information empires*. New York: Vintage, 2011.

# GUARDIÃO DA CONSTITUIÇÃO: UMA ANÁLISE DO CONTROLO DA CONSTITUCIONALIDADE ENTRE O CHEFE DO ESTADO E O TRIBUNAL CONSTITUCIONAL EM ANGOLA

DORIVALDO MANUEL “DORIVAL”<sup>1</sup>

## 1. INTRODUÇÃO

Discorrer sobre o Chefe do Estado e o Guardião da Constituição em Angola de modo a enfatizar o garante da constitucionalidade em face da interferência de um órgão sobre o outro, significa evidenciar um exercício preciso para o enriquecimento do Estado Democrático de Direito, concomitantemente da justiça constitucional. Trata-se de um tema fundamentável à luz do Direito Constitucional, e resulta das leituras sobre «jurisdição constitucional» de Hans Kelsen (2003), isto é, quem deve ser o guardião da constituição (o Chefe do Estado ou o Tribunal Constitucional)<sup>2</sup>.

Decerto, a constituição angolana de 2010 proclama que todos os órgãos de soberania do Estado, isto é, o Executivo, Legislativo e Judiciário devem proteger a Constituição em prol da justiça (art. 108.º, art. 141.º e art. 174, da CRA). No domínio do controlo e fiscalização, a Assembleia Nacional “vela pela aplicação da Constituição e pela boa execução das leis” (art. 162.º al. a, da CRA). O Presidente da República, enquanto Chefe do Estado no domínio da competência, “promove junto do Tribunal Constitucional a fiscalização preventiva e sucessiva da constitucionalidade de actos normativos e tratados internacionais, bem como de omissões internacionais, nos termos previsto na constituição” (art. 119.º al. c, da CRA). Entende-se nos artigos descritos, que velar e promover a fiscalização da constitucionalidade não significa ser o guardião da constituição. Pois, a Constituição da República Angolana pressupõe que no domínio da competên-

---

1 Licenciado em Ciência Política pela Faculdade de Ciências Sociais da Universidade Agostinho Neto (2015-2020), Mestrando em Ciências Jurídico-Políticas pela Faculdade de Direito da mesma Universidade (2023-2024). Monitor de Ética e Prática Política, Organizações Regionais Africanas e Organizações Internacionais, na UAN-FCS. É autor da obra «Poder Nacional: contributo do factor-científico para o desenvolvimento sócio-económico e industrial de Angola. Poeta, escritor e ensaísta.

2 É um artigo produzido como relatório do primeiro semestre do Mestrado em Ciências Jurídico-Políticas da Faculdade de Direito da Universidade Agostinho Neto, em Angola.

cia, é o Tribunal Constitucional o guardião da constituição, porque “aprecia a constitucionalidade de quaisquer normas e demais actos do Estado” (art. 181.º al. a, da CRA). Ademais, para além do chefe de Estado promover a fiscalização, de acordo com a Constituição [art. 119.º al e) e art. 181.º al a)], também indica os guardiões da Constituição, ou seja, quatro juízes do Tribunal Constitucional, incluindo o Presidente do Tribunal. Deste modo, olhando para a realidade do sistema judicial angolano sobre o órgão executivo que indica os guardiões que controlam ou fiscalizam os actos do Estado, entendemos produzir por meio dos elementos estruturantes a seguir.

## **2. PROBLEMA DE PESQUISA**

Até que ponto o Chefe do Estado Angolano pode interferir no Tribunal Constitucional durante o controlo da constitucionalidade das leis e actos do Estado?

## **3. JUSTIFICATIVA**

É um trabalho importante, porque pretende-se aperfeiçoar o conhecimento sobre a justiça constitucional e enriquecer o Direito Público na academia angolana. Como dissemos, anteriormente, ao lermos Hans Kelsen em face da discussão com Carl Schmitt, percebemos que o segundo defende o Chefe do Estado como Guardiã da Constituição e o primeiro defende o Tribunal Constitucional (Kelsen, 2003), cuja discussão motivou-nos a produzir para reflexão da sociedade angolana, fundamentalmente a sociedade dos operadores das ciências jurídico-políticas.

## **4. OBJECTIVO GERAL**

- Analisar a possível interferência do Chefe do Estado no Tribunal Constitucional durante o controlo da constitucionalidade das leis e actos do Estado.

### *4.1. OBJECTIVOS ESPECÍFICOS*

- Sistematizar as abordagens teóricas e históricas sobre os guardiões da constituição no quadro do controlo da constitucionalidade;

- Identificar o controlo da constitucionalidade em Angola e modelos de justiça constitucional adotados pelo Estado;

- Analisar a interferência do Presidente da República na actividade do guardião da constituição, tendo em conta a observação dos factos, da constituição e das leis.

## 5. METODOLOGIA E ESTRUTURA DO ARTIGO

A pesquisa do artigo é de natureza qualitativa, adaptamos o método dedutivo/indutivo e através da técnica recorrida a abordagem documental indirecta, coletamos as informações em livros, artigos, legislações, Dissertações de Mestrado e Teses de Doutorado, que nos permitiram estruturar o trabalho em duas secções I e II. No primeiro, sistematizamos os conceitos, abordagens históricas e teorias sobre a justiça constitucional de modo universal. No segundo, identificamos o controlo de constitucionalidade em Angola e analisamos a possível interferência do Chefe do Estado no Tribunal Constitucional durante o controlo da constitucionalidade, tendo em conta as implicações em face da observação da realidade do sistema judicial em Angola.

## 6. JUSTIÇA CONSTITUCIONAL E CONTROLO DA CONSTITUCIONALIDADE

### 6.1. CONSTITUCIONALISMO

A noção conceptual e histórica do constitucionalismo não precede a noção de justiça constitucional e garantias da constitucionalidade. Tal premissa não é insipiente, porque, embora receba subsistência evolutiva com as discussões do contrato social de Hobbes (2003), Locke (2001) e Rousseau (2002), o constitucionalismo pressupõe “uma teoria normativa da política” (Canotilho, (2003:42)<sup>3</sup>, que “visa estabelecer regimes constitucionais” (Manoel Filho, 2012:144).

Nos meandros da génese do Estado Moderno, a despeito do constitucionalismo a “garantia dos direitos fundamentais tornou-se ideia inerente a definição da constituição” (Leandro Ferreira, 2009: 288). Segundo Louis Henkin (*apud* André Tavares, 2012: 26) existem 7 principais exigências para se reconhecer o constitucionalismo e, dentre elas, descrevemos a 4<sup>a</sup> e 6<sup>a</sup> exigência, porque se confluem aos preceitos *a posteriori* da justiça constitucional, tais são:

1. Governo limitado, separação de poderes e *cheks and balances*, controlo civil dos militares, governo das leis e *judicial control*, assim como um Judiciário independente;
2. E instituições que monitorem e assegurem o respeito à Constituição.

Assim, percebe-se que o constitucionalismo em determinados Estados visa ultrapassar o contrato social de Hobbes, limitando e democratizando os poderes em prol da protecção da constituição e controlo da constitucionalidade por órgãos legitimados.

---

3 Gomes Canotilho (ibidem) assevera-nos que existem vários constitucionalismos, deste modo sem descurar os puros, como o constitucionalismo inglês, francês e americano, sendo preferível tratar-se de vários movimentos constitucionais para se chegar a noção básica de constitucionalismo.

### 6.1.1. Constituição

A constituição na literatura do constitucionalismo compreende-se lhe no âmbito histórico inseparável e em vários preceitos, quer na perspectiva Político-liberal com Karl Schmitt, quer na perspectiva sociológica com Ferdinand Lassalle, e sobretudo na perspectiva jurídica com Hans Kelsen e outros (Lassalle, 2013:9-12).

Porém, em face da limitação histórica, faz-se o enquadramento contextual do objecto de estudo, sustentando através de Jorge Miranda que a constituição é “a base da ordem jurídica, o fulcro das suas sinergias, o fundamento último da actividade do Estado” (Miranda, 2008:25)<sup>4</sup>. Ou seja, para Jónatas Machado e Nogueira da Costa, o conceito material de constituição para o legado francês do constitucionalismo liberal,

Assenta na defesa dos direitos fundamentais e do princípio da separação de poderes, a teorização do poder constituinte, a primazia dos direitos fundamentais, a prevalência da lei e a legalidade da administração, a liberdade religiosa e a laicidade do Estado (Machado e da Costa, 2011:26).

Deste modo, é sobre a égide da constituição e os elementos que lhe assentam, que a justiça constitucional torna-se tema relevante, isto é, como preferiu dizer Paulo Bonavides (2004:127), “uma premissa da democracia jurídica e com legitimidade”.

#### 6.1.1.1. *Justiça Constitucional e controlo da constitucionalidade*

Quando se fala de justiça constitucional dá uma certeza de que se fala também de jurisdição constitucional, que pressupõe chegar a instituições, i.e., o Tribunal Constitucional ou aos tribunais legitimados para o controlo da constitucionalidade (Canotilho, 2011). Observando Hans Kelsen (2003), à luz da percepção jurídico-política, tais instituições correspondem ao princípio do Estado de Direito.

Destarte, o controlo da constitucionalidade é uma ideia ligada a supremacia da constituição, e uma espécie de actuação, que verifica a adequação de um acto jurídico à Constituição, que determina o modo de produção da norma infraconstitucional para que seja aprovada e introduzida no ordenamento jurídico, tanto no que diz respeito às regras de competência, quanto no que respeita ao procedimento legislativo, ou actos em forma de lei, inclusive os que só contêm normas individuais, por exemplo, o orçamento e todos aqueles que, por alguma razão, tendem a ser vistos como meros actos administrativos pela doutrina

---

4 Tal conceito conflui-se ao de Aristóteles (1998), segundo o qual, numa perspectiva sócio-real, a constituição é o modo como se constitui uma comunidade, sociedade ou Estado.

tradicional, a despeito de terem forma de lei (De Moraes, 2003, Kelsen, 2003, Machado e da Costa, 2011, Filho, 2012, Bonavides, 2004, Mascarenha, 2008, Agra, 2003).

Nagib Filho (2002:284) defende que os efeitos de inconstitucionalidade são suficientemente compreendidos em face da história. Deste modo, é através da observação histórico-comparativa que percebemos três clássicos modelos de garantia da constitucionalidade. Assim, observando Jorge Miranda, tais são:

1. Modelo de fiscalização política (um modelo francês ligado aos dogmas do constitucionalismo europeu do século XVIII e XIX);
2. Modelo de fiscalização judicial (desenvolvido nos EUA desde 1803);
3. Modelo de fiscalização jurisdicional concentrado em tribunal constitucional (ou austríaco de 1920) estendido na Europa (Miranda, 2008, 217-218).

Cujos modelos de justiça constitucional foram criados para defesa dos Direitos fundamentais e da lei suprema susceptíveis de serem violados por entidades públicas e privadas. Para Bacelar Gouveia (2014:582) há vários critérios de aplicação de inconstitucionalidade<sup>5</sup>: sendo a estrutura do acto inconstitucional por acção e por omissão. A primeira abrange os actos legislativos incompatíveis com o texto constitucional [...], e a segunda, de forma total, configura-se quando o legislador, tendo o dever jurídico de atuar, abstenha-se inteiramente de fazê-lo, deixando um vazio normativo na matéria (Luís Barroso, 2012, 83-87).

Ademais, Machado e Da Costa (2011:330-331) defendem de forma sistemática que os modelos de controlo da constitucionalidade das leis podem ser preventivo (antes da entrada em vigor da lei) ou sucessivo (depois da entrada em vigor da lei), este último pode ser sucessivo abstrato por via principal (Tribunal Constitucional) ou concreto por via incidental (qualquer tribunal) e, quer a preventiva ou sucessiva, confluem-se à inconstitucionalidade por acção e não por omissão.

### **6.1.2. Modelos organizatórios de justiça constitucional**

Embora já descritos em síntese. Porém, importa salientar os legitimados fiscalizadores a partir dos três (o político, judicial e jurisdicional concentrado) ou os dois modelos de controlo judicial difuso e concentrado, que exercem maior influência na jurisdição constitucional em todo mundo (Walber Agra, 2003:56).

---

5 Segundo a lição de LÚCIO BITTENCOURT (*apud* André Tavares, 2012:217), a inconstitucionalidade identifica-se em uma de quatro possíveis situações: "1ª) desrespeito à forma prescrita; 2ª) inobservância de condição estabelecida; 3ª) falta de competência do órgão legiferante; 4ª) violação de direitos e garantias individuais.

O modelo de controlo político é muitas vezes concebido como ineficaz (Manoel Filho, 2012), em que, entre o parlamento e o monarca no cenário de “haver questões de constitucionalidade, elas eram resolvidas ou pelo monarca ou pelo acordo das partes, sem recurso a uma terceira instância” (Blanco de Moraes, 2006:270)<sup>6</sup>. Pois, há controlo difuso, no modelo norte-americano da *judicial review*, quando a qualquer juiz e tribunal compete apreciar a alegação de inconstitucionalidade das leis ou questões jurídico-constitucionais nos processos a eles submetidos, e é concentrado, no modelo europeu, toda vez que a competência para julgar a questão de constitucionalidade é reservada a um único órgão especializado em matérias jurídico-constitucionais (Regina Hirose, 2010, Machado e Da Costa, 2011).

O modelo concentrado foi criado por Hans Kelsen, em 1920, por meio da Constituição austríaca, sendo melhorado com a reforma constitucional de 1929 (Regina Hirose, 2010:37). Kelsen debateu com Carl Schmitt acerca da questão sobre quem deve ser o guardião da constituição (Kelsen, 2003, Bahia, 2004, Amaral, 2014). Seu modelo sobre o tribunal constitucional agrega elementos do modelo de controlo político (pelo Parlamento ou órgão político) e do modelo judicialista (difuso), por ostentar características de órgão jurisdicional diferente de outros tribunais, i.e., pela sua organização e modo de recrutamento dos juízes<sup>7</sup> (Miranda, 2008).

## 6.2. O GUARDIÃO DA CONSTITUIÇÃO: CHEFE DE ESTADO OU TRIBUNAL CONSTITUCIONAL?

Como salientamos anteriormente com as ideias de Walber Agra (2003), tanto o modelo norte-americano de 1803 como o modelo europeu de 1920 exercem maior influência na jurisdição constitucional em todo mundo. O modelo difuso prevaleceu-se como facto adquirido, e o modelo concentrado triunfou-se como problema a partir de 1929 a 1931, isto é, num debate entre Carl Schmitt e seu escrito intitulado “O Guarda da Constituição” e Hans Kelsen com a sua resposta sobre “Quem deve ser o defensor ou o guardião da Constituição” (Maria Amaral, 2014:140).

Carl Schmitt (*apud* Fabiano Furlan, 2010: 132) defendeu que seria o Presidente do Reich ou Chefe de Estado o Guardião da constituição. Porém,

---

6 De acordo com Carlos Blanco de Moraes (ibidem), quanto ao modelo francês, o carácter pactício da actividade legislativa nos regimes dualistas, centrado na co-decisão legiferante entre parlamento (que delibera as normas legais) e o monarca (que as sancionava constitutivamente), dispensava a criação de órgãos supra-partes destinados a resolver controvérsias decorrentes da contradição do direito ordinário e a constituição.

7 No sistema político-jurídico angolano, a questão da organização, recrutamento ou nomeação dos juízes tem gerado muitas discussões dialéticas na academia e sociedade civil, tal questão é sobre o Presidente nomear o juiz guardião, e através desta nomeação haver decisões do tribunal constitucional em favor do governo vigente.



pelos seguintes motivos: o presidente não comprometeria a sua actuação; possuía relativa estabilidade para tecer atuações que não fossem prejudicadas pela permanência no poder; possuía poderes eficientes para atuar em caso de necessidade como legislador extraordinário para os parâmetros de um Estado Legiferante como sistema fechado de legalidade; o princípio democrático seria preservado, já que o Presidente seria eleito pela totalidade do povo; o Presidente representaria um contrapeso para o pluralismo de grupos sociais e económicos de poder, de modo a melhor defender a unidade do povo alemão<sup>8</sup>.

Hans Kelsen (2003:246) ao fazer interpretação do art.º 48 da Constituição do Reich, salienta que as competências, que Carl Schmitt atribuiu ao Presidente, de tal maneira o torna senhor soberano do Estado, tais objectivos não são compatíveis a um guardião da constituição. Assim, pondo em causa os silogismos de Schmitt, defendeu que o guarda da constituição seria um tribunal independente:

Que funciona como um tribunal constitucional central na medida em que, num processo litigioso, deve decidir sobre a constitucionalidade dos atos do parlamento (especialmente leis) ou do governo (especialmente decretos) que tenham sido contestados, cassando atos em caso de sua inconstitucionalidade e eventualmente julgando sobre a responsabilidade de certos órgãos colocados sob acusação (Kelsen, *ibidem*:248).

Apesar de tal discussão merecer abordagem profundamente exaustiva, interessa contextualmente para Angola, observa-se que a questão da visão de Schmitt ficou para atrás e é notável que, em muitos Estados, por conveniência, o Presidente da República mediante o modelo apresentado por Kelsen em coligação com o modelo difuso, nomeia o juiz presidente do tribunal constitucional e demais juizes, facto que poderia, eventualmente, não comprometer a actuação do Chefe do Estado tal como defendeu Carl Schmitt (quanto a neutralidade e independência político-partidária), em casos de decisão de inconstitucionalidade das leis e actos do Estado.

## **7. CONSTITUCIONALISMO E CONTROLO DA CONSTITUCIONALIDADE EM ANGOLA: ANÁLISE ENTRE O CHEFE DO ESTADO E O TRIBUNAL CONSTITUCIONAL**

### *7.1. CONSTITUCIONALISMO EM ANGOLA*

Parafraseando Gomes Canotilho (2003), o constitucionalismo não se esgota nas suas origens puras, porque há vários constitucionalismos, tal como há em Angola, e assentam nos Estados constitucionais, Estados que para Canotilho

---

8 Embora seja observado de tal maneira controversa, é certo que, do ponto de vista ontológico, alguns postulados de Carl Schmitt não parecem inverdades. Pois, defendia que “o Tribunal Constitucional consolidaria uma aristocracia de toga que violaria o princípio democrático, até mesmo pelo seu modo burocrático-aristocrático de organização. Pois evidenciava que a função decisiva do controlo da constitucionalidade representava uma decisão política” (*Schmitt apud* Fabiano Furlan *ibidem*:136).

(1993), fundamentam-se na defesa ou garantias da constituição. Ademais, observando Adérito Correia e Bornito de Sousa (1996), percebe-se o constitucionalismo angolano à luz do estatuto-jurídico enquanto colônia, antes e após da proclamação da independência com a criação da Lei Constitucional de 11 de Novembro de 1975 e suas alterações até a Lei n.º 12/91, de 6 de Março, considerada como nova constituição e aprofundada com a Lei de Revisão Constitucional n.º 23/92, de 16 de Setembro<sup>9</sup>.

### 7.1.1. Jurisdição constitucional

Em países como EUA, Alemanha, Portugal, Itália, Espanha ou Brasil, a jurisdição constitucional por serem devidamente enquadradas, contribuem para construção efetiva de um Estado de Direito Democrático, concomitantemente dos Direitos Fundamentais (Machado, Da Costa e Hilário, 2017:302). Angola, por exemplo, é um Estado de Direito democrático [...] (art.º 2, da CRA)<sup>10</sup>, que buscou entre os modelos de jurisdição constitucional adoptar um modelo misto, i.e., concentrado e difuso (Bacelar Gouveia, 2014, Raúl Araújo, 2020).

Deste modo, como dissemos no rodapé número 9, a Lei de Revisão Constitucional n.º 23/92, de 16 de Setembro (art.º 134, 153, 154, 155 e 156) introduz a justiça constitucional, concomitantemente o Tribunal Constitucional como guardião da constituição para apreciação da estrutura inconstitucional das normas por acção e omissão declaradas<sup>11</sup>. De outro modo, embora o guardião fosse o TC, tal tribunal não estava instituído no instante, e suas funções, de acordo com o artigo 6.º da Lei de Revisão Constitucional eram exercidas pelo Tribunal Supremo (Raúl Araújo, 2020:3)<sup>12</sup>.

Apesar de Machado, da Costa e Hilário (2017) e Alexandrino (2013) e outros abordarem com precisão, Bacelar Gouveia (2014:598), nos apresenta em sua

---

9 Para Bacelar Gouveia (2014:592), a defesa da constituição trata da fiscalização da constitucionalidade dos actos do poder público, por meio da adoção de mecanismos destinados a apreciar a conformidade desses actos com a Constituição, aplicando as devidas consequências no caso de virem a ser descobertas situações de conflito constitucional. Ademais, Naldemar Lorenço (2019:202) ajuda-nos a esclarecer que a primeira Constituição Angolana nasce com a independência de Angola, após a dominação colonial, com a designação de Lei Constitucional, nessa Constituição não existiam processos de fiscalização da constitucionalidade. Isto é, de 1975 a 1991 existiram variadas revisões constitucionais, mais nenhuma delas foi capaz de introduzir a fiscalização da constitucionalidade (sic). A revisão de 1992 cria o Tribunal Constitucional e consequentemente a fiscalização da constitucionalidade, as funções do Tribunal Constitucional passaram a ser desempenhadas pelo Tribunal Supremo, até a data de 2008, quando foi institucionalizado o Tribunal Constitucional.

10 Um Estado regido por normas e princípios, que desde 1992 busca proteger os Direitos dos homens. Para Norberto Bobbio (2004:9), sem tais “direitos do homem reconhecidos e protegidos, não há democracia; sem democracia, não existem as condições mínimas para a solução pacífica dos conflitos”.

11 Lei de Revisão Constitucional nº 23/92, de 16 de Setembro. Consultado em <https://www.tchiweka.org/biblioteca/b-01553> [15/05/2023].

12 Observando Raúl Araújo (2020), a Lei n.º 2/08, de 17 de Junho, Lei Orgânica do Tribunal Constitucional e a Lei n.º 3/08, de 17 de Junho, Lei do Processo Constitucional (*vide* [www.safiii.org/ao/legis/num\\_act/lodpc363.pdf](http://www.safiii.org/ao/legis/num_act/lodpc363.pdf)), ambas aprovadas pela Assembleia Nacional, percebe-se que o Tribunal Constitucional foi criado ou instituído em Angola, somente, em 2008.

obra os sistemas (ou mecanismos) do controlo da constitucionalidade de Angola mediante a Constituição de 2010 (vide art.º 228, 230, 232, da CRA), tais são:

1. Sistema jurisdicional, e não político, porque esta tarefa está cometida a órgãos de soberania que são tribunais;
2. Sistema difuso e concentrado, porque a intervenção de fiscalização é atribuída tanto aos tribunais em geral como especificamente ao Tribunal Constitucional, ainda que este tendo a última palavra;
3. Sistema preventivo e sucessivo, porque a fiscalização incide tanto no procedimento de elaboração de certos atos jurídico-públicos como fundamentalmente depois de os atos jurídico-públicos estarem concluídos;
4. Sistema de fiscalização da inconstitucionalidade por ação e por omissão, porque fiscaliza a inconstitucionalidade que se traduz na violação da Constituição tanto por ação como por omissão (Gouveia, 2014).

Assim, embora surge na Lei Orgânica de Processo nas vestes de “recurso ordinário de inconstitucionalidade, acrescenta-se-lhe o sistema de fiscalização concreta<sup>13</sup>, porque, trata-se de um mecanismo ou sistema de controlo muito utilizado na defesa dos Direitos Fundamentais (José Alexandrino, 2013:111).

#### *7.1.1.1. Chefe do Estado e Tribunal Constitucional: competências*

O compromisso de defesa da justiça constitucional assenta em todos os poderes, sem exceção do parlamento. O Chefe do Estado Angolano, desde a Lei Constitucional de 1975 (em face do conselho de revolução)<sup>14</sup> até a Constituição de 2010, suas competências ou poderes em relação aos outros poderes são observáveis. Porém, quanto as competências, a Constituição de 2010 atribui ao chefe de Estado, poderes de nomeação de magistrados judiciais<sup>15</sup>, isto é, nomeia quatro dos onze juízes membros do Tribunal Constitucional, incluindo o Juiz Presidente [art.º 119 e) e 181 n.º 3, da CRA].

---

13 Não há um artigo explícito na CRA, em face do controlo concreto-difuso, daí que para Jorge Miranda (*apud* Gouveia, 2014), “embora os tribunais garantam e assegurem a observância da Constituição (artigo 177.º, n.º 1), não parece ter-se contemplado uma fiscalização difusa, concreta e incidental.

14 Era um órgão do Estado presidido pelo Chefe de Estado Angolano, que exercia a função legislativa da Assembleia do Povo (este órgão que só veio a ser instituído em 1980). Pois, o Conselho da Revolução definia a política interna e externa, aprovava o orçamento, nomeava e exonerava os membros do governo sob indicação do MPLA (Adérito Correia e Bornito de Sousa, 1996:22).

15 Cf. Armando GUEDES e Maria CARAPÊTO (2019:38), o Chefe do Estado nomeia os juízes do Tribunal Supremo, sob proposta do Conselho Superior da Magistratura Judicial [art.º 119 f) e 181 n.º 2 e 3]; os juízes do Tribunal de Contas [art.º 119 g) e 182 n.º 2]; os juízes do Supremo Tribunal Militar [art.º 119 h) e 183 n.º 2]; três dos membros do Conselho Superior da Magistratura Judicial [art.º 119 t) e 184 n.º 2]; parte dos membros do Conselho Superior da Magistratura do Ministério Público [art.º 119 t) e 190 n.º 3 c)]; e, sob proposta deste último órgão, o Procurador-Geral da República, os adjuntos deste, os Vice-Procuradores Gerais da República e ainda os Procuradores Militares [art.º 119 i) e 189 n.º 4 e 6].

Em Angola, no exercício da função jurisdicional, quer o Tribunal Constitucional como os demais tribunais são independentes e imparciais, estando apenas sujeitos à Constituição e à lei (art.º 175, da CRA). Quanto aos poderes do Chefe do Estado, o Tribunal Constitucional ao reconhecer no acórdão de fiscalização preventiva da CRA<sup>16</sup>, que a independência dos tribunais é um princípio inseparável do Estado democrático [...], de modo a salvaguardá-los da ingerência e pressões dos demais poderes, não entendeu que o princípio da independência fosse violado pela atribuição de poderes de nomeação dos juizes ao Presidente da República, podendo o poder judicial diante do poder executivo ser dependente ou afetar o exercício independente das suas competências (Ventura *apud* Guedes e Carapêto, 2019:37-38).

Vejamos que tais actores elucidam a questão da possível dependência do Tribunal Constitucional ao Chefe do Estado, que junto daquela instituição promove o controlo de constitucionalidade preventiva e sucessiva dos actos normativos, tratados internacionais, assim como emissões inconstitucionais, nos termos previsto na constituição [art. 119.º al. c), da CRA].

Para além do Chefe de Estado, 1/10 dos deputados à Assembleia Nacional em efetividade de funções; Grupos Parlamentares, Procurador Geral da República, Provedor da Justiça e a Ordem dos Advogados também podem requerer declaração de inconstitucionalidade ao guardião da Constituição angolana (art.º 130 n.º 2, da CRA).

Embora a dedução supra inferida sobre a dependência seja falível, é certo que podemos questionar, se o exercício independente de competência do Tribunal Constitucional de “apreciar a constitucionalidade das leis, dos decretos presidenciais, das resoluções, dos tratados, das convenções e dos acordos internacionais ratificados e de quaisquer normas, nos termos previstos na alínea a) do n.º 2 do artigo 180.º da Constituição” (art.º 16, da lei n.º 2/08, de 17 de junho), concomitantemente, aquelas competências contenciosas e não contenciosas relativas as eleições, partidos e órgãos de poder político, conforme distinguidos por Jorge Miranda (2008:162-165)<sup>17</sup>, podem ser afectados sob interferência do Chefe do Estado ou não, em função da relação que ambos se predispõem no exercício de funções ou por conveniência da indicação.

De acordo com o acórdão nº 319/13 e a CRA de 2010 (art.º 162), o Parlamento não fiscaliza os actos do Chefe do Estado e demais membros do executivo<sup>18</sup>, a despeito do efeito desse acórdão, defendemos um controlo dos actos

---

16 *Vide* Acórdão do TC de Angola 111/2010 <https://jurisprudencia.tribunalconstitucional.ao/wp-content/uploads/2019/04/111.pdf>.

17 *Vide* sobre os actos contenciosos e não contenciosos art.º 16, da lei n.º 2/08, de 17 de junho (LOTIC).

18 *Vide* acórdão nº 319/13, que gerou debates contraditórios quanto a posição do Tribunal Constitucional.

normativos e demais actos do Estado com justeza pelo guardião da Constituição. Pois, é notável que, desde 2008, o Tribunal Constitucional desempenha as suas funções como guardião das normas e princípios constitucionais [...], mas a semelhança de muitos tribunais jurisdicionais africanos enfrenta vários problemas funcionais como:

1. Dificuldade de implementação das suas decisões;
2. E autonomia administrativa; financeira e patrimonial; que subsistem dificuldades na compreensão da natureza do Tribunal Constitucional, havendo quem entenda ser um tribunal político e sem características de um verdadeiro tribunal judicial, defendendo-se, mesmo, que os seus juízes não são magistrados judiciais (Raúl Araújo, 2020:3).

Tais situações debilitam o enquadramento da jurisdição constitucional. Por isso, defende-se que haja um tribunal, que não se envolva em disputas políticas ou desordene as regras democráticas e atue como órgão político (Urbano *apud* Raúl, *ibidem*:9).

Nos Estados Constitucionais, de acordo com Dalmo de Abreu Dallari:

Por diversos motivos, muitos juízes maioria deles, sem dúvida afirmam que são apolíticos, considerando que isso é indispensável para o reconhecimento de sua imparcialidade e independência [...], e é evidente que o juiz não deve ser ligado a qualquer organização de fins políticos, que busque a conquista e o uso dos órgãos do poder do Estado para a implantação de suas idéias ou a promoção de seus interesses (Dallari, 1931:85).

Pode-se inferir dessa menção que o Tribunal Constitucional Angolano deve, mediante os mecanismos de controlo da constitucionalidade, administrar a justiça com independência real, e conforme a CRA (art.º 179, nº 6) os Juízes em exercício de funções não devem se sujeitar a ligações político-partidária, mas devem fazer “das suas decisões uma ordem e não parecer ou sugestão” (Dallari, 1931:88).

### **7.1.2. Mecanismos de controlo da constitucionalidade**

Como observamos anteriormente, os mecanismos ou sistemas de controlo da constitucionalidade em Angola, que a Constituição de 2010, tanto como a Lei nº 2/8, de 17 de Junho (Lei Orgânica do Tribunal Constitucional) e a Lei nº 3/8, de 17 de junho (Lei do Processo do Tribunal Constitucional) proclamam, são as de forma preventiva, sucessiva abstrata (e concreta). Tais mecanismos de fiscalização visam prevenir conflitos e julgar a validade ou invalidade das normas e actos do Estado, funcionando de acordo com a legitimidade democrática indirecta<sup>19</sup>.

---

<sup>19</sup> Legitimidade dos tribunais constitucionais é, antes de tudo, a legitimidade da própria Constituição [...] como diz JORGE MIRANDA, o poder de invalidar actos com força de lei baseia-se exactamente no facto de os juízes constitucionais serem

### 7.1.2.1. *Controlo preventivo*

É um mecanismo de controlo da constitucionalidade das normas, que visa evitar situações de inconstitucionalidade ou violações dos Direitos Humanos (Jónatas Machados, Nogueira da Costa e Esteves Hilário, 2017). Todavia, na possibilidade de supor inconstitucionalidade, cuja fiscalização deve ser por legitimidade processual requerida pelo Chefe do Estado e 1/10 dos Deputados à Assembleia Nacional em efetividade de funções, num prazo de 20 dias a contar da data de recepção, ao Tribunal Constitucional (art.º 228, da CRA). Cujo tribunal tem 45 dias para se pronunciar acerca da inconstitucionalidade, mas por razões de urgência, tal prazo pode ser encurtado pelos requerentes legitimados (art.º 228, n.º 4 da CRA)<sup>20</sup>.

### 7.1.2.2. *Controlo abstrato sucessivo*

Tanto o controlo abstrato preventivo (*a priori*) como o controlo abstrato sucessivo (*a posteriori*) são mecanismos respeitantes a inconstitucionalidade por acção (Machado e Da Costa, 2011). Porém, trata-se de um modelo tipicamente concentrado pelo qual da máxima intervenção dada pelo Tribunal Constitucional contra os actos legislativos. É controlo sucessivo quando acontece depois da entrada em vigor das normas, é controlo abstrato quando é realizado independentemente da decisão de qualquer caso concreto (Lourenço, 2019:209). Para Jónatas Machado e Nogueira da Costa (2011:251-252) a legitimidade processiva activa para desencadear o controlo abstrato sucessivo é restrito<sup>21</sup>, não havendo qualquer ação popular de impugnação de normas com fundamento na respectiva inconstitucionalidade. Ora, ao contrário dos dois autores, concordamos com Alexandrino (2013) e Lourenço (2019), que defendem que os cidadãos ou particulares podem ter acesso indireto do controlo abstrato sucessivo, porque apresentando petições aos órgãos legitimados de soberania podem defender os Direitos Humanos ou a Constituição da República de Angola<sup>22</sup>.

### 7.1.2.3. *Controlo concreto*

Para Gomes Canotilho (1993:967) está associado ao modelo jurisdicional difuso e incidental, também é designado de acção judicial (ou modelo america-

---

escolhidos por órgãos democraticamente legitimados, órgãos representantes do povo, como se da mesma origem resultassem (Leandro Ferreira, 2009:282 291).

20 A intervenção do Tribunal Constitucional, na decisão que este órgão venha a tomar na base de critérios de constitucionalidade, oscila entre uma *decisão positiva* – aceitando a existência de normas inconstitucionais – e uma *decisão negativa* – não encontrando nas normas cuja apreciação foi requerida qualquer vício de inconstitucionalidade (Bacelar Gouveia, 2014:606).

21 Como já nos referimos sobre tais requentes, Vide artigo 230.º n.º 2, da CRA.

22 O Tribunal Constitucional funciona aqui como um verdadeiro legislador negativo, projetando o resultado da sua decisão tanto no presente, como no passado e no futuro (José Alexandrino, 2013:111).

no), e pressupõe que todo tribunal, que tem de decidir um caso concreto, está obrigado, por causa da ligação com a constituição, a fiscalizar se as normas jurídicas aplicáveis ao caso são ou não válidas. Como já anteriormente referimos, apesar do fundamento do artigo 177.º, da CRA, Jorge Miranda (*apud* Gouveia, 2014) alega que a Constituição Angolana não é explícita ao contemplar este modelo difuso, facto que levou Marcy Lopes a discordá-lo, alegando que:

Quando o Tribunal Constitucional aprecia em recurso a constitucionalidade das decisões dos demais tribunais que recusem a aplicação ou apliquem normas cuja constitucionalidade tenha sido suscitada durante o processo, ao abrigo das alíneas d) e e), do nº 2 do art.º 180 da CRA, este tribunal não o faz no âmbito da fiscalização concentrada [...], mas, sim, em sede da fiscalização concreta e incidental em instância de recurso. Deste modo, o sistema [...] é misto (Lopes, 2016:152).

Quer dizer, trata-se de um sistema solto, solicitado por particulares, cujo controlo de constitucionalidade é feito por qualquer juiz ou tribunal, diferente do modelo concentrado feito apenas por um órgão, o Tribunal Constitucional. Bacelar Gouveia (2014:613) ajuda-nos a esclarecer que as regras processuais aplicáveis aos recursos estão definidas na Lei n.º 3/08 de 17 de Junho (LOPC).

#### *7.1.2.4. Inconstitucionalidade por omissão*

Refente a inconstitucionalidade por omissão, a Constituição de 2010, proclama no art.º 332.º. E, como supra referido, é representado quando o legislador, tendo o dever jurídico de atuar, abstenha-se inteiramente de fazê-lo, deixando um vazio normativo na matéria (Luís Barroso, 2012). Deste modo, pode ser desencadeado pelo Presidente da República, 1/5 dos Deputados em efetividade de funções e o Procurador Geral da República em qualquer instante (art. 32º da LOPC). Porém, cabe ao Tribunal Constitucional dar conta da omissão legislativa à Assembleia Nacional, indicando aos órgãos um prazo razoável para a supressão da lacuna ou inação (Artigo 35.º da LOPC).

#### *7.2. IMPLICAÇÕES SOBRE O GUARDIÃO DA CONSTITUIÇÃO*

Em Angola, desde 1992, a Constituição proclama que o guardião para garantia da Constituição é o Tribunal Constitucional, sendo o Chefe do Estado um órgão que não tem legitimidade e legalidade para interferir nas decisões do Tribunal Constitucional independente e imparcial, mas tem competências para requerer ao guardião da Constituição o controlo preventivo e sucessivo da constitucionalidade, não obstante a nomeação dos juizes lhe conferir vantagens, o que não significa subordinação. Verifica-se que a perspectiva de Carl Schmitt prevalece na realidade judiciária angolana (e muitas outras realidades), se entendermos que a nomeação dos juizes ou a Estrutura Organizatória do Tribunal Constitucional pode influenciar a interferência do Chefe do Estado, que indica juizes por mérito

de conveniência e susceptíveis de não comprometerem a atuação dos seus actos, em caso de incumprimento da lei e das leis.

## 8. CONCLUSÃO

Numa Abordagem sempre incompleta, buscamos através de métodos e objectivos definidos analisar a interferência do Chefe do Estado Angolano no Tribunal Constitucional durante controlo da constitucionalidade e, tendo em conta a observação teórica e conceptual dos factos, da constituição e as leis, desenvolvemos em dois capítulos o problema, fazendo um exercício desafiador para o enriquecimento do enquadramento da justiça constitucional em Angola. Porém, o problema levantado não mereceu uma resposta deveras objectiva, porque a Constituição não proclama o que pode vir acontecer na prática quanto a interferência do Chefe do Estado Angolano.

Assim, concluímos que o entendimento do constitucionalismo não precede a noção de justiça constitucional ou controlo da constitucionalidade, tal justiça que nos dias contemporâneos tornou-se premissa da democracia, tal controlo que ligado a supremacia da constituição permite-a verificar a adequação dos actos jurídicos. Deste modo, sustenta-se de dois modelos difuso e concentrado, que na esfera das discussões de Carl Schmitt e Hans Kelsen, expandiram-se em vários Estados tal como em Angola. Destarte, em Angola o constitucionalismo originou propriamente com a Lei Constitucional de 11 de Novembro de 1975, e somente com a Lei nº 23/92, de 16 de Setembro introduziu-se a justiça constitucional, tendo, até a Constituição de 2010, o Tribunal Constitucional como o Guardião da Constituição. Ademais, observou-se as competências de nomeação dos magistrados judiciais, e constatou-se que os tribunais são órgãos independentes, e que o Tribunal Constitucional ao reconhecer no acórdão de fiscalização preventiva da Constituição, que a independência é um princípio inseparável do Estado de Direito Democrático, de modo a salvaguardá-lo das interferências e pressões dos demais poderes, não percebeu que tal princípio fosse violado pela atribuição ou nomeação dos Juizes ao Chefe do Estado, podendo aqueles serem dependentes deste, e este afetar o exercício independente do controlo da constitucionalidade, concomitantemente da Administração da Justiça. De outro modo, muitas coisas não foram profundamente esclarecidas, mas o certo é que em nenhuma parte da Constituição constata-se que o Chefe do Estado deve interferir no Tribunal Constitucional, pelo contrário, entende-se no texto constitucional, que os Juizes em exercício de funções não devem se sujeitar a ligações político-partidária, mas devem fazer das suas decisões uma ordem e não parecer ou sugestão a outros órgãos do Estado.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDRINO, Melo José. O novo constitucionalismo angolano. Lisboa: Instituto de Ciências Jurídico-Políticas, 2013.



- CANOTILHO, Gomes. Direito Constitucional (6ª ed.). Coimbra: Almedina, 2003a.
- \_\_\_\_\_. Direito constitucional e teoria constitucional (7ª ed.). Coimbra: Almedina, 2003b.
- \_\_\_\_\_. Direito constitucional e teoria constitucional (7ª ed.). Coimbra: Almedina, 1993.
- BARROSO, Luís Roberto. O controlo de constitucionalidade no direito brasileiro (6ª ed.). São Paulo: Saraiva, 2012.
- CORREIA, Adérito, DE SOUSA, Bornito. Angola história constitucional. Coimbra: Almedina Almeida, 1996.
- GOUVEIA, Jorge Bacelar. Direito constitucional de Angola. Lisboa: IDILP, 2014.
- LASSALE, Ferdinand. O que é uma constituição. Lisboa: Escola Editora, 2013.
- LOPES, Marcy. A sindicância constitucional dos actos políticos: admissibilidade constitucional e a sua concretização no sistema de fiscalização em Angola. Luanda: Almedina, 2016.
- MACHADO, Jónatas E. M., COSTA, Paulo Nogueira da. Direito constitucional angolano. Coimbra Editora: Lisboa, 2011.
- MACHADO, Jónatas E. M., COSTA, Paulo N. da., HILÁRIO C. Esteves. Direito constitucional angolano (4ª ed.). Luanda: Petrony, 2016.
- MIRANDA, Jorge. Manual de direito constitucional tomo VI: inconstitucionalidade e garantia da constituição (3ª ed.). Lisboa: Coimbra editora, 2008.
- MORAIS, Carlos Blanco de. Justiça constitucional tomo I: garantia da constituição e controlo da constitucionalidade (2ª ed.). Lisboa: Coimbra Editora, 2006.
- TAVARES, André Ramos. Curso de direito constitucional (10ª ed.). São Paulo: Saraiva, 2012.

### **Livros acesso online**

- ARISTOTÉLES. Política, 1988. recuperado de [https://repositorio.ufpe.br/bitstream/123456789/4861/1/arquivo7225\\_1.pdf](https://repositorio.ufpe.br/bitstream/123456789/4861/1/arquivo7225_1.pdf) [10/05/2023].
- CASTANHEIRA, Paulo. Manual de Direito Constitucional. Recuperado de [file:///C:/Users/h/Downloads/Paulo\\_Mascarenhas\\_MANUAL\\_DE\\_DIREITO\\_CONS.pdf](file:///C:/Users/h/Downloads/Paulo_Mascarenhas_MANUAL_DE_DIREITO_CONS.pdf) [06/04/2023].
- AMARAL, Maria Lúcia. Revisitar Carl Schmitt: a defesa da Constituição, 2014. Carlos Blanco de Moraes e Luís Pereira Coutinho (org). Carl Schmitt revisitado (133-150). Recuperado de [https://www.icjp.pt/sites/default/files/publicacoes/files/icjp\\_ebook\\_carlschmittrevisitado.pdf](https://www.icjp.pt/sites/default/files/publicacoes/files/icjp_ebook_carlschmittrevisitado.pdf) [10/05/2023].
- BOBBIO, Norberto. A era dos direitos, 2004. Recuperado de [https://edisciplinas.usp.br/pluginfile.php/297730/mod\\_resource/content/0/norberto-bobbio-a-era-dos-direitos.pdf](https://edisciplinas.usp.br/pluginfile.php/297730/mod_resource/content/0/norberto-bobbio-a-era-dos-direitos.pdf) [10/04/2022].
- DALLARI, Dalmo de Abreu. O poder dos juízes, 1931. Recuperado de [https://edisciplinas.usp.br/pluginfile.php/4305162/mod\\_resource/content/0/DALLARI%2C%20Dalmo.%20O%20Poder%20dos%20Ju%2C%20ADzes.%20Cap.%20X%20%28p%20C3%A1ginas%2085%20a%2094%29.pdf](https://edisciplinas.usp.br/pluginfile.php/4305162/mod_resource/content/0/DALLARI%2C%20Dalmo.%20O%20Poder%20dos%20Ju%2C%20ADzes.%20Cap.%20X%20%28p%20C3%A1ginas%2085%20a%2094%29.pdf) [17/05/2023].
- GUEDES, Armando Marques, CARAPÊTO Maria João. Dos poderes do Chefe de Estado no direito comparado, 2019. Recuperado de [file:///C:/Users/h/Downloads/Os\\_poderes\\_dos\\_chefes\\_de\\_estado\\_no\\_direi.pdf](file:///C:/Users/h/Downloads/Os_poderes_dos_chefes_de_estado_no_direi.pdf) [20/09/2019].
- FILHO, Gonçalves Ferreira Manoel. Curso de direito constitucional, 2012. Retirado de [file:///C:/Users/h/Downloads/Curso\\_de\\_Direito\\_Constitucional\\_Manoel\\_G.pdf](file:///C:/Users/h/Downloads/Curso_de_Direito_Constitucional_Manoel_G.pdf) [10/02/2023]
- HOBBS, Thomas, 2003. Recuperado de <https://marcosfabionuva.files.wordpress.com/2011/08/leviatc3a3.pdf> [20/07/2018].
- LOOK, John. Segundo tratado sobre o governo civil, 2021. Recuperado de [file:///C:/Users/h/Downloads/CLUBE\\_DO\\_LIVRO\\_LIBERAL\\_SEGUNDO\\_TRATADO\\_S.pdf](file:///C:/Users/h/Downloads/CLUBE_DO_LIVRO_LIBERAL_SEGUNDO_TRATADO_S.pdf) [03/07/2018].
- KELSEN, Hans. Jurisdição Constitucional Recuperado de [https://edisciplinas.usp.br/pluginfile.php/5392772/mod\\_resource/content/1/KELSEN.pdf](https://edisciplinas.usp.br/pluginfile.php/5392772/mod_resource/content/1/KELSEN.pdf) [20/03/2023].
- ROUSSEAU, Jean-Jacques. Do contrato social, 2003. Recuperado de <https://www.ebooksbrasil.org/adobe-book/contratosocial.pdf> [02/07/2018].

## Artigo acesso online

BAHIA, Alexandre. Controlo concentrado de constitucionalidade: o guardião da constituição no embate entre Hans Kelsen e Carl Schmitt, 2004. Revista Brasília 1(18) 87-103. Recuperado de <https://www2.senado.leg.br/bdsf/bitstream/handle/id/1009/R164-06.pdf?sequence=4&isAllowed=y> [12/04/2023].

BONAVIDES, Paulo. Jurisdição constitucional e legitimidade: algumas observações sobre o Brasil, 2004. Retirado de <https://www.scielo.br/j/ea/a/fjv37CkWwWvGcKpDfM6cwwmp/?format=pdf&lang=pt> [02/05/2023].

Fabiano Ferreira. O guardião da constituição: debate entre Carl Schmitt e Hans Kelsen, 2010. A&C Revista de Direito Administrativo & Constitucional 1(23) 121-146. Recuperado de <file:///C:/Users/h/Downloads/291-321-1-PB.pdf> [12/05/2023].

FERREIRA, Leandro E. da Gama. A legitimidade da justiça constitucional, 2009. Recuperado de <file:///C:/Users/h/Downloads/9149-Artigo-15290-1-10-20200629.pdf> [03/03/2023].

FILHO, Nagib Slaib. Breve história do controlo de constitucionalidade, 2002. Revista da EMERJ 1(36) 280-239. Recuperado de [http://www.abdpc.org.br/abdpc/artigos/Nagib%20Slaibi%20Filho%20\(5\)%20-formatado.pdf](http://www.abdpc.org.br/abdpc/artigos/Nagib%20Slaibi%20Filho%20(5)%20-formatado.pdf) [03/3/2032].

LORENÇO, Naldemar Miguel. Breve comentário sobre a fiscalização da constitucionalidade em Angola, 2019. Revista Jurídica digital data vénia 1(20) 201-219. Recuperado de [https://www.datavenia.pt/ficheiros/edicao10/datavenia10\\_p201\\_218.pdf](https://www.datavenia.pt/ficheiros/edicao10/datavenia10_p201_218.pdf) [02/3/2023].

MIRANDA, Jorge. Direito de acesso à justiça constitucional, 2011. Recuperado de [file:///C:/Users/h/Downloads/Acesso\\_a\\_justica\\_constitucional.pdf](file:///C:/Users/h/Downloads/Acesso_a_justica_constitucional.pdf) [07/03/2023].

MORAIS, de Alexandre. Direito Constitucional (13ª ed.), 2003. Retirado de [https://jornalistaslivres.org/wp-content/uploads/2017/02/DIREITO\\_CONSTITUCIONAL-1.pdf](https://jornalistaslivres.org/wp-content/uploads/2017/02/DIREITO_CONSTITUCIONAL-1.pdf) [07/05/2023].

KELSEN, Hans. A garantia da jurisdição constitucional: a justiça constitucional, 2003. Recuperado de <file:///C:/Users/h/Downloads/1401-Texto%20do%20Artigo-4093-4594-10-20130716.pdf> [01/02/2023].

Dissertação, Tese e Manuais Didáticos

AGRA, Walber de Moura. Jurisdição constitucional: diretrizes para o incremento da sua legitimidade (Tese de Doutoramento), 2003. Recife Firense. Recuperado de [https://repositorio.ufpe.br/bitstream/123456789/48611/arquivo7225\\_1.pdf](https://repositorio.ufpe.br/bitstream/123456789/48611/arquivo7225_1.pdf) [10/05/2023].

ARAÚJO, Raúl. A tutela constitucional dos direitos fundamentais em Angola: uma análise crítica do modelo existente e a prática do tribunal constitucional, 2020.

HIROSE, Regina Tamami. Actos normativos e controlo concentrado de constitucionalidade (Dissertação de Mestrado). Pontifícia Universidade Católica de São Paulo – PUC/SP, Brasil, 2010. Recuperado de <https://tede2.pucsp.br/bitstream/handle/9048/1/Regina%20Tamami%20Hirose.pdf> [10/05/2023].

## Documentos Jurídicos e Leis

Lei de Revisão Constitucional nº 23/92, de 16 de Setembro. Consultado em <https://www.tchiweka.org/biblioteca/b-01553> [15/05/2023].

Constituição da República de Angola: promulgada em 23 de Fevereiro de 2010. Luanda: Imprensa Nacional.

Lei nº 2/8, de 17 de Junho, Lei Orgânica do Tribunal Constitucional. <https://gazettes.africa/archive/ao/2008/ao-government-gazette-dated-2008-06-17-no-110.pdf>.

Lei nº 3/8, de 17 de junho. Lei do Processo do Tribunal Constitucional. [www.safiii.org/ao/legis/num\\_act/lodpc363.pdf](http://www.safiii.org/ao/legis/num_act/lodpc363.pdf).

Acórdão nº 319/11, de 23 de Outubro de 2013, do Tribunal Constitucional de Angola. <https://jurisprudencia.tribunalconstitucional.ao/wp-content/uploads/2019/04/319.pdf>.

Acórdão nº 111/2010, de 30 de janeiro de 2010 <https://jurisprudencia.tribunalconstitucional.ao/wp-content/uploads/2019/04/111.pdf>.

# DEMOCRACIA EM TEMPOS DE INTELIGÊNCIA ARTIFICIAL. DESAFIOS E OPORTUNIDADES

GUILHERME MORAES CARDOSO<sup>1</sup>

## 1. INTRODUÇÃO

O cruzamento entre a inteligência artificial (IA) e os princípios democráticos que fundamentam o modelo brasileiro constitui um campo de estudo de crescente importância e complexidade. À medida que as tecnologias de IA continuam a evoluir e a moldar diversos aspectos da vida contemporânea, surgem inúmeros desafios e oportunidades que afetam diretamente a própria essência da democracia e por que não dizer, sua existência.

É fundamental explorar profundamente as implicações dessa convergência, compreendendo tanto os riscos inerentes quanto aos potenciais contribuições para a consolidação de sistemas democráticos robustos e inclusivos.

Este artigo empreende uma análise crítica e abrangente do cenário atual. Inicialmente, cumpre-se o propósito de definir de maneira precisa o que representa a inteligência artificial, considerando suas dimensões técnicas e conceituais. Em seguida, abordam-se os desafios relacionados ao uso da IA destacando-se questões relativas à autonomia de decisões, responsabilidade e ética, elementos necessários para se compreender as implicações da IA no contexto democrático.

Ainda nesta pesquisa se encontra presente uma reflexão sobre a relação entre a democracia e os sistemas de IA, especialmente diante de um mundo onde a crescente automatização de processos decisórios e a influência dessas tecnologias se tornam cada vez mais constantes. A proposta principal é justamente analisar, ainda que brevemente, como a IA impacta diretamente a qualidade e a legitimidade dos Estados democráticos.

Nesse sentido, um dos principais focos desta pesquisa reside na discussão dos desafios contemporâneos associados à influência da IA na democracia, com destaque especial para o fenômeno das fake news. As notícias falsas, potencial-

---

<sup>1</sup> Doutorando do Programa de Pós-graduação em Direito da Universidade de Marília – PPGD/UNIMAR, bolsista CAPES. Mestre em Teoria do Direito e do Estado pelo UNIVEM Marília. Professor Universitario na Faculdade de Ensino Superior e Formação Integral – FAEF (Garça/SP), advogado.

mente amplificadas pela automação e pela capacidade de personalização da IA, emergem como um dos problemas mais urgentes e complexos a serem enfrentados, ameaçando a integridade do processo democrático.

Este artigo estudo baseou-se em uma metodologia de pesquisa rigorosa, que envolveu revisão bibliográfica, análise de estudos de caso e pesquisa empírica, buscando não apenas compreender a extensão dos desafios apresentados pela IA à democracia, mas também identificar possíveis soluções e políticas que aptas a orientar a continuidade do desenvolvimento futuro dessas tecnologias, em consonância com os princípios democráticos. O trabalho se divide em duas partes sendo a primeira utilizada para amparar o leitor de quesitos técnicos relacionados a IA e a segunda parte disposta para o enfrentamento da interferência desta tecnologia na manutenção da democracia, dando ênfase a proliferação de *fake news*.

Espera-se não apenas contribuir para o debate acadêmico, mas também fornecer orientações práticas todos aqueles interessados na modernização, no futuro e dentro desse contexto a adaptação às mudanças que a era da IA impõe à compreensão e prática da democracia.

## **2. A INTELIGÊNCIA ARTIFICIAL. BREVE CONCEITUAÇÃO**

A inteligência artificial, doravante sendo utilizada neste artigo a sigla (IA) está desempenhando um papel cada vez mais significativo na vida humana, impulsionando a inovação tecnológica e oferecendo cada vez mais oportunidades em diversas áreas. Contudo, o uso de recurso, ferramenta (se é que existe uma terminologia correta e única para referenciar a IA) também apresenta desafios e riscos levando a sociedade, de modo geral, a questionar e refletir sobre uma regulamentação que garanta utilização ética e responsável.

De início, indispensável compreender a questão terminológica a respeito da utilização da expressão inteligência artificial posto que, para alguns especialistas no assunto não seria correto falar em inteligência, já que estaria diretamente ligada ao ser humano. Não existe razoabilidade em pensar numa espécie de inteligência artificial, mas sim conhecimentos desenvolvidos artificialmente mediante enriquecimento por informações disponibilizadas pelo ser humano.

Ao ser humano foi atribuída a possibilidade de pensar, de raciocinar e consequentemente desenvolver sua inteligência. Logo, se inteligência é fruto do “pensar”, para se falar em inteligência artificial é importante discutir se uma máquina pode criar um modelo artificial que simule a mente humana.

A mente humana compreende inúmeras formas de pensar, de compreender, de propor ações, que a depender de onde esteja o indivíduo, seu conhecimento, sua vivência, experiências, será de uma forma e noutros casos, sendo

diferente as circunstâncias acima, outra, totalmente diferente. Levando isso em consideração, compreende-se a dificultosa tarefa atribuída a máquina de penetrar a mente humana (se é que existe essa possibilidade).

O estudo da IA e sua utilização não é algo do momento. Os primeiros trabalhos sobre o tema datam o ano de 1943. Cumpre ao momento trazer a lume uma definição do que vem a ser inteligência artificial (se é que existe tal possibilidade).

Existem diversas ferramentas fazendo uso da inteligência artificial. Pontos positivos e negativos se evidenciam do uso dessas ferramentas, em especial quando se vislumbra a possibilidade de utilizá-la para lago ruim ou que coloque a natureza humana em risco.

Vale dizer que essa possivelmente é uma das maiores preocupações em relação ao uso da inteligência artificial e sua aplicação no cotidiano das pessoas. Alguns, inclusive, demonstram enorme preocupação com a possibilidade de uma suposta substituição do homem pelas ferramentas apoiadas na inteligência artificial.

Logo, cabe refletir a respeito da necessidade ou não de regulação do uso da IA. Como se sabe, nem sempre a regulamentação é suficiente para se evitar problemas, prejuízos, ou como no caso da inteligência artificial, utilizá-la de forma correta; melhor dizendo, de forma ética. Fosse assim, a sociedade não enfrentaria problemas em relação a práticas tipificadas como crime, pois a simples existência da regulamentação impondo uma pena em face de ocorrência da prática da conduta já seria evitada pelo agente.

## 2.1. O QUE É INTELIGÊNCIA ARTIFICIAL

Urge responder: o que é a inteligência artificial? Em breves palavras poderíamos conceituar a IA como a possibilidade de máquinas adquirirem capacidade de imitar ou replicar certos aspectos da natureza humana fazendo uso de algoritmos, sistemas computacionais que executem tarefas normalmente realizadas pela inteligência humana. Conforme justificou-se acima: capacidade de processar, aprender, perceber, compreender a linguagem natural e tomar decisões.

Na obra “*Atlas of AI*” de *Katy Crawford*<sup>2</sup>, um dos principais rótulos sobre a inteligência artificial, a autora discorrendo sobre a IA, explica que:

[...] Argumento que a IA não é nem artificial nem inteligente. Em vez disso, a inteligência artificial é incorporada e material, feita de recursos naturais, combustível, trabalho humano, infraestrutura, logística, histórias e classificações. Os sistemas de IA não são autônomos, racio-

---

2 CRAWFORD, Kate. *Atlas of AI*. [S. l.]: Yale University Press, 2021. p.8

nais ou capazes de discernir qualquer coisa sem treinamento extensivo e computacionalmente intensivo com grandes conjuntos de dados ou regras e recompensas predefinidas. Na verdade, a inteligência artificial como a conhecemos depende inteiramente de um conjunto muito mais amplo de estruturas políticas e sociais. E devido ao capital necessário para construir a IA em escala e as formas de ver que ela otimiza os sistemas de IA, eles são projetados para atender aos interesses dominantes existentes. Nesse sentido, a inteligência artificial é um registro de poder.<sup>3</sup>

Os principais subcampos vinculados à inteligência artificial são: a) *machine learning* (aprendizado da máquina); b) redes neurais (acrescenta-se a *deep learning*); c) processamento de linguagem na sua forma natural; d) *computer vision* (visão computacional); e) robótica e f) automação. Na sequência será exposto um pouco mais a respeito de cada um destes subcampos.

O *machine learning*, como a simples leitura do termo permite presumir, é uma forma de desenvolvimento de algoritmos e técnicas que permitam às máquinas aprender a partir de dados sem serem explicitamente programadas; basicamente a máquina se utiliza de um conjunto de dados e identifica padrões, faz previsões e toma decisões com base nesses padrões que foram criados.

Ponto interessante desse subcampo da IA é que a máquina recebe uma programação que a faça aprender a partir de exemplos e experiências; ou seja, ao invés de programar a máquina para que ela execute uma tarefa pré-determinada, a programação será justamente para que ela mesma busque seu aperfeiçoamento, seu próprio aprendizado. Semelhante àquilo que se faz no aprendizado humano. Nos bancos escolares é repassado pelos professores o necessário para o indivíduo se desenvolver cabendo tudo o mais a própria pessoa. Seguindo pela analogia, é o homem na condição de professor da máquina, sua aluna.

O aprendizado da máquina passa por algumas etapas como coleta de dados (e aqui reside uma preocupação especial se utilizados dados pessoais), processamento dos dados coletados (uma espécie de filtragem do que foi coletado selecionando o que é útil e descartando o inútil), a definição do algoritmo (lembrando que existem diversos modelos) e o treinamento do modelo escolhido fazendo uso inicialmente dos dados coletados e filtrados. Após esse processo é avaliada a eficiência desse modelo e se o desempenho alcançado corresponde as expectativas, para então ser implantado.

O processo apresentado acima não é um modelo padrão, até porque o aprendizado da máquina não é algo estático, finito. Pelo contrário, uma vez que os modelos podem ser atualizados e refinados à medida que novos dados se tor-

---

3 *I argue that AI is neither artificial nor intelligent. Rather, artificial intelligence is both embodied and material, made from natural resources, fuel, human labor, infrastructures, logistics, histories, and classifications. AI systems are not autonomous, rational, or able to discern anything without extensive, computationally intensive training with large datasets or predefined rules and rewards. In fact, artificial intelligence as we know it depends entirely on a much wider set of political and social structures. And due to the capital required to build AI at scale and the ways of seeing that it optimizes AI systems are ultimately designed to serve existing dominant interests. In this sense, artificial intelligence is a registry of power.*

nam disponíveis, permitindo aperfeiçoamento contínuo do desempenho e precisão.

As redes neurais artificiais (*artificiais neurais networks*) assemelham-se ao funcionamento do cérebro humano; neurônios artificiais interconectados processam e transmitem informações. Esse modelo de IA costuma ser muito utilizado para tarefas de reconhecimento de padrões e processamento de linguagem natural, outro subcampo a ser explorado na sequência.

Essas redes neurais, também chamada de *deep learning*, permitem o processamento de dados de forma hierárquica e a extração de representações complexas; ao contrário de algoritmos de aprendizado de máquina tradicionais, que requerem recursos humanos para extrair manualmente as características relevantes dos dados. O modelo *deep learning* é capaz de aprender automaticamente as características dos dados através de camadas de processamento.

Quando se fala em processamento de linguagem natural está se falando no desenvolvimento da máquina a ponto de entender e interpretar a linguagem humana em sua forma natural. Envolve, nesta seara, o reconhecimento de fala, geração de texto e até mesmo análise de sentimentos.

A visão computacional (*computer vision*) permite que a máquina entenda e consiga interpretar conteúdo de ordem visual, a exemplo de imagens e vídeos. Em sua análise a máquina reconhece objetos, detecta faces, analisa expressões e até mesmo a movimentação. Esse modelo de IA encontra-se sendo utilizado por veículos autônomos e sistemas de segurança onde se faz o reconhecimento da face para identificação de pessoa procurada.

Por fim, seguindo delimitação proposta para este artigo, a robótica e os processos de automação se registram como subcampos da IA. Esses modelos são treinados para executar tarefas complexas com autonomia processando informações do ambiente, tomando suas próprias decisões e interagindo com o mundo físico. Em se tratando de robótica, oportuno apresentar 3 leis desenvolvidas por Isaac Izamov em seu clássico “Eu, o robô<sup>4</sup>”:

1ª Lei: Um robô não pode ferir um ser humano ou, por inação, permitir que um ser humano sofra algum mal.

2ª Lei: Um robô deve obedecer às ordens que lhe sejam dadas por seres humanos exceto nos casos em que tais ordens entrem em conflito com a Primeira Lei.

3ª Lei: Um robô deve proteger sua própria existência desde que tal proteção não entre em conflito com a Primeira ou Segunda Leis.

---

4 AZIMOV, Isaac. **Eu, Robô**. [S. l.]: Aleph, 2014. p. 5.

Em todas as leis os interesses do homem são colocados à frente de qualquer outro interesse, inclusive o da própria máquina, do robô. Referidas leis apontam para um caminho ético no uso da robótica; também o será em relação a IA? Nos processos de desenvolvimento das máquinas de IA, será possível traçar limiares éticos a ponto de a mesma reconhecer sua fragilidade e hipossuficiência em face do homem ou alcançará tamanha autonomia que num determinado momento compreenderá que pode ser melhor ou até mesmo substituir os seus criados?

## 2.2. DESAFIOS NO USO DA INTELIGÊNCIA ARTIFICIAL

O uso da IA sem uma adequada regulamentação apresenta diversos desafios e riscos para a coletividade, como por exemplo na privacidade e segurança de dados. Este, um dos assuntos mais emergentes nos últimos tempos (em especial nos países da União Europeia graças ao advento da *General Data Protection Regulation*<sup>5</sup> – GDPR e no Brasil, face a Lei Geral de Proteção de Dados – LGPD) posto que antes as ameaças à privacidade não eram tão grandes como atualmente.

Oportuno, talvez, pensar na hipótese de regulação da IA para que seja evitada a violação da privacidade, já que diariamente se processa um imenso volume de dados por todo o globo terrestre; e o que deixa essa afirmação ainda mais preocupante é que na maioria dos casos esse processo de dados está interligado com outros inúmeros tratamentos, uma espécie de rede.

Até porque muitos buscam por informação, muitos querem de tudo e de todos saber. E por trás de tudo isso o lucro, o crescimento alcançado pela exploração de dados alheios. É o que nos apresenta Frank A. Pasquale em sua obra “*The Black Box Society: The Secret Algorithms that Control Money and Information*”<sup>6</sup>:

A publicidade intensiva em dados ajuda a gerar mais de US\$ 150 bilhões por ano em atividade econômica. Os defensores afirmam que isso nos proporciona um ambiente digital cada vez mais personalizado e amigável ao usuário. Mas as empresas de publicidade, e as pessoas que as pagam, não estão no negócio para cuidar da nossa saúde. Eles procuram lucro. Quando clicamos em um anúncio prometendo um desconto, provavelmente há um programa nos bastidores calculando o quanto mais eles podem nos cobrar com base em nossa localização, ou se estamos usando um Mac ou PC, ou até mesmo registros judiciais. Não é apenas a Agência de Segurança Nacional (NSA) que cobiça o conhecimento total das informações; esse também é o objetivo dos profissionais de marketing. Eles desejam essa infinidade de pontos de dados para desenvolver perfis exaustivos. Sobre nós.<sup>7</sup>

---

5 <https://gdpr-info.eu/>

6 PASQUALE, Frank. **Black box society: the secret algorithms that control money and information**. [S. l.]: Harvard University Press, 2015. p. 20.

7 *Data-intensive advertising helps generate over \$150 billion a year in economic activity. Boosters claim that it gives us an ever more personalized, user-friendly Internet. But advertising companies, and the people who pay them, aren't in business for their health. They're looking for profit. When we click on an ad promising a discount, there's probably a program behind the scenes calculating how much more it can charge us on the basis of our location, or whether we're using a Mac or PC, or even court records. It's not only the National Security Agency (NSA) that covets total information awareness; that's the goal of marketers, too. They want that endless array of data points to develop exhaustive profiles. Of us.*



Tem também a presença dos algoritmos de IA maliciosos ou mesmo aqueles sistemas vulneráveis se tornando alvo fácil de ataques cibernéticos, violação de segurança e roubo de informações confidenciais.

Existe também uma preocupação com o desenvolvimento de máquinas que no exercício de sua atuação acaba oferecendo decisões injustas e até mesmo discriminatórias vindo a prejudicar rotinas como as de oferta de crédito, de acesso a serviços e de justiça criminal.

Muitos sistemas de IA, podem acabar se tornando verdadeiras caixas-pretas, tendo seu funcionamento interno não facilmente compreendido. Questões como esta levantam preocupações sobre a transparência e a capacidade de explicar as decisões tomadas por referidos sistemas.

Os padrões discriminatórios criados pela própria máquina em seu processo de desenvolvimento podem trazer reflexos prejudiciais e ao mesmo tempo perigosos para a sociedade. É o caso, por exemplo, das *deep fakes* usadas para manipulação de informação, convencimento e desinformação, as famosas *fake news*.

Esses são apenas alguns dos desafios e riscos associados ao uso da IA e sua necessidade ou não de regulamentação. A implementação de regulamentações eficazes pode ser fundamental para mitigar esses riscos, garantir o uso ético e responsável da IA e promover a confiança e a transparência em seu desenvolvimento e utilização.

### 2.3. AUTONOMIA DE DECISÕES

Antes de avançar na leitura é importante compreender que o escopo principal desse trabalho é discutir a autonomia que as máquinas de IA adquirem em seu processo de desenvolvimento e possíveis riscos que isso venha causar no futuro. Ou seja, corre-se riscos com máquinas de IA desenvolvidas para tomar decisões de forma autônoma?

Vale advertir que a autonomia não é necessariamente uma forma de identificação da IA, tanto pela própria nomenclatura ou pela extensão do comportamento adotado pela máquina. Por esta linha, diversamente do uso do termo autonomia, *Ryan Calo*<sup>8</sup>, sugere por mais adequado tratar por comportamento emergente a capacidade do robô aprender e de se adaptar às circunstâncias.

Provavelmente para que a máquina não traga problemas face a sua autonomia, necessário treiná-la com princípios e ou valores éticos. Isso é claro, partindo do pressuposto que o homem realiza a programação para que a máquina

---

8 CALO, Ryan. Robotics and the new cyberlaw. *SSRN Electronic Journal*, 2014. p. 515.

se desenvolva e aprenda sozinha fazendo uso dos dados por ela mesmo coletados. Neste caso, então, a máquina precisaria aprender a ética, a proceder de forma ética, a propor soluções amparadas pela ética. Eis o grande desafio.

A segurança também acaba sendo uma preocupação para o uso ético dos sistemas de inteligência artificial, especialmente pelo fato de que algoritmos e códigos estão sujeitos as mais diversas ameaças cibernéticas como a manipulação maliciosa e o *hacking*. É essencial que os sistemas de IA sejam projetados com medidas de segurança robustas, criptografia adequada e proteção contra vulnerabilidades para evitar violação de segurança e garantir a integridade dos dados.

Outro ponto muito importante em relação a ética decorre dos vieses cognitivos. E o que vem a ser isso? Para melhor compreensão necessário antes de tudo, compreender o que são algoritmos.

É evidente que para fins deste estudo não se faz necessário esmiuçar o conceito de algoritmo e sua formação amparada pelos alicerces da matemática, já que ela é a base estrutural da IA pelo que explica o maior expoente no assunto, *Philippe C. Jackson Jr*, em sua obra “*Introduction to artificial intelligence*”<sup>9</sup>:

A descrição matemática de algo é, portanto, um conjunto possivelmente infinito, mas finitamente descritível, de sentenças, cada uma das quais afirma algo sobre o objeto sendo descrito. Se o objeto é infinito e ainda assim finitamente descritível, então, intuitivamente, existem “padrões” que se mantêm em todo o objeto, e esses padrões formam a base de nossa descrição matemática.<sup>10</sup>

Um algoritmo pode ser definido em breves linhas como uma sequência de passos finita utilizados para resolver um determinado problema. Quando da construção de um algoritmo devem ser observadas algumas premissas consideradas básicas como: definir ações simples ser possibilitar a presença de dúvidas (ambiguidade), organização ordenada das ações dentro de uma sequência finita de passos.

Certos disso passa-se a compreender a importância do algoritmo para a IA; através do algoritmo o sistema de inteligência será desenvolvido a ponto de, autonomamente, entregar aquilo que dele se espera. Imagine, por exemplo, um robô treinado para encher um copo de água sempre que ele esvaziar. Os possíveis passos na construção desse algoritmo seria: 1) Coloque o copo abaixo do bico de água, 2) abra o registro, 3) acompanhe o enchimento até estar 90% preenchido, 4) Feche o registro.

---

9 JACKSON, Philippe C. **Introduction to artificial intelligence**. Toronto, Ontario: General Publishing Company, Ltd., 1985. p. 35

10 *A mathematical description of something is thus a possibly infinite yet finitely describable set of sentences, each of which states something about the thing being described. If the thing is infinite and yet finitely describable, then, intuitively, there are “patterns” which hold throughout the thing, and these patterns form the basis of our mathematical description.*

Logicamente o exemplo acima é bastante simples, mas demonstra com clareza o conjunto de passos a serem seguidos pela máquina bem como a autonomia dela identificar o copo vazio e tomar a decisão de enchê-lo. Em suma, é isso. Capacidade da máquina analisar uma volumosa quantidade de dados e fazer previsões precisas e eficientes.

Os comandos criados não propuseram para a máquina a análise, mas apenas o “encher o copo quando o mesmo estivesse vazio”. Agora se nesse conjunto fosse inserido para o sistema higienizar o copo antes de enchê-lo todas as vezes que ele for utilizado pelo público alfa ou beta, cria-se uma espécie de viés.

Um dos pontos a se destacar é a necessária transparência da forma como a máquina foi desenvolvida e sua forma de proceder diante das expectativas que foram criadas em relação a sua atuação. Para isso, o processo necessita ser explicável, transparente, de modo que vieses discriminatórios possam ser imediatamente corrigidos.

Além disso, muito importante a replicação do conceito de *accountability*. Sobre o tema, Henrique Alves Pinto em seu artigo “A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária *accountability*”, publicado na Revista de Informação Legislativa, explica que,

[...] não tem uma tradução mais precisa na língua portuguesa, é conceito que denota práticas a serem observadas por aqueles que exercem relevantes funções em dada sociedade, a exemplo dos Poderes Públicos e das grandes corporações empresariais. Nesse sentido, de forma simplificada, *accountability* é o agir pautado por responsabilidade ética, transparência das ações, com uma devida e adequada prestação de contas de tais atos. Tal concepção liga-se à ideia de governança e também à de responsabilidade civil.

À medida que as máquinas de IA se tornam mais autônoma e tomam decisões que podem interferir na vida das pessoas, surgem questões éticas a serem pensadas. Por exemplo, em carros autônomos, qual deve ser a prioridade em situações de acidente? Devem ser considerados como fatores idade, sexo ou status socioeconômicos? Os sistemas de IA devem ser desenvolvidos com capacidade de tomar decisões éticas transparentes e definidas com os valores e normas da sociedade.

Pois bem. Conforme destacado até o presente, a discussão sobre a responsabilização pelo uso IA ainda é assunto que por muito tempo fará parte das preocupações a nível mundial, até porque, por mais que se busque o modelo ideal sabe-se que isso é praticamente impossível. Talvez a melhor proposta seja aquela que consiga dimensionar impactos negativos e responsabilização por ocorrências.

E o que tudo isso tem a ver com a democracia?

### **3. A DEMOCRACIA E OS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL**

Os últimos anos não foram os melhores para se exemplificar o exercício da democracia. Ou talvez até foram posto que aparentemente ela venceu; mas

se isso realmente aconteceu, foi a duras penas, em especial nas últimas eleições presidenciais americanas em que Donald Trump foi derrotado por Joe Biden e no Brasil Jair Messias Bolsonaro por Luís Inácio Lula da Silva.

Para melhor delimitar o foco dessa pesquisa, pautaremos a narrativa sobre os fatos relacionados ao caso brasileiro, sem, contudo, deixar de trazer à tona pontos de semelhança do que em ambos os países aconteceu.

Em uma democracia, não se pode fazer o que se quer. É um projeto político fundamentado na plena cidadania, na construção do bem comum entendido como a experiência da ação do cidadão. É um comando que se cumpre obedecendo. Constrói a cidadania. Leis boas, justas que são cumpridas<sup>11</sup>.

A citação acima é do artigo “*Democracia sin democratas*”<sup>12</sup> do autor argentino Marcos Roitmann Rosenmann onde discute o exercício da democracia e suas derivações, em especial aquelas que revelam uma resistência contra a exploração. Assim como não se pode fazer o que se quer, não se pode querer tudo que quer; o revés faz parte da democracia. E além disso, as disputas dentro da democracia devem ser justas.

É sabido que a democracia, tida por menos pior das formas de governo, também se sustenta (em algumas situações) sobre os pilares da exploração, assim como outros modelos. Evidentemente a proposta desta pesquisa não é confirmar a afirmação feita acima, até por que espera-se que isso seja interpretado de maneira positiva, madura, diferente daquela que a maioria das pessoas idealiza, romantiza; é sim um regime de governo; mas não o melhor, pois isso somente se permitiria concluir se os demais modelos fossem bons; mas o menos pior, pois os demais impraticáveis, opressores. E sobre qual democracia está se falando: aquela idealizada ou aquela real?

Adverte Giovanni Sartori em sua obra *Que és la democracia?*<sup>13</sup>

Definir a democracia - como estamos vendo - não é nada simples nem fácil. “Democracia” é uma palavra que é usada em discursos longos. Ao desenvolver nossos argumentos, devemos ter cuidado com todo tipo de armadilhas. A insídia subjacente - e sempre recorrente - é o simplismo e, por isso (nas palavras de Lenin), “a doença mortal do infantilismo”. É verdade que devemos tornar a ideia de democracia o mais simples possível, já que a pólis exige mais do que qualquer outra que seus próprios princípios e mecanismos sejam amplamente compreendidos. Mas também é possível morrer de simplificação excessiva. A única maneira de resolver os problemas é conhecendo-os, sabendo que eles existem. O simplismo os anula e, assim, os agrava<sup>14</sup>.

---

11 *En democracia no se puede hacer lo que se quiere. Es un proyecto político fundado en la ciudadanía plena, en la construcción del bien común entendido como la vivencia de la acción del yo ciudadano. Es un mandar obedeciendo. Construye ciudadanía. Leyes buenas, justas y que se cumplan.*

12 ROITMAN ROSENMAN, Marcos. **Democracia sin demócratas y otras invenciones**. Buenos Aires: Sequitur, 2005. p. 9.

13 SARTORI, Giovanni. **Que és la democracia?** Tradução: Miguel Ángel González Rodríguez. Firenze: Editora Pátria, 1992. p. 10.

14 *Definir la democracia - lo estamos viendo - no es nada simple ni fácil. “Democracia” es una palabra que se usa en largos discursos. Al desarrollar los planteamientos debemos cuidarnos de toda clase de trampas. La insidia de fondo - y siempre recorrente- es el simplis-*

A democracia contemporânea enfrenta um desafio sem precedentes na era da Inteligência Artificial - a disseminação de notícias falsas que ficou popularmente conhecida como *fake news* trouxe significativo impacto para a sociedade e o sistema político. Já não se permite trabalhar a ideia de governo do povo, feito pelo povo e para o povo (lembrando da conhecida frase do presidente americano Abraham Lincoln); a questão agora se amplia.

### 3.1. DESAFIOS CONTEMPORÂNEOS. A INFLUÊNCIA DA IA

A discussão extrapola os limites filosóficos e recai sobre a necessidade de explicações mais assertivas do tipo: do povo, mas quem será seu representante? Para o povo, mas qual povo? Pelo povo, mas quais interesses do povo serão paudados? Deve prevalecer a vontade da maioria ou a vontade do maior número de pessoas? E isso é bastante delicado, pois se estivermos lidando com a vontade do maior número de pessoas, nem sempre será alcançado o propósito da maioria. É o típico caso das eleições presidenciais do modelo brasileiro.

Suponha-se a existência de um eleitorado de 1.000.000 de pessoas; necessidade de aprovação da maioria do eleitorado para declaração de vitória deste ou daquele candidato que se não alcançada deve submetida novamente ao povo para uma segunda oportunidade, agora restrita a apenas dois concorrentes, para se chegar à “vontade da maioria”. Veja o cenário:

- Candidato A: 400.000 votos.
- Candidato B: 250.000 votos.
- Candidato C: 150.000 votos.
- Candidato D: 100.000 votos.
- Candidato E: 100.000 votos

Sendo este o resultado do pleito eleitoral, seguindo o modelo brasileiro, necessidade de convocação de novas eleições, mas agora em disputa apenas os dois mais votados, que no caso é o candidato A com 400.000 votos e candidato B com 250.000 votos. De imediato já se desconsidera a vontade de 350.000 pessoas (somatória dos votantes nos candidatos C, D e E). Após o segundo tudo se confirma a vitória do candidato A, contando agora com 550.000 votos e candidato B com 450.000.

---

*mo y por ello (en frase de Lenin) “la enfermedad mortal del infantilismo”. Es cierto que se debe hacer fácil, en lo posible, la idea de democracia, ya que la ciudad democrática exige más que cualquier otra que sus propios principios y mecanismos se an generalmente entendidos. Pero de mucha simplificación también se puede morir. El único modo de resolver los problemas es conociéndolos, saber que existen. El simplismo los cancela y, así, los agrava.*

Na realidade o candidato A não foi a escolha de 550.000 pessoas; ele permaneceu sendo a escolha de 400.000 pessoas. Os votos adicionais não foram dados seguindo à vontade, mas sim a necessidade de alcance da maioria – só escolheram por que assim foi determinado.

O cenário fica ainda mais inusitado se após o 2º pleito vence o candidato B, antes com 250.000, agora com 550.000, ficando o candidato A com 450.000 votos, 50.000 a mais que no primeiro pleito. Nesse cenário não prevaleceu a vontade da maioria, pois pela vontade o candidato era opção de apenas 250.000 pessoas; as outras 300.000 pessoas não o queriam, pois não foi a primeira escolha. Porém, não querer o candidato A era maior que o não querer ao candidato B. Teoricamente a prevaleceu a vontade de apenas 250.000 pessoas; as outras 750.000 se conformaram; eis a diferença entre a vontade da maioria (democracia majoritária) e a vontade da maioria de pessoas (democracia consensual).

Ambos os modelos se adequam a máxima de que a vontade da maioria foi feita; o grande problema está na disputa por aqueles indivíduos que não tiveram suas vontades respeitadas; o ideal era a tentativa de convencer a escolher pelo melhor e não pelo outro ser ruim e para isso manipular informações e destruir a democracia. Ou seja, ao invés de convencer que candidato A é o melhor para as necessidades do povo, convence que o candidato B não é a melhor escolha, ainda que o candidato A não seja tão bom assim. É a polarização: escolhe-se este por não querer aquele. A democracia não alcançou a vontade da maioria, alcançou a vontade da maioria de algumas pessoas. E isso precisa ser esclarecido.

Segundo Arend Lijphart em sua obra “Modelos de Democracia”<sup>15</sup>,

[...] existe na ciência política uma tendência surpreendentemente forte e persistente de se associar a democracia somente ao modelo majoritário, e de não reconhecer a democracia de consenso como uma alternativa igualmente legítima. [...] as democracias majoritárias puras, ou quase puras, são na verdade muito raras [...] a maioria das democracias tem traços consensuais significativos ou mesmo predominantes.

A ascensão das mídias sociais e das plataformas de compartilhamento de conteúdo permitiu que *fake news* se espalhassem de forma viral. A IA desempenha um papel significativo nesse processo, uma vez que os algoritmos de recomendação em redes sociais são frequentemente utilizados. Ou a IA ingressa como vilã ou como antagonista.

A proposta aqui não é de recriminar o uso da inteligência artificial, até porque, conforme demonstrou-se acima, seu uso é um caminho sem volta. E o problema pode não estar na inteligência artificial, mas a forma como o algoritmo

---

15 LIJPHART, Arend. **Modelos de democracia: desempenho e padrões em 36 países**. Tradução: Vera Caputo. Rio de Janeiro: Civilização brasileira, 2018. p. 21.

foi desenvolvido; e quem o desenvolveu foi o homem, as vezes em escancarada necessidade de poder, de vencer. Eis o problema da exploração.

### 3.2. FAKE NEWS E SEU PODER DE DESTRUIÇÃO

O fenômeno das *fake news* tem implicações profundas para os princípios democráticos. A disseminação de informações falsas pode distorcer a opinião pública, influenciar eleições, minar a confiança nas instituições democráticas e agravar divisões políticas.

Essa questão fica ainda pior quando se coloca em análise um eleitorado despreparado para avaliar se determinada informação é verdadeira ou falso; e talvez nem seja esse o ponto. Os recursos tecnológicos estão tão avançados que até mesmo aqueles indivíduos mais politizados, imparciais, preocupados, de fato, com as propostas de governo, projetos e atuação política do candidato, acabam se vendo enredado pelas mentiras inventadas para alcançar algum objetivo. No caso, fortalecer uma corrente e destruir outra, antagônica.

Daí vem os questionamentos que outrora permitiu afirmar que a democracia é a menos ruim dos regimes existentes. A democracia depende da existência de um espaço público informado e no qual os cidadãos possam tomar decisões políticas bem fundamentadas. Esse modelo poderia ser reconhecido com uma boa democracia. Nesse sentido, explica Leonardo Morlino<sup>16</sup>:

[...] considero uma democracia de qualidade ou boa aquela que apresenta uma estrutura institucional estável que realiza a liberdade e a igualdade dos cidadãos por meio do funcionamento legítimo e correto de suas instituições e mecanismos. Uma boa democracia é, portanto, inicialmente, um regime amplamente legitimado que satisfaz completamente os cidadãos (qualidade em termos de resultado). Quando as instituições têm o pleno apoio da sociedade civil, podem buscar os valores do regime democrático. Se, pelo contrário, as instituições precisam adiar seus objetivos e gastar energia e recursos para consolidar e manter sua legitimidade, ultrapassar até mesmo o limite mínimo para a democracia se torna uma façanha notável. Em segundo lugar, uma boa democracia é aquela em que os cidadãos, associações e comunidades dos quais ela é composta desfrutam de pelo menos um nível moderado de liberdade e igualdade (qualidade em termos de conteúdo). Terceiro, em uma boa democracia, são os próprios cidadãos que têm o poder de verificar e avaliar se o governo busca os objetivos de liberdade e igualdade de acordo com o estado de direito. Eles monitoram a eficiência da aplicação das leis em vigor, a eficácia das decisões tomadas pelo governo e a responsabilidade política e prestação de contas dos eleitos em relação às demandas expressas pela sociedade civil (qualidade em termos de procedimento)<sup>17</sup>.

---

16 MORLINO, Leonardo. What is a "Good" Democracy? Theory and Empirical Analysis. In: LESSONS FROM SOUTHERN EUROPE, 2002, California. **Lessons from Southern Europe**. [S. l.]: University of California, Berkeley, 2002. p. 20.

17 *A quality democracy is a 'good' democracy. As is evident, the defining problem concerns what is intended by the adjective. Starting from the definition mentioned above, and from the prevailing notions of quality, I consider a quality or good democracy to be one presenting a stable institutional structure that realizes the liberty and equality of citizens through the legitimate and correct functioning of its institutions and mechanisms. A good democracy is thus first and foremost a broadly legitimated regime that completely satisfies citizens (quality in terms of result). When institutions have the full backing of civil society, they can pursue the values of the democratic regime. If, in contrast, the institutions must postpone their objectives and expend energy and resources on consolidating and maintaining their legitimacy, crossing over even the minimum threshold for democracy becomes a remarkable feat. Second, a good democracy is one in*

Então, como alcançar essa democracia de qualidade se os recursos ofertados para os cidadãos nesse processo de escolha do que vale ou não a pena se apresenta vícios, em especial por recursos tecnológicos que dificilmente permitem discutir a veracidade?

Além disso, tem outro ponto muito importante: a velocidade da proliferação dessas notícias, a rapidez com que as *fakes news* podem se espalhar nas redes sociais e em outras plataformas digitais. A IA, por meio de algoritmos de recomendação, muitas vezes promove notícias sensacionalistas e polarizadoras, atraindo a atenção de um público cada vez maior. Isso cria um ambiente propício para a disseminação de informações falsas e prejudiciais.

O problema das *fake news* nas eleições brasileiras é uma preocupação crescente e complexa que tem afetado o cenário político do país nas últimas décadas, especialmente por conta do modelo de política que acabou se instaurando no país: polarizado. Se o indivíduo critica determinado lado, automaticamente é reconhecido como apoiador do outro e vice versa; se discorda de uma posição política ou de uma proposta do governo é taxado de apoiador do outro lado, do outro modelo.

Por conta disso, as discussões sobre política se enfraqueceram, dando espaço a máxima: de que lado você está? E isso é muito ruim porque a essência da democracia acaba se perdendo. Não é mais a vontade do povo em discussão, mas a vontade de grupos de seguidores deste ou daquele político, partido político. A ideologia perdeu espaço; a discordância perdeu espaço; ou o indivíduo está no time A (mesmo que esse defenda alguns pontos que discorde), ou o indivíduo está no time B (mesmo que esse defenda alguns pontos que discorde).

A polarização exacerbada por informações falsas pode levar a um ambiente político cada vez mais tóxico, onde o diálogo e a cooperação se tornam insustentáveis; impacto das *fake news* na democracia é profundo.

E o que são *fake News*? Entendemos por serem aquelas informações deliberadamente falsas ou enganosas apresentadas como notícias verdadeiras. Elas podem variar desde boatos e teorias da conspiração até informações completamente inventadas, muitas vezes com o objetivo de influenciar a opinião pública, ganhar audiência ou alcançar objetivos políticos. Portanto, *fake News* é a mentira que se propaga e causa o mal.

---

*which the citizens, associations, and communities of which it is composed enjoy at least a moderate level of liberty and equality (quality in terms of content). Third, in a good democracy it is the citizens themselves who have the power to check and evaluate whether the government pursues the objectives of liberty and equality according to the rule of law. They monitor the efficiency of the application of the laws in force, the efficacy of the decisions made by government, and the political responsibility and accountability of elected officials in relation to the demands expressed by civil society (quality in terms of procedure).*



Contudo, vem a pergunta: é proibido mentir? A discussão começa a ficar acalorada; a questão não é se proibido ou permitido, mas se possível identificar que o suposto fato, opinião, notícia, é mentira e, caso assim se conclua, quem as produziu. Talvez o maior desafio é identificar aquele que produziu uma *fake News*. A mentira identificada no direito penal brasileiro é tipificada por calúnia.

Então, veja. O maior problema da fake News é a ausência de vestígios de quem a produziu, pois se possível a identificação, a este deverá ser imputada a responsabilidade por eventuais resultados negativos, inclusive a reparação de danos. Daí a resposta para a pergunta de outrora: não é proibido mentir, mas se esta vier a causar dano, que o causador tenha ciência das possíveis responsabilizações pela lei, inclusive condenação criminal.

A IA pode ser empregada para analisar redes sociais e identificar padrões de disseminação de *fake news*. Algoritmos podem rastrear a origem de informações falsas, identificar contas suspeitas e mapear como essas informações se espalham através de comunidades online. Essas análises podem ajudar na identificação de fontes de desinformação e na implementação de estratégias direcionadas para combater sua disseminação.

Nesse momento vale uma importante observação. No Brasil, é livre a manifestação do pensamento, sendo vedado o anonimato. É o que nos apresenta o inciso VI do artigo 5º da Constituição Federal de 1988 (Brasil, 1988). Logo, impedir a criação de perfis falsas é uma obrigação dos provedores de internet (assim definidos pela lei 12.965/2014 – Marco Civil da Internet) (Brasil, 2014). A lei brasileira assim já determina.

A *fake News* existe, em especial, por conta da desinformação. E esse é o ponto que acima se destacou em relação a exploração do indivíduo sob o manto protetivo da democracia. As *fakes news* têm o potencial de desinformar o eleitorado, levando as pessoas a acreditar em informações falsas sobre candidatos, partidos políticos ou questões importantes. Isso prejudica a capacidade dos eleitores de tomar decisões informadas ainda mais quando usadas para manipular o resultado das eleições, disseminando informações enganosas que prejudicam ou beneficiam determinados candidatos. Isso mina a integridade do processo eleitoral.

O Brasil tem buscado adotar medidas para combater as *fakes news* durante as eleições, inclusive com projetos no legislativo, com por exemplo o PL26030/2020, com a finalidade de disciplinar a questão. No entanto, a eficácia dessas medidas ainda é objeto de debate, e há preocupações com a possível censura e restrição da liberdade de expressão.

Retomando para a discussão sobre a interferência da IA na democracia, do mesmo modo que ela possibilita a automatização da produção de *fake news* ela também pode ser uma ferramenta para desmascarar as notícias falsas e coibir

sua propagação. Algoritmos de geração de texto e edição de mídia podem criar conteúdo falso de maneira convincente e eficiente, mas também podem ter por função identificar a inverdade e propagar tal descoberta. A automação torna mais difícil rastrear e conter a propagação dessas informações enganosas pelo homem uma vez que elas podem ser produzidas em grande escala com facilidade, mas não para a máquina.

Algoritmos de aprendizado de máquina podem ser treinados para analisar grandes volumes de informações e identificar padrões associados a conteúdo falso. Isso pode incluir a análise de linguagem, verificação de fontes, comparação com informações de fontes confiáveis e análise de contexto. Além disso, a IA pode ser usada para monitorar a propagação de *fake news* até mesmo em tempo real, permitindo respostas mais rápidas e assim eficazes.

Também possível pensar na IA classificando conteúdo. Algoritmos podem ser usados para marcar ou rotular informações suspeitas como possível falsidade do conteúdo, mas também ajuda as plataformas de mídia social a priorizar a redução da visibilidade dessas informações. Essa proposta se apresenta viável desde que se tenha por alicerce a ética e a transparência nos filtros que forem criados, em especial se o crivo do material selecionado ficar sobre responsabilidade do homem.

Não obstante, ainda não nos parece ser a melhor alternativa uma vez que a máquina de inteligência artificial pode falhar e dentro deste panorama, diagnosticar mentirosa, falsa, informação que era verdade, real. Por conclusão, a informação verdadeira foi censurada pela máquina quando por esta foi considerada falsa.

Em outras palavras, se a máquina de inteligência artificial, cujos algoritmos foram desenvolvidos contendo vieses para identificar fake news, o erro na avaliação fatalmente será uma espécie de censura; é imputar a máquina a tarefa de determinar os limites da liberdade de expressão.

Resta então a dúvida: não se tem uma saída?

Entende-se que ela ainda pode não ter sido encontrada, definida esta ou aquela como a principal estratégia, ou que nem todas as alternativas foram testadas; mas uma que, sempre deve ser levada em consideração, é a educação; em especial, *in casu*, a educação digital. Campanhas de alfabetização digital estão sendo realizadas para ajudar o público a discernir notícias reais de falsas.

Uma campanha de alfabetização digital é um esforço organizado para educar as pessoas sobre como navegar com segurança, eficácia e responsabilidade no ambiente digital. Essas campanhas visam aumentar a literacia digital da população, capacitando os indivíduos a utilizar a tecnologia de forma consciente e crítica.

A IA pode ser usada para personalizar o conteúdo que os usuários veem online. Isso implica em algoritmos que levam em consideração a confiabilidade das fontes e a veracidade das informações ao apresentar conteúdo aos usuários. Essa personalização pode ajudar a reduzir a exposição das pessoas a *fake news* e a promover a diversidade de fontes de informação. Contudo, opositores a essa classificação trarão à baila a liberdade de escolha do indivíduo uma vez que este ficaria condicionado a buscar informações apenas nos veículos rotulados como ideais. Quem faria essa rotulação?

É importante reconhecer que o uso da IA no combate às *fake news* também apresenta desafios éticos. A moderação de conteúdo automatizada pode ser interpretada como censura, levantando questões sobre a liberdade de expressão. Além disso, os algoritmos podem cometer erros e excluir conteúdo legítimo por engano. Portanto, a implementação cuidadosa e transparente dessas soluções é essencial.

A IA tem o potencial de ser uma aliada poderosa na luta contra as *fakes news* na democracia. Sua capacidade de análise de dados em larga escala, detecção de padrões e personalização de conteúdo pode ser aproveitada para identificar e mitigar a disseminação de informações falsas. No entanto, é fundamental que o uso da IA seja acompanhado de considerações éticas e transparência para garantir que a liberdade de expressão seja preservada e que as ações tomadas sejam eficazes na promoção de uma informação mais precisa e responsável.

#### 4. CONCLUSÃO

A conclusão deste artigo destaca a dicotomia existente no papel da inteligência artificial em relação à democracia. É inquestionável que a IA apresente desafios substanciais para a manutenção da democracia, sobretudo no contexto das *fake news*. O fenômeno da disseminação de informações falsas e enganosas, amplificado pela atuação de algoritmos de recomendação enviesados negativamente nas redes sociais, mina a confiança pública nas instituições democráticas e exerce influência prejudicial sobre o processo eleitoral.

É imperativo que as sociedades estejam vigilantes diante dessas ameaças e desenvolvam estratégias capazes de atenuar os riscos inerentes à presença da IA; e que se atente a esse ponto: estratégias para se atenuar o uso incorreto e malicioso da IA e não o seu simples usar.

Não obstante, a IA também pode oferecer oportunidades valiosas para o aprimoramento da democracia. A capacidade da IA de analisar volumes significativos de dados em tempo real possibilita a detecção mais ágil de notícias falsas e desinformação. Além disso, as ferramentas de verificação de fatos apoiadas por IA podem contribuir para a distinção entre conteúdo confiável e enganoso. É o

que se pretendeu demonstrar: a IA pode se converter em uma aliada eficaz no combate às *fake news*, desde que seja empregada de maneira ética e transparente, *accountability* e *liability*.

A adequada regulamentação da IA deve ser levada a discussão. Deve-se estabelecer diretrizes claras para a utilização de algoritmos em plataformas de mídia social, exigindo transparência e responsabilidade por parte das empresas de tecnologia, em especial limitações efetivas na possibilidade de criação de perfis falso. Além disso, é fundamental que os cidadãos sejam devidamente instruídos sobre como identificar e resistir à desinformação, explorando as ferramentas de verificação de fatos apoiadas por IA que se encontram à disposição.

Por fim, a interação entre a IA e a democracia é uma temática complexa e em constante evolução. A IA inegavelmente apresenta obstáculos reais, mas também promove soluções promissoras para o combate às *fake news*. O delineamento do futuro dependerá das escolhas da sociedade no que concerne ao equilíbrio entre esses desafios e oportunidades, com o objetivo de promover uma IA que se coadune com os valores democráticos e resguarde a integridade do processo democrático.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALVES PINTO, Henrique. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária *accountability*. Revista de Informação Legislativa: RIL, v. 57, n. 225, p. 43-60, 2020. Disponível em: [http://www12.senado.leg.br/ril/edicoes/57/225/ril\\_v57\\_n225\\_p43](http://www12.senado.leg.br/ril/edicoes/57/225/ril_v57_n225_p43). Acesso em: 14 jun. 2023.

AZIMOV, Isaac. Eu, Robô. [S. l.]: Aleph, 2014.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 2016.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Senado Federal, 2014.

CALO, Ryan. Robotics and the new cyberlaw. SSRN Electronic Journal, 2014. Disponível em: <https://doi.org/10.2139/ssrn.2402972>. Acesso em: 11 maio 2023.

CRAWFORD, Kate. Atlas of AI. [S. l.]: Yale University Press, 2021. *E-book*. Disponível em: <https://doi.org/10.12987/9780300252392>. Acesso em: 1 maio 2023.

LJPHART, Arend. Modelos de democracia: desempenho e padrões em 36 países. Tradução: Vera Caputo. Rio de Janeiro: Civilização brasileira, 2018.

MORLINO, Leonardo. What is a “Good” Democracy? Theory and Empirical Analysis. *In: LESSONS FROM SOUTHERN EUROPE*, 2002, California. Lessons from Southern Europe. [S. l.]: University of California, Berkeley, 2002.

PASQUALE, Frank. Black box society: the secret algorithms that control money and information. [S. l.]: Harvard University Press, 2015. 320 p.

ROITMAN ROSENMANN, Marcos. Democracia sin demócratas y otras invenciones. Buenos Aires: Sequitur, 2005.

SARTORI, Giovanni. Que és la democracia? Tradução: Miguel Ángel González Rodríguez. Firenze: Editora Pátria, 1992.

# O USO DA IA GENERATIVA EM CAMPANHAS POLÍTICAS E SEUS IMPACTOS NO PROCESSO ELEITORAL DEMOCRÁTICO

ADELE MENDES WEINBERG<sup>1</sup>  
MARINA CRIVELLI SIMÕES<sup>2</sup>

## 1. INTRODUÇÃO

O cenário político contemporâneo é influenciado por uma série de fatores complexos que afetam diretamente o processo eleitoral democrático. A atual interação entre tecnologia e política desempenha um papel cada vez mais decisivo nas estratégias de campanha e influência dos eleitores. Nesse contexto, a Inteligência Artificial Generativa emerge como um ferramental de destaque, por seu potencial de impactar profundamente a maneira como as campanhas políticas hoje são conduzidas já que, em tese, poderiam alterar o funcionamento da democracia.

O uso crescente de Inteligência Artificial Generativa em campanhas políticas faz surgir preocupações quanto à integridade do processo eleitoral, sobretudo no que diz respeito ao seu caráter democrático. Ou seja, estimula o desejo de se descobrir as maneiras pelas quais essa nova tecnologia pode ser utilizada para manipular a percepção pública e, assim, criar conteúdos altamente personalizados, a ponto de gerar desinformação e influenciar a opinião dos eleitores. Ou seja, de que modo essa influência afeta a legitimidade do processo eleitoral democrático e, ao final, como é possível mitigar esse fenômeno danoso.

A hipótese é que o uso da IA generativa em campanhas políticas pode amplificar a polarização política, criar bolhas informativas e minar a confiança pública nas autoridades e instituições democráticas. Por outro lado, acredita-se que, embora a IA generativa ofereça oportunidades inovadoras para o engajamento dos eleitores, aquela também introduz riscos significativos de desinformação e manipulação dos resultados.

Para entender o contexto e as implicações da IA generativa nas campanhas políticas, o artigo recorreu a autores de variadas formações, a fim de realizar um

---

1 Graduanda em Direito pela Universidade Presbiteriana Mackenzie; <http://lattes.cnpq.br/3762831364131543>; [adelemendes@gmail.com](mailto:adelemendes@gmail.com).

2 Graduanda em Direito pela Universidade Presbiteriana Mackenzie; <https://lattes.cnpq.br/5528812216256630>; [marinacrivellismoes@gmail.com](mailto:marinacrivellismoes@gmail.com).

estudo comparativo bibliográfico, por meio da análise de fontes primárias e secundárias de artigos, reportagens e documentários. O enfoque está em três casos emblemáticos de campanhas políticas recentes que fizeram uso da IA generativa para gerar desinformação. Ademais, será explorada a questão da regulamentação e de propostas legislativas para mitigar o problema em questão.

A pesquisa destacará, portanto, as implicações reais da IA generativa nas campanhas políticas, desde a personalização extrema de mensagens até a possível manipulação da opinião pública. Espera-se, com os resultados alcançados, melhor informar o debate sobre possíveis regulamentações, práticas éticas e responsáveis no uso da IA generativa em contextos políticos, bem como promover uma compreensão mais aprofundada de como a tecnologia está impactando o processo eleitoral democrático.

Busca, assim, lançar luz sobre a interação humano-máquina, explorando as ramificações da IA generativa nos processos decisórios como um todo. Pois à medida que essa tecnologia continua a evoluir, é fundamental entender seus potenciais riscos e benefícios, a fim de garantir a integridade e a legitimidade nas tomadas de decisão em um mundo cada vez mais digital.

O artigo será estruturado em cinco sessões. A primeira contém os elementos de uma campanha política democrática; a segunda define desinformação no contexto de campanhas políticas; a terceira ilustra desinformação em campanhas políticas recentes: a dos EUA (2016), a do Quênia (2022) e a do Brasil (2022). Já a quarta sessão alerta para o uso de *bots e deepfakes* via Inteligência Artificial na política. E a quinta, ao final, faz recomendações específicas de como amplificar a detecção de desinformação gerada por esses novos aparatos tecnológicos.

## 2. DESENVOLVIMENTO

Desde a sua criação, os sistemas de IA Generativa (GenAI, em inglês) têm causado preocupação com a informação por estes gerada. Principalmente a partir de 2023, com a disponibilização *online* e gratuita do ChatGPT para o grande público, pois a popularização do uso desse novo tipo de tecnologia começou a impactar mais fortemente o cotidiano das pessoas com acesso à internet. Esse fenômeno, no entanto, tem gerado um alerta entre estudiosos e especialistas que não demoraram a perceber que, ao contrário do jornalismo tradicional, o conteúdo produzido pela IA não é submetido a praticamente nenhum tipo de curadoria, fazendo com o que seja tomado como verdade não passe, muitas vezes, de desinformação; ou seja, conteúdos incertos, imprecisos e/ou incompletos que são intencionalmente falsos e concebidos para causar dano. Motivados princi-

palmente para ganhar dinheiro, auferir vantagem indevida e/ou gerar influência política em contextos eleitorais.<sup>3</sup>

A preocupação com a veracidade das informações disponibilizadas nas GEnAIs é grande a ponto de existir um termo para traduzir a geração de resultados em tom de autoridade que, a princípio, podem parecer plausíveis, mas que são factualmente incorretos ou não relacionados ao contexto dado: são as chamadas alucinações da IA<sup>4</sup>. A tecnologia, no entanto, não se limita à criação de conteúdo na forma de textos, mas é também capaz de gerar imagens, sons e até mesmo vídeos e códigos. Assim como a criação de textos, essas outras produções também não estão isentas da falta de maior curadoria, aumentando a difusão de conteúdos potencialmente desinformativos. Sobretudo quando os tipos de linguagem são diversos.

Isso se dá pelo fato de que as imagens geradas por GEnAI demonstram alta capacidade de persuasão, considerando que a tecnologia já é capaz de sincronizar movimentos labiais e criar expressões faciais detalhadas em cenários altamente compatíveis com a realidade<sup>5</sup>. Por isso o termo *deepfake* para designar conteúdos falsos produzidos por IA utilizando as ferramentas listadas; sobretudo em tom pejorativo, malicioso, considerando o intuito de disseminar desinformação ao criar um cenário falso. O ator e cineasta norte americano Jordan Peele, por exemplo, chocou a população ao publicar um vídeo produzido por ele mesmo, onde o suposto ex-presidente dos Estados Unidos Barack Obama se pronunciava<sup>6</sup>, com o objetivo de conscientizar o público sobre as capacidades de persuasão de um *deepfake*. Com isso, provou que não só a IA generativa é possível de falha, como também pode ser programada para transmitir mensagens incorretas.

Peele não só alertou sobre os perigos do uso de *deepfakes* no geral, mas escolheu fazer isso especificamente em um contexto político, usando uma figura com influência política mundial. A “brincadeira” feita pelo autor denuncia uma das principais preocupações com a previsão do uso generalizado da IA Generativa no ano de 2024: a sua utilização em campanhas políticas para gerar conteúdos de imagem e texto manipulados.

---

3 WARDLE, Claire. **Understanding Information Disorder**. First Draft, out. 2019, p.8. Disponível em: <<https://firstdraft-news.org/long-form-article/understanding-information-disorder/>>. Acesso em: 12 out. 2023.

4 SAMPAIO, Rafael Cardoso. **ChatGPT and other AIs will change all scientific research: initial reflections on uses and consequences**. Disponível em: <<https://preprints.scielo.org/index.php/scielo/preprint/view/6686/12682>>. Acesso em: 4 out. 2023.

5 BOTELHO, Thaís Helena Falcão; NÖTH, Winfried. Deepfake: Inteligência Artificial para discriminação e geração de conteúdos. In: **TECCOGS – Revista Digital de Tecnologias Cognitivas**, n. 23, jan./jun. 2021, p. 69-78. Disponível em: <<https://revistas.pucsp.br/index.php/teccogs/article/view/55979/37927>>. Acesso em: 9 out. 2023.

6 FOLHA DE SÃO PAULO. **Diretor Jordan Peele faz vídeo com Obama para denunciar notícias falsas**, São Paulo, 18 de abril de 2018. Disponível em: <<https://www1.folha.uol.com.br/mundo/2018/04/diretor-jordan-peele-faz-video-com-obama-para-denunciar-noticias-falsas.shtml>>. Acesso em: 5 out. 2023.

### 3. ELEMENTOS DE UMA CAMPANHA POLÍTICA DEMOCRÁTICA

O objetivo precípua de uma campanha política é mediar a relação entre partidos, eleitores e candidatos. Por meio da discussão de programas de governo, apresentação de propostas e historificações dos candidatos, levantam questões basilares para a escolha eleitoral, visando tornar o eleitor um cidadão melhor informado. “Há, portanto, percepção já consensual de que as campanhas eleitorais têm algum impacto nas escolhas do eleitorado, especialmente quanto mais disputadas forem as eleições e quanto mais competitiva for a luta eleitoral”<sup>7</sup>.

Uma campanha política democrática, por sua vez, busca compor elementos que configurem características essenciais a esse regime político. Nas palavras de Jorge Miranda<sup>8</sup>:

Democracia exige exercício do poder pelo povo, pelos cidadãos, em conjunto com os governantes; e esse exercício deve ser atual, e não potencial, deve traduzir a capacidade dos cidadãos de formarem uma vontade política autónoma. Mais: democracia significa que a vontade do povo, quando manifestada nas formas constitucionais, deve ser o critério de ação dos governantes.

Nesse sentido, a veracidade das informações disseminadas em campanhas políticas é essencial para que esta se configure como democrática, uma vez que garante justamente a construção da vontade política autónoma descrita por Miranda. A veracidade dos fatos e argumentos utilizados pelo eleitor para decidir seus votos e posicionamentos garante que a soberania do povo, resguardada fortemente pelo regime político democrático, seja também verídica, uma vez que suas opiniões e decisões serão baseadas no senso crítico autónomo, isento de manipulação ou embasamento equivocado.

Ademais, o Supremo Tribunal Federal (STF) reconheceu por meio da Arguição de Descumprimento de Preceito Fundamental (ADPF) n. 541, que “o exercício do direito de voto é componente essencial da democracia representativa”<sup>9</sup>. Para além do voto, um processo eleitoral democrático deve contar com a plena liberdade de expressão, associação, manifestação e criação de partidos. Sem os demais elementos, o simples direito ao voto se torna inefetivo para o exercício da democracia.

Bem como o Tribunal Superior Eleitoral (TSE) definiu propaganda política como “o ato que leva ao conhecimento geral, ainda que de forma simulada, a candidatura, mesmo que apenas postulada, a ação política que se pretende de-

---

7 PIVA, Otávio. **Campanhas eleitorais e democracia: o diálogo a partir do direito de resposta**. Porto Alegre, 2014. Disponível em: <file:///C:/Users/Adele%20Mendes/Downloads/2014\_piva\_campanhas\_eleitorais\_democracia.pdf>. Acesso em: 9 out. 2023.

8 MIRANDA, Jorge. **Manual de Direito Constitucional**, VII, Coimbra, 2007, págs. 59 e segs.

9 BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental 541**. Distrito Federal, 26 set. 2018. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=749828733>. Acesso em: 12 out. 2023.



envolver ou as razões que induzam a concluir que o beneficiário é o mais apto ao exercício da função pública”<sup>10</sup>. Configura-se aqui uma ferramenta essencial para que o eleitor tenha o conhecimento necessário para escolher candidatos com base na afinidade ou concordância de valores, como melhor acima descrito.

#### 4. DESINFORMAÇÃO NO CONTEXTO DE CAMPANHAS POLÍTICAS

A desinformação é um recurso utilizado como estratégia deliberada ou maliciosa de comunicação com o objetivo de induzir o público-alvo a uma compreensão equivocada da realidade, podendo ocorrer com a construção de narrativas falsas e outros recursos para manipular pessoas com fins inescrupulosos em diversos contextos. Em um artigo publicado em 2017, a colunista Margaret Sullivan do jornal estadunidense *Washington Post*, definiu o conceito de *fake news* como: “mentiras construídas de forma deliberada, na forma de artigos de notícia, com a informação”<sup>11</sup>.

Já especialistas que estudam desinformação a classificaram em sete espécies de acordo com os impactos negativos que estas causam: conexão falsa, contexto falso, contexto manipulado, conteúdo falso, conteúdo manipulado, conteúdo criado e, por fim, sátira e paródia. Sobre esses tipos de distorção, pesquisadores da Fundação Getúlio Vargas concluem:

A partir daí, os autores fazem a classificação dos elementos — agente (tipo nível de organização, motivação, automação, audiência) e intérprete (leitura da mensagem e ação tomada) — e das fases — criação, produção e distribuição — que compõe o “information disorder”. Como é explicitado, “O agente que cria uma mensagem fabricada pode ser diferente do agente que distribui a mensagem”<sup>12</sup>.

A propagação de notícias falsas ou manipuladas total ou parcialmente incide especialmente no ambiente das redes sociais, visto que são os grandes propulsores de fatos e opiniões distribuídos de forma massificada, e em razão da descentralização do compartilhamento de conteúdo. O compartilhamento indiscriminado desses conteúdos e sem checagem de suas fontes representa uma grave ameaça ao processo democrático, podendo ser uma arma poderosa em períodos de campanhas eleitorais.

Isso porque a manipulação de informação que induz a uma determinada inclinação ao voto já elimina por si só a configuração de uma democracia plena

---

10 BRASIL. Tribunal Superior Eleitoral. **Ac de 19.12.2014** no R-Rp nº 83193, rel. Min. Dias Toffoli

11 SULLIVAN, Margaret. **It’s time to retire the tainted term ‘fake news’**. *Washington Post*, Washington, 18 abril 2018. Democracy dies in darkness. Disponível em: <[https://www.washingtonpost.com/lifestyle/style/its-time-to-retire-the-tainted-term-fake-news/2017/01/06/a5a7516c-d375-11e6-945a-76f69a399dd5\\_story.html](https://www.washingtonpost.com/lifestyle/style/its-time-to-retire-the-tainted-term-fake-news/2017/01/06/a5a7516c-d375-11e6-945a-76f69a399dd5_story.html)>. Acesso em: 5 out. 2023.

12 FGV, DAPP. **Desinformação nas eleições 2018 [recurso eletrônico]: o debate sobre fake news no Brasil**. Coordenador Marco Aurélio Ruediger. Rio de Janeiro 2019. Disponível em: <[https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/29093/5/BWEB%20PT%5D%20Relatório%20Fake%20News%20ON%20-%20ref%20policy%20paper%202.pdf?>](https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/29093/5/BWEB%20PT%5D%20Relatório%20Fake%20News%20ON%20-%20ref%20policy%20paper%202.pdf?) Acesso em: 10 out. 2023.

por meio de eleição, influenciando os resultados de uma votação e, conseqüentemente, tirando a autonomia do eleitor, já que não é mais capaz de votar no que acredita ou em quem tem mais afinidade. Logo, está propenso a acreditar em informações falsas e que não condizem com a realidade para, assim, construir sua opinião política acerca de candidatos ou de suas propostas. Sua liberdade para construção de um senso crítico é, então, contaminada por falsas premissas.

Assim, ao manipular campanhas políticas por meio de desinformação, manipula-se também o eleitorado, eliminando elementos fundamentais para a configuração de um processo político democrático.

## 5. DESINFORMAÇÃO EM CAMPANHAS POLÍTICAS RECENTES

Quando se discute sobre os impactos da desinformação no contexto democrático, uma questão fundamental é o período de campanhas eleitorais, geralmente marcadas por intensos períodos de polarização política, potencializados por muitas promessas que não se cumprem.<sup>13</sup>

E um fenômeno com grandes impactos negativos é a utilização de notícias falsas como anteriormente colocado, especialmente se criadas por IA generativa de textos e imagens, com o objetivo de condicionar as pessoas a votarem em um candidato específico por meio de falsas narrativas sobre os outros candidatos, de gerar sentimentos de desconfiança e indignação ou de simplesmente semear dúvidas quanto a legitimidade das instituições democráticas.

### 5.1. ELEIÇÕES PARA PRESIDÊNCIA ESTADUNIDENSE EM 2016

Um caso bastante emblemático foi o da empresa britânica *Cambridge Analytica*. A corporação esteve envolvida em diversos escândalos após investigações que comprovaram que a empresa usou tecnologias de IA para interferir parcialmente em processos democráticos. Especialmente durante as eleições estadunidenses e o plebiscito em que ocorreu a votação do Brexit no Reino Unido. A IA foi utilizada como uma forma de manipulação de algoritmos para destinar conteúdos específicos para os indivíduos e influenciar as suas perspectivas pessoais.

Além disso, vieram à tona denúncias gravíssimas de violação à privacidade por conta do vazamento de dados de aproximadamente 87 milhões de perfis da

---

13 RÖHE, Anderson. Infodemia, Direitos Humanos e a Indústria da Desinformação Digital. In: **V Congresso Internacional de Direitos Humanos de Coimbra**, 2020. p. 356. Disponível em :< [https://a3ec55aa-1c0f-448d-a555-bf0db2483a45.filesusr.com/ugd/8f3de9\\_aa1800128ec9419e837460a08ac70ffe.pdf](https://a3ec55aa-1c0f-448d-a555-bf0db2483a45.filesusr.com/ugd/8f3de9_aa1800128ec9419e837460a08ac70ffe.pdf)>. Acesso em: 12 out. 2023.

rede social *Facebook*<sup>14</sup> Esse caso foi tão impactante que influenciou importantes legislações internacionais que visam aplicar regras para as empresas e garantir a privacidade das pessoas que utilizam os serviços de internet, como a *Digital Services Act*, na União Europeia.

A polêmica envolvendo a Cambridge Analytica impactou profundamente o a visão da relação entre política de proteção de dados, campanhas políticas e redes sociais. Governos do mundo inteiro desenvolveram leis e regulações específicas para proteger os usuários e as empresas necessitam ajustar as suas práticas e responsabilidade<sup>15</sup>.

Nesse sentido, o acontecimento foi essencial para as discussões sobre os impactos de *fake news* e desinformação na democracia. O documentário realizado pela Netflix e dirigido por Karin Amara “*The Great Hack*”<sup>16</sup> ou Privacidade Hackeada em português, fez uma análise detalhada sobre o caso em questão, com depoimentos e gravações das sessões dos tribunais.

## 5.2. ELEIÇÕES PARA PRESIDÊNCIA QUENIANA EM 2022

Um outro exemplo recente foram as recentes eleições que ocorreram no Quênia em 2022, na qual foi desencadeada uma avalanche de notícias falsas e de discursos de ódio entre os apoiadores dos dois principais candidatos do país, Willian Ruto e Raila Odinga<sup>17</sup>. Foram identificados pela *MAPEMA consortium* – uma tecnologia de ponta que utiliza técnicas de *machine learning*, inteligência artificial e outras ferramentas para identificar conteúdo - 550 mil conteúdos considerados prejudiciais para o processo eleitoral democrático, publicados na rede social *Facebook* durante os períodos de eleições Quenianas.<sup>18</sup> O resultado foi inclusive questionado pelo candidato que perdeu as eleições, Raila Odinga, ao afirmar sistematicamente que as eleições foram fraudadas.

## 5.3. ELEIÇÕES PARA PRESIDÊNCIA BRASILEIRA EM 2022

Um exemplo mais contundente, por ser no Brasil, foi a narrativa agressiva contra o Tribunal Superior Eleitoral -TSE, na qual foi sistematicamente alegado

---

14 WAKKA, Wagner. **87 milhões de usuários tiveram dados do Facebook expostos; BR é o 8º da lista**. Canaltech. Notícias, Segurança. 4 abr. 2023. Disponível em: < <https://canaltech.com.br/seguranca/87-milhoes-de-usuarios-tiveram-dados-do-facebook-expostos-br-e-o-8a-da-lista-111264/>>. Acesso em: 15 out. 2023.

15 WAKKA, Wagner. **87 milhões de usuários tiveram dados do Facebook expostos; BR é o 8º da lista**. Canaltech. Notícias, Segurança. 4 abr. 2023. Disponível em: < <https://canaltech.com.br/seguranca/87-milhoes-de-usuarios-tiveram-dados-do-facebook-expostos-br-e-o-8a-da-lista-111264/>>. Acesso em: 15 out. 2023.

16 NETFLIX. **The Great Hack**. Direção Karin Amara. 2019. 2h 19min.

17 MEDIUM. **Unmasking hate speech in Kenyan elections with AI and collaboration**. Code for Africa. 12 jun. 2023. Disponível em: < <https://medium.com/code-for-africa/unmasking-hate-speech-in-kenyan-elections-with-ai-and-collaboration-576e37d4ccb5>>. Acesso em: 10 out. 2023.

18 CIPESA. **Kenya's 2022 political sphere overwhelmed by disinformation**. July 26, 2022. Disponível em: <<https://cipesa.org/2022/07/11187-2/>>. Acesso em: 9 out. 2023.

que as eleições de 2022 foram fraudadas após a vitória do atual presidente da república, Luiz Inácio Lula da Silva.

Tanto a oposição do candidato eleito, quanto os eleitores do então presidente Jair Messias Bolsonaro não só arguíram ao TSE, como também alegaram que a eleição fora alvo de fraudes. Essa alegação foi fruto de inúmeros documentos e análises falsas que circularam pela internet, muitas vezes sem fontes ou assinaturas, alegando que a contagem de votos ou o sistema de urnas no geral haveriam sido corrompidos. Tal ofensiva, no entanto, foi fortemente contra-argumentada com estudos, análises e revisões legítimas feitas pelos órgãos competentes. Ainda assim, era tão enraizada a desinformação sobre a legitimidade do processo eleitoral que levou o candidato Lula da Silva à presidência, que os eleitores de seu opositor, insatisfeitos com as pesquisas oficiais, foram levados a cometer uma invasão às instalações do Planalto, Congresso e Supremo Tribunal Federal - STF.<sup>19</sup>

Vale ressaltar também que Jair Bolsonaro se utilizou do discurso que descredibiliza a votação por meio das urnas desde a sua eleição para presidência, como parte de sua campanha política, bem como contribuiu com a desinformação acerca da sua legitimidade entre os seus eleitores. O que veio a ser entendido *a posteriori* como um atentado terrorista, essencialmente antidemocrático, ainda foi defendido pelos responsáveis usando discursos pró democracia, ao alegarem que estariam evitando uma eleição fraudada, qual seja, antidemocrática<sup>20</sup>.

Esse episódio reflete fortemente o poder que a desinformação tem sobre uma eleição democrática, especialmente em contextos no qual é utilizada para caracterizar atos comprovadamente democráticos como sendo “antidemocráticos”. Nesse sentido, os eleitores são manipulados a ponto de tomarem atitudes que manifestadamente acreditam estarem de acordo com a realidade; quando, na verdade, seus posicionamentos e conseqüentemente intenção de votos são embasados em informações falsas, disseminadas justamente com a intenção de evitar que a população construa um senso crítico livre e autônomo acerca das propostas e feitos políticos.

O atual ministro do Supremo Tribunal Federal, José Antônio Dias Toffoli escreveu:

Em tal cenário- caracterizado, no extremo pela destruição de uma compreensão comum da realidade – cria-se também uma atmosfera de medo. É nas fraturas sociais que se semeiam os

---

19 ROCHA, Aline Scarponi Pinto. **De manifestantes à terroristas: o enquadramento midiático e a circulação de sentidos do acontecimento 8 de janeiro de 2023**. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. In: 46º Congresso Brasileiro de Ciências da Comunicação – PUC-Minas – 4 a 8 set.2023. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sistemas.intercom.org.br/pdf/link\_aceite/nacional/11/0806202308562264c-f8a66715b4.pdf>. Acesso em: 12 out. 2023.

20 Ibidem.

medos, e o maior deles é o medo do outro, visto como inimigo, oponente, ameaça. O medo alimenta o preconceito e o ódio e é por eles alimentado, criando um ciclo vicioso. Tudo isso polui o debate democrático. O cidadão passa a formar suas opiniões e a conduzir na democracia guiada por ilusões, por inverdades, e a deturpação da realidade obstrui os caminhos da democracia. Ademais ultrapassando a fronteira do pluralismo – compreendido como “equilíbrio dinâmico” entre as diferenças como embate construtivo e transformador – inviabiliza-se o diálogo<sup>21</sup>.

## 6. USO DE BOTS E DEEPPFAKES NA POLÍTICA

Como se vê, o uso de tecnologias para gerar desinformação em campanhas políticas não é um fenômeno novo. Em 2016, as eleições norte-americanas já eram alvo de discussões polêmicas no mundo todo por conta do uso de *fake news* e algoritmos para manipular os eleitores. Bombardeados por desinformação e conteúdo extremista que alimentavam não só a opinião pública, inibindo o pensamento crítico, mas constituindo também em sua maioria desinformação para prejudicar o adversário concorrente, a população estadunidense foi alvo de uma eleição que se afastou muito de seu caráter democrático. No Brasil, o fenômeno se repetiu em 2022, novamente levando os eleitores a uma votação que se afastou de elementos democráticos por inibir seu pensamento crítico autônomo. No mesmo ano, Quênia passava pelo mesmo transtorno.

Por isso, o ano que se segue (2024) é alvo de preocupação ainda maior por conta da previsão do uso generalizado da IA Generativa para disseminação de deepfakes e *fake news*; o que pode conter um poder persuasivo ainda maior do que nos episódios passados, uma vez que agora se vale de imagens sintéticas ultra realistas. O uso de imagens manipuladas em vídeos onde supostas pessoas com poder de persuasão aparecem é ainda mais convincente, além de ser mais difícil de identificar a veracidade do conteúdo quando gerado por Inteligência Artificial.

## 7. COMO MITIGAR A DIFICULDADE DE DETECÇÃO DE DESINFORMAÇÃO GERADA POR IA GENERATIVA

Uma vez que a desinformação causa ameaças reais ao processo democrático, importante salientar que é preciso adotar estratégias articuladas para evitar a propagação de conteúdos falsos, especialmente em períodos eleitorais. Vários países, incluindo o Brasil, estão trabalhando em legislações que sejam eficazes contra a proliferação e a propagação desses conteúdos; como por exemplo, o *Digital Services Act*, criado pelo Parlamento Europeu e que serviu de exemplo para o resto do mundo. Esse *benchmarking* global da União Europeia sobre o restante do mundo é fruto do chamado Efeito Bruxelas, que André Sanches Siqueira

---

21 Supremo Tribunal Federal – STF. **Medida cautelar na arguição de descumprimento de preceito fundamental 572, Distrito Federal**, Disponível em: <<https://www.conjur.com.br/dl/resumo-voto-fachin.pdf>>. Acesso em: 10 out. 2023.

Campos define como a: “capacidade europeia de promover a sua globalização regulatória por meio de normas, regras e regulamentos que desenvolveu através de sua experiência histórica e institucional, utilizando-se desses instrumentos conectividade com vistas a traduzir sua ação externa em influência política.”<sup>22</sup>. Sobre seus efeitos no Brasil no contexto da desinformação, conclui Alesandro Gonçalves Barreto<sup>23</sup>:

Mesmo em países como o Brasil, tal como foi demonstrado neste artigo, é possível vislumbrar tanto o aspecto prático quanto o jurídico, constantes no Efeito Bruxelas. No âmbito prático, as relações com os provedores de aplicação, tais como Facebook, Google e Twitter, deixam clara a materialização da aplicabilidade dos mecanismos e regramentos das relações comerciais estabelecidas no Código de Conduta sobre a Desinformação. Em relação ao campo jurídico, o tema da desinformação traveste de forma categórica a interferência oferecida pela UE junto ao Poder Legislativo brasileiro, na medida em que existem mais de 50 projetos de lei inspirados nos regramentos europeus de combate a desinformação em trâmite. Eis que, o que regula o mercado interno da UE passa a balizar as relações estabelecidas em solo brasileiro<sup>24</sup>.

### 7.1. DETECÇÃO DE INFORMAÇÕES

No caso de imagens, vídeos ou áudios que são manipulados por intermédio da IA generativa é importante investir em modelos de detecção de informações. Ao realizar uma comparação com as propostas de regulamentação, que geralmente apresentam um processo mais moroso, a alocação de recursos em tecnologias que permitam a distinção entre conteúdo produzido por seres humanos e aquele gerado por sistemas de Inteligência Artificial pode representar uma solução eficaz para a mitigação dos potenciais riscos associados à tecnologia, enquanto aguardamos a concretização da regulamentação. A perda da capacidade de diferenciar entre conteúdo produzido por humanos e aquele gerado por IA acarreta uma série de desafios dentro do contexto de campanhas políticas democráticas, que variam desde questões relacionadas a manipulação e conteúdo *online* até a criação de campanhas de desinformação.

Uma outra faceta dessa discussão diz respeito à identificação do agente responsável pelo investimento em tecnologias de detecção. É provável que os ganhos que vêm da detecção de conteúdos gerados por sistemas de IA não se equiparem àqueles proporcionados por ferramentas criativas, o que pode desencorajar investimentos no setor privado.<sup>25</sup>

---

22 CAMPOS, André Sanches Siqueira. ‘Efeito Bruxelas’: a dimensão da globalização regulatória europeia no sul da ásia. Observatório de Regionalismo, Dossiê 2021. Disponível em: <chrome-extension://efaidnbmninnibpcapjpcglefindmkaj/http://observatorio.repri.org/wp-content/uploads/2022/02/Dossi%C3%AA-2021-Cap-14.pdf>. Acesso em: 8 out. 2023.

23 BARRETO, Alesandro Gonçalves. Desinformação e o Efeito Bruxelas: regramentos europeus para além de suas fronteiras e o caso brasileiro. In: **Revista Eletrônica Direito & TI** – Porto Alegre, VI.1, N.15, jan/abr, 2023. Disponível em: <https://direitoeti.emnuvens.com.br/direitoeti/article/view/158/126>. Acesso em: 8 out. 2023.

24 Ibidem.

25 BEYER, Jan Nicola. *The race to detect AI can be won*. 2023. Disponível em: <https://www.politico.eu/article/artificial-intelligence-ai-detection-race-can-be-won/>. Acesso em: 13 out. 2023.

Apesar dessa constatação, é plausível que a disseminação desse tipo de tecnologia estimule a necessidade de identificar criações geradas por IA, de forma análoga ao que ocorreu com o crescimento da internet e a subsequente necessidade de desenvolver *softwares* antivírus em resposta à proliferação de vírus de computador.<sup>26</sup>

Enquanto as estruturas legais estão em processo de formulação, é necessário que se debatam soluções técnicas capazes de contribuir para o desenvolvimento ético e responsável da tecnologia, visando a um código de conduta para a mitigação dos riscos associados à disseminação de desinformação por meio de sistemas de Inteligência Artificial Generativas nos meios de comunicação e informação.

Quanto ao uso da Inteligência Artificial como uma aliada contra a proliferação de desinformação, as grandes empresas de tecnologia estão investindo maciçamente em construção de *softwares*: a empresa Meta, por exemplo, que é responsável pelas redes sociais *Facebook* e *Instagram*, divulgou seu posicionamento sobre a utilização de Inteligência Artificial contra o avanço de notícias falsas<sup>27</sup>:

A Inteligência Artificial (IA) é uma ferramenta crucial para enfrentar esses desafios e impedir a disseminação de desinformação, porque nos permite alavancar e escalar o trabalho dos verificadores de fatos independentes que revisam o conteúdo de nossos serviços. Trabalhamos com mais de 60 organizações de verificação de fatos em todo o mundo, que revisam conteúdos em mais de 50 idiomas<sup>28</sup>.

## 7.2. INDICADORES

Uma outra forma de inibir que conteúdos gerados por IA generativa sejam utilizados em campanhas políticas para gerar desinformação é incluir indicadores. Esses rótulos ou sinais indicativos devem estar presentes em toda e qualquer informação, imagem ou vídeo que tenha sido total ou parcialmente produzida por IA Generativa, garantindo que qualquer um que receba a informação esteja ciente que ela foi total ou parcialmente gerada por um não humano; portanto, existe a possibilidade de ter sido manipulada ou não ter passado por algum tipo de curadoria.

O TikTok é um exemplo de rede social que já está tomando providências nesse sentido:

A inteligência artificial possibilita oportunidades criativas incríveis, mas pode confundir ou enganar os espectadores se eles não souberem que o conteúdo foi gerado ou editado artificialmente. A rotulagem do conteúdo ajuda a resolver esse problema, deixando claro para os

---

26 Ibidem.

27 META. **Usando inteligência artificial para detectar desinformação e conteúdo abusivo sobre COVID-19**. Notícia recentes. 12 mai. 2020. Disponível em: < <https://about.fb.com/br/news/2020/05/usando-inteligencia-artificial-para-detectar-desinformacao-e-conteudo-abusivo-sobre-covid-19/>>. Acesso em: 10 out. 2023.

28 Ibidem.

espectadores quando o conteúdo é significativamente alterado ou modificado pela tecnologia de IA. É por isso que estamos lançando uma nova ferramenta para que os criadores informem facilmente sua comunidade quando publicarem conteúdo gerado por IA<sup>29</sup>.

A plataforma ainda foi além e demonstrou seu comprometimento com *o Responsible Practices for Synthetic Media*, um código de práticas recomendadas do setor para transparência de IA e inovação responsável. O código em questão conta com apoio de grandes empresas como a Google, Meta, Microsoft e inúmeros outros agentes desenvolvedores de tecnologias que envolvem IA Generativa.<sup>30</sup> No mais, a rede explica que baseou sua iniciativa em estudos de especialistas como o Dr. David G. Rand, do MIT, que explora como os espectadores percebem diferentes tipos de rótulos de IA.<sup>31</sup>

Os estudos de Rand sobre como as pessoas percebem e reagem a rótulos de IA podem fornecer *insights* valiosos sobre como os eleitores interpretam e confiam nas informações durante campanhas políticas. Pois compreender essas dinâmicas é essencial para identificar e inibir a desinformação. Além disso, pesquisas com o mesmo enfoque podem ajudar na criação de rótulos eficazes para identificar conteúdo gerado por IA em campanhas políticas. Rótulos claros e informativos podem alertar os eleitores sobre a natureza do conteúdo e promover a conscientização sobre a possível manipulação.

Assim, indicadores de conteúdos feitos por IA têm o potencial de melhorar a conscientização, a transparência e a resiliência contra a desinformação em campanhas políticas, contribuindo para um ambiente político mais saudável e democrático. A rotulação como método também traz algumas outras vantagens para além do combate à desinformação, como em casos nos quais a IA é usada para gerar imagens ou áudios falsos que possam prejudicar a privacidade de indivíduos; no caso, os rótulos podem ajudar a proteger a segurança e a reputação das pessoas envolvidas.

Além disso, rotular conteúdo de IA pode facilitar a futura implementação de regulamentações e políticas governamentais relacionadas ao uso da IA, tornando mais claro quando a intervenção regulatória for necessária. O intuito é o de educar o público sobre as capacidades e limitações da IA, ajudando as pessoas a se tornarem mais alfabetizadas digitalmente e permitir que pesquisadores e analistas identifiquem e, assim, estudem o impacto da IA na sociedade, facilitando a coleta de dados confiáveis.

---

29 TIKTOK. **Novos rótulos para trazer mais contexto ao conteúdo gerado por IA**, 19 set. 2023. Disponível em: < <https://newsroom.tiktok.com/pt-br/novos-rotulos-para-trazer-mais-contexto-ao-conteudo-gerado-por-ia>>. Acesso em: 9 out. 2023.

30 Ibidem.

31 EPSTEIN, Z.; FANG, M. C.; ARECHAR, A. A.; RAND, D. G. **What label should be applied to content produced by generative AI?**. Disponível em: < [osf.io/preprints/psyarxiv/v4mfz](https://osf.io/preprints/psyarxiv/v4mfz)>. Acesso em: 11 out. 2023.



## 8. CONCLUSÃO

A utilização da Inteligência Artificial Generativa em campanhas políticas e seus impactos no processo eleitoral democrático é um tema de crescente relevância no cenário político atual. Ao longo deste artigo, exploramos diversos aspectos dessa questão, desde a ascensão da GenAI no contexto político até os desafios que ela apresenta e as possíveis estratégias para mitigar seus efeitos negativos.

A IA Generativa está se tornando uma ferramenta poderosa para a manipulação de informações e para disseminar a desinformação em campanhas políticas. Isso é uma ameaça significativa aos elementos essenciais de uma campanha política democrática, que devem se basear em princípios como transparência, explicabilidade, o acesso à informação precisa e a participação informada dos eleitores. Isso porque a desinformação no contexto de campanhas políticas, muitas vezes impulsionada por *bots* e *deepfakes*, mina a confiança do eleitorado e compromete a integridade do processo eleitoral. Portanto, é crucial que os responsáveis por conduzir campanhas políticas e os órgãos reguladores estejam atentos a esses desafios, bem como adotem medidas proativas para combater a desinformação.

No caso de imagens, vídeos ou áudios que são manipulados por intermédio da IA generativa é importante investir em modelos de detecção de informações, instaurar um monitoramento contínuo para melhor detecção, e por fim, adicionar indicadores aos conteúdos que comuniquem que aquela imagem ou vídeo em questão não são reais, e sim uma manipulação maquinímica. Ou, no caso de textos sintéticos, que foram elaborados por uma IA generativa; indicando, portanto, que não deve ter havido curadoria sobre aquela “informação”.

Logo, a detecção de desinformação pela IA exige constante desenvolvimento. As soluções devem se adaptar para acompanhar as táticas e estratégias dos criadores de desinformação. E a combinação de conhecimentos técnicos e multidisciplinares é essencial para o combate desse problema que representa uma ameaça nociva para o nosso Estado democrático de Direito, podendo desencadear consequências que prejudiquem a sociedade.

## REFERÊNCIAS BIBLIOGRÁFICAS

BARRETO, Alesandro Gonçalves. Desinformação e o Efeito Bruxelas: regramentos europeus para além de suas fronteiras e o caso brasileiro. In: **Revista Eletrônica Direito & TI** – Porto Alegre, Vl.1, N.15, jan/abr, 2023. Disponível em: <https://direitoeti.emnuvens.com.br/direitoeti/article/view/158/126>. Acesso em: 8 out. 2023.

BEYER, Jan Nicola. The race to detect AI can be won. 2023. Disponível em: <https://www.politico.eu/article/artificial-intelligence-ai-detection-race-can-be-won/>. Acesso em: 13 out. 2023.

BOTELHO, Thaís Helena Falcão; NÖTH, Winfried. Deepfake: Inteligência Artificial para discriminação e geração de conteúdos. In: **TECCOGS – Revista Digital de Tecnologias Cognitivas**, n. 23, jan./jun. 2021, p. 69-78. Disponível em: <https://revistas.pucsp.br/index.php/teccogs/article/view/55979/37927>. Acesso em: 9 out. 2023.

BRASIL. Supremo Tribunal Federal – STF. **Medida cautelar na arguição de descumprimento de preceito fundamental 572**, Distrito Federal, Disponível em: <<https://www.conjur.com.br/dl/resumo-voto-fachin.pdf>>. Acesso em: 10 out. 2023.

BRASIL. Supremo Tribunal Federal - STF. **Arguição de Descumprimento de Preceito Fundamental 541**. Distrito Federal, 26 set. 2018. Disponível em: <<chrome-extension://efaidnbmnnpbpcjpcglclefindmkaj/https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=749828733>>. Acesso em: 12 out. 2023.

BRASIL. Tribunal Superior Eleitoral - TSE. **Ac de 19.12.2014** no R-Rp nº 83193, rel. Min. Dias Toffoli

BRASIL. Tribunal Superior Eleitoral - TSE. **Propaganda político-eleitoral**. Disponível em: <<https://www.tse.jus.br/institucional/escola-judiciaria-eleitoral/publicacoes/revistas-da-eje/artigos/propaganda-politico-eleitoral>>. Acesso em: 12 out. 2023.

BRASIL. Tribunal Superior Eleitoral -TSE. **TSE aprova resolução para dar mais efetividade ao combate à desinformação no processo eleitoral**. 20 out. 2022. Disponível em: <<https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/tse-aprova-resolucao-para-dar-mais-efetividade-ao-combate-a-desinformacao-no-processo-eleitoral>>. Acesso em: 12 out. 2023.

CAMPOS, André Sanches Siqueira. **‘Efeito Bruxelas’: a dimensão da globalização regulatória europeia no sul da ásia**. Observatório de Regionalismo, Dossiê 2021. Disponível em: <<chrome-extension://efaidnbmnnpbpcjpcglclefindmkaj/http://observatorio.repri.org/wp-content/uploads/2022/02/Dossi%C3%AA-2021-Cap-14.pdf>>. Acesso em: 8 out. 2023.

CIPESA. **Kenya’s 2022 political sphere overwhelmed by disinformation**. Jul. 26, 2022. Disponível em: <<https://cipesa.org/2022/07/11187-2/>>. Acesso em: 9 out. 2023.

EPSTEIN, Z.; FANG, M. C.; ARECHAR, A. A.; RAND, D. G. **What label should be applied to content produced by generative AI?**. Disponível em: <[osf.io/preprints/psyarxiv/v4mfmz](https://arxiv.org/abs/2309.16771)>. Acesso em: 11 out. 2023.

FGV DAPP. **Desinformação na era digital: amplificações e panorama das Eleições 2018**. Rio de Janeiro, 2018. Disponível em: <<https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/25742/Desinforma%C3%A7%C3%A3o%20Policy-Paper-2%20Sala.pdf?sequence=1&isAllowed=y>>. Acesso em: 11 out. 2023.

FOLHA DE SÃO PAULO. **Diretor Jordan Peele faz vídeo com Obama para denunciar notícias falsas**. São Paulo, 18 abr. 2018. Disponível em: <<https://www1.folha.uol.com.br/mundo/2018/04/diretor-jordan-peele-faz-video-com-obama-para-denunciar-noticias-falsas.shtml>>. Acesso em: 5 out. 2023.

HARBATH, Katie. **History of the Cambridge Analytica Controversy**. Bipartisan Policy Center, mar. 2023. Disponível em: <<https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/>>. Acesso em: 5 out. 2023.

MARQUES, Simone Dias. **Pós-realidade e Teoria da Desinformação: inquietações sobre o uso massivo de IA Generativa**. 5º Fórum de estudos em informação, sociedade e ciência, Porto Alegre: UFRGS, 2023. Disponível em: <<chrome-extension://efaidnbmnnpbpcjpcglclefindmkaj/https://lume.ufrgs.br/bitstream/handle/10183/265448/001177114.pdf?sequence=1>>. Acesso em: 11 out. 2023.

MEDIUM. **Unmasking hate speech in Kenyan elections with AI and collaboration**. Code for Africa. 12 jun. 2023. Disponível em: <<https://medium.com/code-for-africa/unmasking-hate-speech-in-kenyan-elections-with-ai-and-collaboration-576e37d4ccb5>>. Acesso em: 10 out. 2023.

META. **Usando inteligência artificial para detectar desinformação e conteúdo abusivo sobre COVID-19**. Notícia recentes. 12 mai. 2020. Disponível em: <<https://about.fb.com/br/news/2020/05/usando-inteligencia-artificial-para-detectar-desinformacao-e-conteudo-abusivo-sobre-covid-19/>>. Acesso em: 10 out. 2023.

MIRANDA, Jorge. **Manual de Direito Constitucional**, VII, Coimbra, 2007, págs. 59 e segs.

NETFLIX. **The Great Hack**. Direção por Karin Amera. 2019. 2h 19min.

PINTO, Aline Rocha Scarponi. De manifestantes à terroristas: o enquadramento midiático e a circulação de sentidos do acontecimento 8 de janeiro de 2023. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. In: **46º Congresso Brasileiro de Ciências da Comunicação – PUC-Minas – 4 a 8/9/2023**. Disponível em: <[chrome-extension://efaidnbmnnpbpcjpcglclefindmkaj/https://sistemas.intercom.org.br/pdf/link\\_aceite/nacional/11/0806202308562264cf8a66715b4.pdf](chrome-extension://efaidnbmnnpbpcjpcglclefindmkaj/https://sistemas.intercom.org.br/pdf/link_aceite/nacional/11/0806202308562264cf8a66715b4.pdf)>. Acesso em: 12 out. 2023.

PIVA, Otávio. **Campanhas eleitorais e democracia: o diálogo a partir do direito de resposta**. Porto Alegre, 2014. Disponível em: <file:///C:/Users/Adele%20Mendes/Downloads/2014\_piva\_campanhas\_eleitorais\_democracia.pdf>. Acesso em: 9 out. 2023.

RÖHE, Anderson. Infodemia, Direitos Humanos e a Indústria da Desinformação Digital. In: **V Congresso Internacional de Direitos Humanos de Coimbra, 2020**. Disponível em: <https://a3ec55aa-1c0f-448d-a-555-bf0db2483a45.filesusr.com/ugd/8f3de9\_aa1800128ec9419e837460a08ae70ffe.pdf>. Acesso em: 12 out. 2023.

SAMPAIO, Rafael Cardoso. **ChatGPT and other AIs will change all scientific research: initial reflections on uses and consequences**. Disponível em: <https://preprints.scielo.org/index.php/scielo/preprint/view/6686/12682>. Acesso em: 4 out. 2023.

SULLIVAN, Maragret. **It's time to retire the tainted term 'fake news'**. Washington Post, Washington, 18 abr. 2018. Democracy dies in darkness. Disponível em: <https://www.washingtonpost.com/lifestyle/style/its-time-to-retire-the-tainted-term-fake-news/2017/01/06/a5a7516c-d375-11e6-945a-76f69a399dd5\_story.html>. Acesso em: 5 out. 2023.

TIKTOK. **Novos rótulos para trazer mais contexto ao conteúdo gerado por IA**. 19 set. 2023. Disponível em: < https://newsroom.tiktok.com/pt-br/novos-rotulos-para-trazer-mais-contexto-ao-conteudo-gerado-por-ia>. Acesso em: 9 out. 2023.

WAKKA, Wagner. **87 milhões de usuários tiveram dados do Facebook expostos; BR é o 8º da lista**. Canaltech. Notícias, Segurança. 4 abr. 2023. Disponível em: < https://canaltech.com.br/seguranca/87-milhoes-de-usuarios-tiveram-dados-do-facebook-expostos-br-e-o-8a-da-lista-111264/>. Acesso em: 15 out. 2023.

WARDLE, Claire. **Understanding Information Disorder**. First Draft, out. 2019. Disponível em: <https://firstdraftnews.org/long-form-article/understanding-information-disorder/>. Acesso em: 12 out. 2023.

# A LGPD BRASILEIRA E O OBSTÁCULO À PESQUISA ACADÊMICA: O CASO DO ‘FÓRUM DE CIDADÃOS PARTICIPANTES’

TATIANA VIEIRA DE MORAES<sup>1</sup>  
CELSO MARAN DE OLIVEIRA<sup>2</sup>

## 1. INTRODUÇÃO

A informação é elemento estruturante em um momento histórico de avanços tecnológicos e digitais e, nesse contexto, o indivíduo torna-se vulnerável à circulação e comercialização de seus dados pessoais, de sua intimidade e privacidade. Para proteção, controle e imposição de limites ao uso e tratamento de dados pessoais, os ordenamentos jurídicos vêm se reestruturando e se adaptando, como é o caso do Brasil.

Assim, a Lei Geral de Proteção de Dados (LGPD) brasileira foi publicada neste cenário e traz consigo princípios, fundamentos, regras e procedimentos para a segurança e proteção de dados pessoais, sem impedir, no entanto, a possibilidade de seu tratamento<sup>3</sup>. Em algumas situações, a LGPD prevê certa flexibilidade, como é o caso do tratamento de dados para fins de pesquisa acadêmica, uma vez que há necessidade de se compatibilizar a proteção de dados pessoais “com o pluralismo de ideias e a liberdade de manifestação do pensamento, bem como com a promoção da inovação científica no País”<sup>4</sup>.

Assim, objetiva-se neste artigo expor as nuances da LGPD quanto ao acesso e tratamento de dados pessoais para fins de pesquisa acadêmica, bem como apresentar o caso da criação do ‘Fórum de Cidadãos Participantes’ como uma alternativa à negativa a um órgão de pesquisa quanto ao acesso e tratamento de

- 
- 1 Doutoranda em Ciências Ambientais (PPGCAm/UFSCar) com período sanduíche na Universidade de Coimbra. Advogada; <https://lattes.cnpq.br/3999527499047171>; [tativmoraes@gmail.com](mailto:tativmoraes@gmail.com) - Mestre em Ciência Ambiental (PGCA/UFF). Especialista em Direito Ambiental (PUC-Rio). Mestre em Ciência Ambiental (PGCA/UFF). Especialista em Direito Ambiental (PUC-Rio). Especialista em Advocacia Pública (ESAP/UERJ). Especialista em Meio Ambiente (MBE/COPPE/UFRRJ). Graduada pela Faculdade de Direito/UFF. Experiência na área de Direito Ambiental, Legislação Ambiental e Ciências Ambientais.
  - 2 Doutor em Ciências da Engenharia Ambiental (USP); <http://lattes.cnpq.br/9911833172043700>; [celmaran@ufscar.br](mailto:celmaran@ufscar.br) – Mestre em Direito da Integração (Universidade de Coimbra). Graduado em Direito pela Faculdade de Direito de São Carlos. Professor do Departamento de Ciências Ambientais da Universidade Federal de São Carlos.
  - 3 COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de dados pessoais comentada**. São Paulo: Revista dos Tribunais, 2019, p. 39.
  - 4 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo - Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas**. Brasília: ANPD, 2023, p. 9.

dados pessoais para fins exclusivamente de estudos acadêmicos em democracia ambiental.

A literatura e os estudos de democracia participativa demonstram que a participação social por meio da escolha aleatória estratificada da população participante é a técnica mais apropriada para o equilíbrio e equidade no processo participativo. No entanto, propõe-se como problemática que a interpretação limitada e a má aplicação da LGPD podem criar verdadeiros obstáculos à plena democracia participativa por impedir a aplicação das melhoras técnicas e métodos democrático-participativos quando impossibilitam o acesso e tratamento de dados pessoais para fins de estudos e pesquisa acadêmica.

A relevância do assunto é justificada pela necessidade de constante discussão a respeito da implantação e interpretação da Lei Geral de Proteção de Dados no Brasil, de modo que a proteção de dados pessoais seja garantida, sem impedir que a pesquisa acadêmica e processos participativos democráticos sejam obstados.

O artigo utiliza abordagem metodológica de natureza qualitativa<sup>5678</sup>, pois proporciona descrições sobre uma realidade específica e a pesquisa pode ser classificada como descritiva<sup>9</sup> e exploratória<sup>10</sup>, uma vez que desenvolve processo analítico a partir de interpretações diversas dos atores sociais envolvidos com o objeto investigado. Quanto ao procedimento exploratório, foi realizado levantamento bibliográfico em plataformas científicas de pesquisa, acesso à legislação e normas em páginas oficiais, bem como descrição de estudo de caso a partir de contato direto dos autores com a situação estudada.

## 2. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD E A PESQUISA ACADÊMICA

A importância da *Proteção de Dados Pessoais* (PDP) passou a ter maior notoriedade com o advento do *Regulamento Geral sobre a Proteção de Dados* nº 679 de 2016 da União Europeia<sup>11</sup>, uma vez que a PDP passou a ser considerada um

- 
- 5 GODOY, Arilda Schmidt. Introdução à pesquisa qualitativa e suas possibilidades. *Revista de Administração de Empresas*, v. 35, n. 2, 1995.
  - 6 GODOY, Arilda Schmidt. Pesquisa Qualitativa: tipos fundamentais. *Revista de Administração de Empresas*, v. 35, n. 3, 1995.
  - 7 CRESWELL, John W. *Projeto de Pesquisa: Métodos Qualitativo, Quantitativo e Misto*. 3ª. ed., Porto Alegre: ARTMED, 2010.
  - 8 MILES, Matthew B.; HUBERMAN, A. Michael. *Qualitative data analysis: An expanded sourcebook*. 2 ed., London: Sage publication, 1994.
  - 9 BOGDAN, Robert. C.; BIKLEN, Sari. *Investigação qualitativa em educação*. Porto: Porto Editora, p. 134-301, 1994.
  - 10 SELTZ, Claire; WRIGHTSMAN, Lawrence Samuel; COOK; Stuart Wellford. *Métodos de pesquisa nas relações sociais*. São Paulo: Herder, 1967.
  - 11 UNIÃO EUROPEIA. Regulamento nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril. Bruxelas: *Jornal Oficial da União Europeia*, L 119, 4 de maio de 2016.

direito fundamental assegurado por todos seus os Estados-Membros<sup>12</sup>. A partir de então diversos outros países passaram a se preocupar com normatização da PDP.

No caso brasileiro, a tutela jurídica da PDP, até 2018, se dava de forma difusa e não específica na legislação, a exemplo do Código de Defesa do Consumidor e Lei de Acesso à Informação<sup>13</sup>. Uma Consulta Pública visando à elaboração de um Anteprojeto de Lei de Proteção de Dados Pessoais foi aberta em 2010<sup>14</sup> e, posteriormente, os Projetos de Lei nº 4.060/2012<sup>15</sup> e 330/2013<sup>16</sup> foram apresentados, respectivamente, à Câmara dos Deputados e ao Senado Federal. Nova Consulta Pública foi realizada em 2015<sup>17</sup> e o Projeto de Lei nº 5.276/2016<sup>18</sup>, elaborado após os debates públicos, foi anexado ao PL 4.060/2012.

Após longa tramitação, é publicada a Lei nº 13.709, de 14 de agosto de 2018<sup>19</sup>, denominada *Lei Geral de Proteção de Dados Pessoais (LGPD)*, que só teve pleno vigor a partir de 1º de agosto de 2021.

Destaque-se que, devido à importância, autonomia valorativa e suas peculiaridades, a PDP foi incluída entre os *direitos e garantias fundamentais* no Brasil por meio da Emenda Constitucional nº 115, de 10 de fevereiro de 2022<sup>20</sup>, que alterou o art. 5º da Constituição da República<sup>21</sup>, com acréscimo do inciso LXXIX, *in verbis*:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

---

12 *Ibid.*, consideração nº 1.

13 ANGELO, Edna da Silva. Lei geral de proteção a dados pessoais como elemento da agenda 2030: acesso à informação e desenvolvimento de competência crítica. *Revista ACB*, v. 26, n. 3, 2021, p. 3.

14 1º debate público sobre proteção de dados pessoais: <http://pensando.mj.gov.br/dadospessoais2011/debata-a-norma/>

15 BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.060, de 13 de junho de 2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Câmara dos Deputados, 2012.

16 BRASIL. Senado Federal. **Projeto de Lei nº 330, de 13 de agosto de 2013**. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Brasília: Senado Federal, 2013.

17 2º debate público sobre proteção de dados pessoais: <http://pensando.mj.gov.br/dadospessoais/>

18 BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5.276, de 13 de maio de 2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília: Câmara dos Deputados, 2016.

19 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018].

20 BRASIL. [Constituição (1988)]. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Brasília, DF: Presidência da República, [2022].

21 BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2023].

A LGPD *objetiva* proteger os direitos fundamentais de liberdade, de intimidade e de privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural<sup>22</sup> e, para tanto, estabelece o regramento e os procedimentos para o acesso, uso, tratamento, armazenamento e compartilhamento de dados pessoais. A LGPD indica, ainda, sanções administrativas<sup>23</sup> às infrações às regras e procedimentos de PDP<sup>24,25</sup>.

Nesse sentido, a lei preconiza o fortalecimento da PDP e garante o autodomínio do titular sobre seus dados pessoais, sem deslegitimar a possibilidade de tratamento destes dados<sup>26</sup>. Da mesma forma, gera segurança jurídica não apenas ao titular dos dados, mas também aos agentes de tratamento, uma vez que estabelece e consolida as bases normativas da PDP e fornece o fundamento legal para o tratamento dos dados pessoais<sup>27,28,29</sup>.

A LGPD é *fundamentada* no respeito à privacidade; na autodeterminação informativa; na liberdade de expressão, de informação, de comunicação e de opinião; na inviolabilidade da intimidade, da honra e da imagem; no desenvolvimento econômico e tecnológico e a inovação; na livre iniciativa; na livre concorrência, na defesa do consumidor; nos direitos humanos; no livre desenvolvimento da personalidade; na dignidade; e no exercício da cidadania pelas pessoas naturais<sup>30</sup>.

Há duas categorias de destinatários da LGPD: o *titular dos dados* e os *agentes de tratamento*. O *titular* é a pessoa natural, identificada ou identificável, a quem os dados pessoais pertencem<sup>31</sup>. Os *agentes de tratamento* são o controlador e o operador. O controlador é pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões atinentes ao seu tratamento. O operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamen-

---

22 BRASIL, 2018, arts. 1º e 17.

23 *Ibid.*, arts. 52 a 54.

24 KRÜGER, Cristiane; BALDASSARI, Adriana Cristina Castanho; LOPES, Luis Felipe Dias; SILVA, Lizana Ilha. Lei Geral de Proteção de Dados Pessoais: uma análise dos determinantes junto aos profissionais de Contabilidade. **Revista Catarinense de Ciência Contábil**, v. 20, 2021, p. 3.

25 FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Viviane da Silveira. Compliance de dados pessoais. In: TEPEPINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters, 2019, p. 680.

26 ANGELO, *op. cit.*, p. 7.

27 CARVALHO, Hannibal Escobar Ramos Henriques; FREITAG, Alberto Eduardo Besser; SANTOS, Daiane Rodrigues. Impactos da implantação da Lei Geral de proteção de dados pessoais no brasil: uma análise bibliométrica. **Revista de Gestão e Secretariado**, v. 13, n. 3, 2022, p. 1401.

28 BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a lei geral de proteção de dados pessoais. **Argumenta Journal Law**, n. 32, p. 202-203.

29 MALDONADO, Viviane Nóbrega (coord.). **LGPD - Lei Geral de Proteção de Dados Pessoais: manual de implementação**. São Paulo: Revista dos Tribunais, 2019, p. 16.

30 BRASIL, 2018, art. 2º.

31 *Ibid.*, art. 5º, inciso I.

to de dados pessoais de acordo com as orientações do controlador<sup>323334</sup>. Assim, a segurança dos dados pessoais é responsabilidade dos agentes de tratamento, que devem garantir que não ocorram vazamentos dos dados ou acessos não autorizados a estes<sup>3536</sup>.

Os *dados pessoais* são apresentados como um conceito aberto pela LGPD<sup>37</sup>, configurando-se como informações relacionadas à pessoa natural identificada ou identificável, o que pode se referir ao nome, domicílio, e-mail, idade, dentre muitas outras informações da pessoa<sup>38</sup>. No entanto, a LGPD detalha que alguns dados pessoais são considerados *sensíveis*, a exemplo das informações relacionadas à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual e dado genético ou biométrico<sup>39</sup>. Tais informações, além de muito íntimas e particulares, podem levar à identificação do titular, bem como suscitar aspectos discriminatórios e invasivos<sup>4041</sup>, devendo ser tutelados com maior cautela.

Ressalte-se que, embora muito se discuta a respeito de dados virtuais, a LGPD tutela os dados pessoais coletados e estruturados tanto em meio *digital*, como em meio *físico*<sup>4243</sup>.

Como órgão responsável pela regulação, controle e fiscalização da aplicação da LGPD, foi instituída a *Autoridade Nacional de Proteção de Dados (ANPD)*<sup>44454647</sup>, a quem compete exclusivamente a aplicação das sanções<sup>48</sup> previstas àqueles que desobedecerem às regras e procedimentos da lei<sup>49</sup>.

---

32 BOTELHO, *op. cit.*, p. 203-204.

33 FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. São Paulo: Revista dos Tribunais, 2019, p. 21.

34 BRASIL, 2018, art. 5º, incisos VI e VII.

35 *Ibid.*, art. 46.

36 FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, 2019, p. 296.

37 BOTELHO, *op. cit.*, p. 200.

38 FINKELSTEIN, FINKELSTEIN, *op. cit.*, p. 296.

39 BRASIL, 2018, art. 5º, inciso II.

40 FINKELSTEIN, FINKELSTEIN, *op. cit.*, p. 297.

41 CARVALHO; FREITAG; SANTOS, *op. cit.*, p. 1401.

42 BRASIL, 2018, art. 5º, inciso IV.

43 ANGELO, *op. cit.*, p. 4.

44 BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2019].

45 ANGELO, *op. cit.*, p. 6.

46 BOTELHO, *op. cit.*, p. 205.

47 FINKELSTEIN, FINKELSTEIN, *op. cit.*, p. 294.

48 BRASIL, 2018, art. 52.

49 *Ibid.*, art. 55-K.



Quanto à sua *aplicabilidade*, a LGPD esclarece a *quem* e a *que tipo de tratamento* de dados a norma se direciona, bem como aos que a lei não se aplica em sua totalidade. Assim, como titular de dados pessoais, a lei é aplicada a qualquer pessoa natural; já como agente de tratamento, aplica-se a LGPD a quaisquer pessoas física ou jurídica que realizem, no território brasileiro, a operação de tratamento desses dados, o que abrange coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração<sup>5051</sup>.

A lei preconiza, ainda, que o tratamento de dados deve observar os princípios da boa-fé; finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização; e prestação de contas<sup>52</sup>.

Por outro lado, o diploma normativo *não se aplica totalmente* ao tratamento de dados pessoais nas seguintes hipóteses<sup>53</sup>: a) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; b) realizado para fins exclusivamente jornalístico, artísticos ou *acadêmicos*; c) realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais; d) a dados pessoais provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Há, portanto, hipóteses de *afastamento parcial* da LGPD e, na sequência, será dado enfoque ao acesso e tratamento de dados pessoais para pesquisa acadêmica.

### **3. ACESSO E TRATAMENTO DE DADOS PESSOAIS PARA FINS EXCLUSIVAMENTE ACADÊMICOS**

Dentre as hipóteses de *afastamento parcial* da LGPD, está o tratamento de dados pessoais, inclusive os sensíveis<sup>54</sup>, para fins acadêmicos, que diz respeito à realização de estudos e pesquisas<sup>55</sup> por *órgão de pesquisa*<sup>56</sup>.

---

50 *Ibid.*, art. 3º e art. 5º, inciso X.

51 CARVALHO; FREITAG; SANTOS, *op. cit.*, p. 1401.

52 BRASIL, 2018, art. 3º.

53 BRASIL, 2018, art. 4º.

54 *Ibid.*, art. 11, inciso II, alínea c.

55 A ANDP utiliza as expressões *estudo e pesquisa* indistintamente. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), *op. cit.*, p. 8.

56 BRASIL, 2018, art. 7º, inciso IV.

De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), este afastamento parcial da LGPD pretende estabelecer uma relação de equilíbrio: “de um lado, a proteção de dados pessoais e as garantias da privacidade e da autodeterminação informativa e, de outro, a liberdade acadêmica e o livre fluxo de informações necessário para a realização de estudos e pesquisas nas mais diversas áreas do saber”<sup>57</sup>. De todo modo, este afastamento da norma “deve ser interpretado restritivamente, limitando-se às situações em que o tratamento de dados pessoais esteja estritamente vinculado ao exercício da liberdade acadêmica”<sup>58</sup>

*Órgão de pesquisa*, para a LGPD, é um órgão ou entidade da administração pública direta ou indireta ou uma pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico<sup>59</sup>. A ANPD destaca alguns exemplos de órgãos de pesquisa: Instituições de Ensino Superior públicas ou privadas sem fins lucrativos; centros de pesquisa nacionais e entidades públicas que realizam pesquisas<sup>60</sup>.

Para os estudos relacionados à saúde pública, os órgãos de pesquisa também poderão acessar bases de dados pessoais, desde que atendendo as regras e procedimentos específicos previstos na LGPD<sup>61</sup>.

Outra exceção disposta na LGPD para a pesquisa acadêmica diz respeito à eliminação dos dados pessoais após o término de seu tratamento, uma vez que a diploma normativo autoriza a conservação dos dados para estudo pelo órgão de pesquisa, caso seja necessário<sup>62,63</sup>.

Assim, pela LGPD, é autorizado o tratamento de dados pessoais visando à pesquisa acadêmica, desde que se garanta as seguintes medidas:

- a) sempre que possível, a anonimização dos dados pessoais<sup>64</sup>, em atendimento aos princípios da prevenção e segurança dos titulares<sup>65</sup>;
- b) “medidas protetivas necessárias e adequadas para a mitigação de riscos aos titulares dos dados pessoais”<sup>66</sup>;

---

57 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), *op. cit.*, p. 5.

58 *Ibid.*, p. 19.

59 BRASIL, 2018, art. 5º, inciso XVIII.

60 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), *op. cit.*, p. 29.

61 BRASIL, 2018, art. 13.

62 *Ibid.*, art. 16, inciso II.

63 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), *op. cit.*, p. 13.

64 BRASIL, 2018, art. 5º, inciso XI.

65 *Ibid.*, art. 6º, incisos VII e VIII.

66 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), *op. cit.*, p. 15.

- c) O tratamento dos dados deve estar amparado em uma das hipóteses legais previstas na LGPD, tal como o consentimento do titular, a realização de estudos por órgão de pesquisa e o atendimento a interesse legítimo<sup>67</sup>;
- d) adoção do princípio da boa-fé e demais princípios da LGPD no tratamento dos dados<sup>68</sup>;
- e) os estudos e pesquisas em saúde pública devem observar requisitos específicos<sup>69</sup>: os dados pessoais devem ser tratados exclusivamente dentro do órgão de pesquisa; o tratamento dos dados deve ser estritamente para a finalidade da pesquisa; os dados pessoais devem ser mantidos e armazenados em ambiente controlado e seguro e, sempre que possível, com a sua anonimização ou pseudonimização; é vedada a transferência dos dados pessoais para terceiros; devem ser respeitados os padrões éticos relacionados à pesquisa; é vedada a revelação dos dados pessoais no momento da divulgação dos resultados ou parte dos estudos.

#### 4. ESTUDO DE CASO: A CRIAÇÃO DO ‘FÓRUM DE CIDADÃOS PARTICIPANTES’ (FCP)

Uma sociedade fundamentada em preceitos democráticos preconiza a maior proximidade dos cidadãos com os assuntos públicos, principalmente o envolvimento e integração da população na construção de políticas públicas. A partir desta premissa, o Centro de Estudos em Democracia Ambiental da Universidade Federal de São Carlos (CEDA-UFSCar) direcionou seus estudos e pesquisas na construção de metodologia participativa para políticas públicas ambientais no município de São Carlos, SP, Brasil, visando alcançar os preceitos da sustentabilidade local.

A par das inúmeras metodologias aplicáveis para a discussão e construção de políticas públicas, o CEDA-UFSCar propôs-se em construir uma metodologia participativa para políticas públicas ambientais naquele município, de modo a elevar o nível da participação popular, possibilitando, assim, que os cidadãos não sejam simplesmente informados ou consultados, mas que possam contribuir com a tomada de decisão, ascendendo, assim, na escada de participação de Arnstein<sup>70</sup> ao patamar em que o governo atribui poder à população.

---

67 *Ibid.*, p. 22.

68 BRASIL, 2018, art. 6º.

69 *Ibid.*, art. 13.

70 ARNSTEIN, Sherry. R. A ladder of citizen participation. *Journal of the American Institute of Planners*, v. 35, p. 216-224, jul. 1969.

Neste sentido, o CEDA-UFSCar idealizou a construção de uma metodologia verdadeiramente participativa e que se adequasse à realidade local e, para tanto, utilizou como modelo-base as experiências de participação social existentes e critérios obtidos a partir de métodos já experimentados.

Durante a formação do novo método participativo, identificou-se a necessidade de um agente ou uma instituição facilitadora para atuar durante todo o processo, papel que tem sido desempenhado pelo Ministério Público do Estado de São Paulo<sup>71</sup>.

Ao se atingir a fase de aplicação do método, a proposta consistia em uma *seleção aleatória estratificada* de municípios, por meio de *classificação por cotas e ponderação*, em espaço amostral o mais amplo possível, contemplando todo o município de São Carlos-SP.

Em uma *seleção aleatória estratificada*<sup>72</sup> a população é dividida em grupos (estratos) considerando um ou mais atributos sociodemográficos comuns, garantindo que haja representação de subgrupos ou estratos específicos. Por exemplo, divisão considerando os critérios sociodemográficos de gênero, idade, local de residência, dentre outros. Assim, é possível aumentar a percepção de equidade, uma vez que supera os vieses demográficos.

A *classificação por cotas e ponderação*<sup>73</sup> garante maior representatividade de grupos de participantes menos engajados, pois permite correções *ex ante* ao resultado do sorteio, evitando distorções previsíveis, além de calibrar ainda mais precisamente a composição da amostra, aumentando a probabilidade de que o grupo seja suficientemente heterogêneo. Um exemplo seria dar mais peso aos menores de 25 anos em um sorteio para compensar a taxa de participação tradicionalmente mais baixa dessa faixa etária.

Para criar o espaço amostral e posteriormente convidar os municípios selecionados a participarem do método, a forma de obtenção dos dados pessoais para recrutamento da população indicada pelos métodos participativos estudados é a partir de banco de dados pessoais, tal como o cadastro eleitoral, banco de informações de títulos de imóveis ou banco de dados de domicílios do serviço de correios. O método do *Júri Cidadão*, por exemplo, praticado pela *New Democracy*<sup>74</sup>, utiliza-se do banco de dados de domicílios do serviço de correios da Austrália (*Australia Post*) para postarem convites aos cidadãos:

---

71 Na pessoa do 7º Promotor de Justiça de São Carlos, em atenção ao princípio do Promotor Natural.

72 SORTITION FOUNDATION. **Sortition Resource Guide for Educators**. Cambridge: Sortition Foundation, 2020, p. 4.

73 BERTELSMANN STIFTUNG. **Citizens' participation using sortition** – A practical guide to using random selection to guarantee diverse democratic participation. Gütersloh: Bertelsmann Stiftung, 2018, p. 11.

74 NEW DEMOCRACY. **What is a Citizens' Jury?** Walsh Bay: New Democracy Foundation, 2023.

Enviamos convites para uma amostra aleatória de endereços físicos (não endereços de cobrança) extraídos de informações de títulos de imóveis ou bancos de dados dos Correios da Austrália. Isto assegura que os inquilinos e aqueles que não estão nos registros eleitorais sejam alcançados - em resumo, a mais ampla base de dados possível. Os destinatários do convite são solicitados a se cadastrar on-line para indicar que estão disponíveis para a seleção final. Com base naqueles disponíveis, é feito um segundo sorteio aleatório que procura corresponder de forma aleatória às proporções demográficas requeridas. Este sorteio gera a composição final do júri. (Tradução nossa)<sup>75</sup>.

Considerando a inexistência de um banco público de dados de títulos de imóveis e de domicílios pelo serviço de correios no município de São Carlos-SP, optou-se pelo acesso aos dados de eleitores. Para tanto, o CEDA-UFSCar emitiu ofício ao 7º Promotor de Justiça de São Carlos (MPSP) esclarecendo os objetivos da pesquisa e solicitando consulta ao cadastro de eleitores dos Cartórios Eleitorais do Município de São Carlos para acesso a dados pessoais, tais como: sexo, idade, profissão e endereço, exclusivamente para fins de pesquisa acadêmica, a fim de aplicar o método participativo em estudo. O CEDA-UFSCar destacou que, no decorrer da pesquisa, seriam adotadas todas as medidas de proteção dos dados previstas na LGPD.

Assim, o MPSP requereu ao juízo da 121ª Zona Eleitoral de São Carlos-SP o acesso aos dados indicados, gerando o processo nº 0600024-06.2022.6.26.0121. Em sentença prolatada em 17/06/2022, o juízo indeferiu o requerimento formulado, com fundamento no sigilo dos dados solicitados e com base normativa no inciso X do art. 5º da Constituição de República, na LGPD e no art. 29 da Resolução do Tribunal Superior Eleitoral (TSE) nº 21.538/2003.

Em sua fundamentação, a r. Sentença entende que “a quebra do sigilo acarreta consequências gravíssimas para todos os partícipes da quebra do sigilo. Não basta o consentimento do eleitor”. Assim entendeu o i. Magistrado em sua decisão:

O requerimento formulado objetiva compartilhar dados pessoais do eleitor, o que é absolutamente impossível. Como já acentuado, a finalidade da coleta dos dados pessoais serviu exclusivamente para o seu alistamento eleitoral, e nada mais do que isso. Transferir os dados para o Grupo de Pesquisa implicaria em afrontar os princípios da finalidade e da adequação, expondo esses dados para finalidades incompatíveis com o propósito inicial.

Destaque-se que o CEDA-UFSCar enquadra-se no conceito de *órgão de pesquisa*, uma vez que a Instituição de Ensino Superior (UFSCar) é entidade da administração pública, sem fins lucrativos, legalmente constituída sob as leis brasileiras, com sede e foro no País e inclui em sua missão institucional e em seus objetivos a pesquisa científica e acadêmica.

---

75 *Ibid.*

A decisão judicial que negou acesso ao CEDA-UFSCar aos dados pessoais de eleitores fundamentou-se na LGPD e no art. 29 da Resolução do TSE nº 21.538/2003<sup>76</sup>, que dispunha sobre o alistamento e serviços eleitorais mediante processamento eletrônico de dados, a regularização de situação de eleitor, a administração e a manutenção do cadastro eleitoral, o sistema de alistamento eleitoral, a revisão do eleitorado e a fiscalização dos partidos políticos.

A LGPD, como visto, possibilita o acesso aos dados para fins acadêmicos. Já a Resolução do TSE nº 21.538/2003, por seu turno, foi revogada pela Resolução nº 23.659, de 26 de outubro de 2021<sup>77</sup>, que dispõe sobre a gestão do Cadastro Eleitoral e sobre os serviços eleitorais que lhe são correlatos. Esta norma estabelece que a gestão do Cadastro Eleitoral será efetuada com observância da conformidade do tratamento dos dados aos princípios e regras previstos na LGPD<sup>78</sup>.

Além disso, pelas Resoluções do TSE nº 23.656, de 7 de outubro de 2021<sup>79</sup> e nº 23.650, de 9 de setembro de 2021<sup>80</sup>, é possibilitado o acesso a dados pessoais custodiados pela Justiça Eleitoral quando presente uma das hipóteses de tratamento previstas na LGPD.

A partir deste ponto, o CEDA-UFSCar buscou outros bancos e registros de dados já existentes e acessíveis à pesquisa. A alternativa sugerida e executada pelo MPSP foi pleitear ao Município os dados registrais de imóveis. No entanto, as informações eram insuficientes para a pesquisa, uma vez que compreendiam apenas o número do registro dos imóveis e a localização (endereço), sem a inserção dos dados pessoais dos proprietários.

Em consequência da negativa judicial, optou-se, então, pela construção de uma base de dados própria a partir do autocadastramento dos munícipes interessados em participar das políticas públicas ambientais de São Carlos-SP. Foi elaborado um convite à população são carlense, com ampla divulgação em mídias sociais e por meio de cartazes distribuídos e afixados em locais de grande circulação. O convite continha um *QR Code* e as publicações midiáticas<sup>81</sup> indicavam o

---

76 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 21.538, de 14 de outubro de 2003**. Dispõe sobre o alistamento e serviços eleitorais mediante processamento eletrônico de dados, a regularização de situação de eleitor, a administração e a manutenção do cadastro eleitoral, o sistema de alistamento eleitoral, a revisão do eleitorado e a fiscalização dos partidos políticos, entre outros. Brasília: TSE, 2003.

77 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.659, de 26 de outubro de 2021**. Dispõe sobre a gestão do Cadastro Eleitoral e sobre os serviços eleitorais que lhe são correlatos. Brasília: TSE, 2021.

78 *Ibid.*, art. 1º, II.

79 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.656, de 7 de outubro de 2021**. Dispõe sobre o acesso a dados pessoais constantes dos sistemas informatizados da Justiça Eleitoral (JE). Brasília: TSE, 2021. Art. 1º, inciso II e art. 2º, parágrafo 4º.

80 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.650, de 9 de setembro de 2021**. Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral. Brasília: TSE, 2021.

81 Notícia divulgada em 24/08/2022 na página da UFSCar: <https://www.ufscar.br/noticia?codigo=14875>

*link* de um formulário eletrônico<sup>82</sup> para preenchimento pelo próprio titular dos dados pessoais, solicitando o nome, o e-mail e o telefone.

Assim, este grupo de pessoas cadastradas recebeu a denominação de ‘Fórum de Cidadãos Participantes’ (FCP) e, tendo o MPSP como entidade facilitadora, o FCP é atualmente um grupo de aproximadamente 100 residentes do município de São Carlos cadastrados e convidados a dialogarem sobre suas percepções ambientais, seus enfrentamentos quanto às demandas relacionadas aos assuntos públicos ambientais da cidade, nas quais se veem como agentes que podem contribuir para a formulação do planejamento de políticas públicas ambientais e solução dos problemas ambientais municipais em diversos cenários.

O FCP surge, assim, a partir do insucesso no acesso a dados pessoais do Cadastro Eleitoral de São Carlos-SP, por negativa judicial, o que impossibilitou o órgão de pesquisa promover a seleção aleatória estratificada e a classificação por cotas e ponderação, o que possibilitaria a participação popular mais justa e equitativa.

## 5. CONCLUSÃO

A LGPD é o principal diploma legal sobre proteção e tratamento de dados pessoais no ordenamento jurídico brasileiro e outras leis e normas que envolvam a temática devem ser criadas e interpretadas com base nela.

No caso da pesquisa acadêmica, em que o acesso e tratamento de dados pessoais é expressamente possível, a LGPD não só legitima a viabilidade do uso dos dados pessoais, como confere a segurança jurídica necessária para os pesquisadores. Assim, a norma estabelece as regras e procedimentos para proteção dos titulares, sem criar obstáculos ao acesso e tratamento de dados pessoais para fins de pesquisas e estudos acadêmicos.

As pesquisas acadêmicas sobre democracia participativa baseiam-se na participação de pessoas, portanto, o acesso e tratamento de dados de titulares é intrínseco a estes estudos. Dessa forma, a interpretação e aplicação deficitária da LGPD, sem levar em conta as nuances e especificidades trazidas pelo próprio diploma legal, acabam obstando o avanço de técnicas e métodos que viabilizem a democracia participativa em seu grau mais elevado.

## REFERÊNCIAS BIBLIOGRÁFICAS

ANGELO, Edna da Silva. Lei geral de proteção à dados pessoais como elemento da agenda 2030: acesso à informação e desenvolvimento de competência crítica. **Revista ACB**, v. 26, n. 3, p. 1–14, 2021. Disponível em: <https://revista.acbsc.org.br/racb/article/view/1816>. Acesso em: 30 set. 2023.

---

82 *Link* do formulário eletrônico:  
[https://docs.google.com/forms/d/e/1FAIpQLSfYL\\_Vvr2gGc7sg0KlxCOJru7ED7674VIfGvVwf4kSRnwF2QQ/viewform](https://docs.google.com/forms/d/e/1FAIpQLSfYL_Vvr2gGc7sg0KlxCOJru7ED7674VIfGvVwf4kSRnwF2QQ/viewform)

ARNSTEIN, Sherry R. A ladder of citizen participation. *Journal of the American Institute of Planners*, v. 35, p. 216-224, jul. 1969.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo - Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas**. Brasília: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>. Acesso em: 08 out. 2023.

BERTELSMANN STIFTUNG. **Citizens' participation using sortition** – A practical guide to using random selection to guarantee diverse democratic participation. Gütersloh: Bertelsmann Stiftung, 2018. Disponível em: <https://www.bertelsmann-stiftung.de/en/publications/publication/did/citizens-participation-using-sortition>. Acesso em: 24 maio 2022.

BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a lei geral de proteção de dados pessoais. *Argumenta Journal Law*, n. 32, p. 191–207, 2020. DOI: <https://doi.org/10.35356/argumenta.v0i32.1840>. Disponível em: <https://seer.uenp.edu.br/index.php/argumenta/article/view/312>. Acesso em: 27 set. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.060, de 13 de junho de 2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília: Câmara dos Deputados, 2012. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 04 out. 2023

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5.276, de 13 de maio de 2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Brasília: Câmara dos Deputados, 2016. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 04 out. 2023

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2023]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 05 out. 2023.

BRASIL. [Constituição (1988)]. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Brasília, DF: Presidência da República, [2022]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/emendas/emc/emc115.htm](https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm). Acesso em: 05 out. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709compilado.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm). Acesso em: 04 out. 2023.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/113853.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm). Acesso em: 04 out. 2023.

BRASIL. Senado Federal. **Projeto de Lei nº 330, de 13 de agosto de 2013**. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Brasília: Senado Federal, 2013. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 04 out. 2023.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 21.538, de 14 de outubro de 2003**. Dispõe sobre o alistamento e serviços eleitorais mediante processamento eletrônico de dados, a regularização de situação de eleitor, a administração e a manutenção do cadastro eleitoral, o sistema de alistamento eleitoral, a revisão do eleitorado e a fiscalização dos partidos políticos, entre outros. Brasília: TSE, 2003. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2003/resolucao-no-21-538-de-14-de-outubro-de-2003>. Acesso em: 07 out. 2023.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.650, de 9 de setembro de 2021**. Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral. Brasília: TSE, 2021. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-650-de-9-de-setembro-de-2021>. Acesso em: 07 out. 2023.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.656, de 7 de outubro de 2021**. Dispõe sobre o acesso a dados pessoais constantes dos sistemas informatizados da Justiça Eleitoral (JE). Brasília: TSE, 2021. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-656-de-7-de-outubro-de-2021>. Acesso em: 07 out. 2023.



BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.659, de 26 de outubro de 2021**. Dispõe sobre a gestão do Cadastro Eleitoral e sobre os serviços eleitorais que lhe são correlatos. Brasília: TSE, 2021. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-659-de-26-de-outubro-de-2021>. Acesso em: 07 out. 2023.

CARVALHO, Hannibal Escobar Ramos Henriques; FREITAG, Alberto Eduardo Besser; SANTOS, Daiane Rodrigues. Impactos da implantação da Lei Geral de proteção de dados pessoais no Brasil: uma análise bibliométrica. **Revista de Gestão e Secretariado**, v. 13, n. 3, p. 1398–1411, 2022. DOI: <https://doi.org/10.7769/gesec.v13i3.1412>. Disponível em: <https://ojs.revistagesec.org.br/secretariado/article/view/1412>. Acesso em: 27 set. 2023.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de dados pessoais comentada**. São Paulo: Revista dos Tribunais, 2019.

CRESWELL, John W. **Projeto de Pesquisa: Métodos Qualitativo, Quantitativo e Misto**. 3ª. ed., Porto Alegre: ARTMED, 2010.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. São Paulo: Revista dos Tribunais, 2019.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2019. DOI: <http://dx.doi.org/10.26668/IndexLawJournals/2358-1352/2019.v23i9.5343>. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/5343>. Acesso em: 03 out. 2023.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Viviane da Silveira. Compliance de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters, 2019, p. 677-713.

GODOY, Arilda Schmidt. Introdução à pesquisa qualitativa e suas possibilidades. **Revista de Administração de Empresas**, v. 35, n. 2, 1995.

GODOY, Arilda Schmidt. Pesquisa Qualitativa: tipos fundamentais. **Revista de Administração de Empresas**, v. 35, n. 3, 1995.

KRÜGER, Cristiane; BALDASSARI, Adriana Cristina Castanho; LOPES, Luis Felipe Dias; SILVA, Lizana Ilha. Lei Geral de Proteção de Dados Pessoais: uma análise dos determinantes junto aos profissionais de Contabilidade. **Revista Catarinense da Ciência Contábil**, v. 20, 19 pp, 2021. DOI: <https://doi.org/10.16930/2237-766220213220>. Disponível em: <https://revista.crcsc.org.br/index.php/CRCSC/article/view/3220>. Acesso em: 30 set. 2023.

MILES, Matthew B.; HUBERMAN, A. Michael. **Qualitative data analysis: An expanded sourcebook**. 2 ed., London: Sage publication, 1994.

NEW DEMOCRACY. **What is a Citizens' Jury?** Walsh Bay: New Democracy Foundation, 2023. Disponível em: <https://www.newdemocracy.com.au/what-is-a-citizens-jury/>. Acesso em: 07 out. 2023.

SELLTIZ, Claire; WRIGHTSMAN, Lawrence Samuel; COOK; Stuart Wellford. **Métodos de pesquisa nas relações sociais**. São Paulo: Herder, 1967.

SORTITION FOUNDATION. **Sortition Resource Guide for Educators**. Cambridge: Sortition Foundation, 2020. Disponível em: [https://d3n8a8pro7vnm.cloudfront.net/sortitionfoundation/pages/675/attachments/original/1607614921/Sortition\\_Foundation\\_Resource\\_Guide\\_for\\_Educators.pdf?1607614921](https://d3n8a8pro7vnm.cloudfront.net/sortitionfoundation/pages/675/attachments/original/1607614921/Sortition_Foundation_Resource_Guide_for_Educators.pdf?1607614921). Acesso em: 23 maio 2022.

UNIÃO EUROPEIA. Regulamento nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril. Bruxelas: **Jornal Oficial da União Europeia**, L 119, 4 de maio de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 04 out. 2023.

# DIREITO PENAL E INTELIGÊNCIA ARTIFICIAL: ANÁLISE SOBRE A NECESSIDADE DE HAVER UMA REGULAMENTAÇÃO PARA GARANTIA DE DIREITOS FUNDAMENTAIS, SOB A ÓTICA DA PROPOSTA DE REGULAMENTO DA UNIÃO EUROPEIA SOBRE INTELIGÊNCIA ARTIFICIAL, DE 21 DE ABRIL DE 2021

ANA CRISTINA CRESTANI<sup>1</sup>

## 1. INTRODUÇÃO

Ao longo dos anos, a sociedade foi se transformando cada vez mais, passando por diversas revoluções industriais até chegar na quarta revolução industrial, conhecida como a revolução da digitalização do mundo. Em um cenário de muita inovação tecnológica, houve um domínio da área de tecnologia no mercado mundial.

Luciano Floridi, utiliza o termo *onlife* para ajudar entender o ambiente em que vivemos. Ele explica que “tornará cada vez mais difícil distinguir entre a vida online e a offline, por isso, a vida na infoesfera<sup>2</sup> não faz mais sentido perguntar se uma pessoa está online ou offline, conectado ou não conectado”.<sup>3</sup>

Como consequência deste cenário, a inteligência artificial vem afetando, cada vez mais, a vida de milhões de pessoas, seja de forma direta ou indireta. É fato que o crescente número da utilização da ia em diversos setores, dentre eles, indústrias, produção agrícola, empresas, bancos e até mesmo operadores

---

1 Mestranda em Direito na área de Ciências Jurídico-Criminais pela Faculdade de Direito da Universidade de Coimbra. Bacharel em Direito pela Universidade Pontifícia Católica de Minas Gerais; Orcid ID 0009-0004-4528-2328; contato do correio eletrônico: anaacristinac@hotmail.com

2 *Infoesfera* nesse contexto, segundo Floridi, é uma atualização do velho termo “ciberespaço”, um termo para ajudar a definir o ambiente em que a sociedade vive, feito de informações, fluxos de dados, interações com softwares e sistemas automáticos, em um misto de analógico e digital.

3 Floridi, L. (s.d.). “Ser humano e inteligência artificial: os próximos desafios do Onlife [Entrevista com Luciano Floridi]”. Instituto Humanitas Unisinos (2020).

do direito), visam obter os benefícios provenientes da ia, como ações voltadas a otimização do tempo para a realização do processo produtivo, porém, junto com os benefícios, a ia possui riscos inerentes, dentre eles a violação dos direitos fundamentais.

O próprio PE, reconhece essa realidade e demonstra essa preocupação, afirmando na sua Resolução de 06 de outubro de 2021<sup>4</sup> que, nos “últimos anos, se verificaram grandes avanços no desenvolvimento da IA, fazendo desta uma das tecnologias estratégicas do século XXI, com potencial para gerar benefícios substanciais em termos de eficiência, precisão e comodidade, trazendo, assim, uma mudança positiva para a sociedade, mas também sérios riscos para os direitos fundamentais e para as democracias alicerçadas no Estado de direito.”<sup>5</sup>

Diante desta situação, a UE, assim como outros países, sentiu a necessidade de entender como funciona os sistemas de ia, quais os impactos que a utilização desses sistemas podem causar, principalmente os impactos referente a violação dos direitos fundamentais, e, em sequência, criar meios para regulamentar o uso da ia, para que a ia seja desenvolvida e utilizada com um viés ético e que sejam respeitados os direitos fundamentais.

Nesse contexto, a Comissão Europeia, em dezembro de 2018 elaborou uma Carta de ética europeia sobre o uso da ia em sistemas judiciais e seu ambiente<sup>6</sup>, para tratar do processamento de decisões e dados judiciais por ia.

Posteriormente, em 08 de abril de 2019, foi publicado pelo GPAN IA (um grupo independente de peritos criado em junho de 2018 pela Comissão Europeia), um guia com orientações éticas para a IA de confiança, defendendo, em síntese, que uma IA de confiança deve ser lícita (legal), ética e sólida (tanto do ponto de vista técnico, quanto do ponto de vista social).<sup>7</sup>

Em sequência, em 19 de fevereiro de 2020, a Comissão Europeia publicou o Livro branco sobre a ia - uma abordagem europeia virada para a excelência e a confiança, sendo que, conforme descrito no documento “a abordagem europeia para a IA visa promover a capacidade de inovação da Europa no domínio da IA, apoiando simultaneamente o desenvolvimento e a adoção de uma IA ética e fiável em toda a economia da UE.”<sup>8</sup>

---

4 European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters

5 European Parliament.(2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI); 3

6 Comissão Europeia para a Eficácia da Justiça (CEPEJ). “Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente”. Dezembro de 2018.

7 Comissão Europeia. Orientações éticas para uma inteligência artificial de confiança. 2019.

8 Comissão Europeia. Livro branco sobre a inteligência artificial - uma abordagem europeia virada para a excelência e a confiança. Bruxelas 2020.

Subsequentemente, em 21 de abril de 2021, foi publicada a proposta de Regulamento do PE e do CE que estabelece regras harmonizadas em matéria de ia e altera determinados atos legislativos da União<sup>9</sup> que será analisada nos tópicos a seguir.

## 2. BREVES NOTAS SOBRE INTELIGÊNCIA ARTIFICIAL

A inteligência artificial pode ser entendida como “a capacidade que uma máquina para reproduzir competências semelhantes às humanas como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade.”<sup>10</sup>

No entanto, um dos problemas encontrados no que concerne aos estudos envolvidos nas áreas de ia, é a dificuldade de definir e conceitua-lá, tendo em vista que há uma tendência de se confundir ia com sistemas complexos de informação.

Apesar das diversas áreas de estudos de ia, esta possui características que são inerentes em qualquer área. Conforme explica Vinicius Padrão e Carlos Souza “ainda que o termo inteligência artificial englobe diversas funcionalidades e uma pluralidade de conceitos, é possível então pontuar algumas características gerais: capacidade de raciocínio por meio da aplicação de regras lógicas a um conjunto de dados disponíveis, reconhecimento de padrões, sejam esses visuais ou comportamentais, e o aprendizado por meio de seus erros e acertos para potencializar a eficácia de suas ações.”<sup>11</sup>

No livro branco, a ia é resumida como um “conjunto de tecnologias que combinam dados, algoritmos e capacidade computacional.”<sup>12</sup>

Para efeitos desse estudo, devemos entender por sistemas de ia conforme definido no art.3º da proposta de regulamento, como sendo “um programa informático desenvolvido com uma ou várias técnicas de abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage.”<sup>13</sup>

---

9 Parlamento Europeu/Conselho. Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da União, 2021.

10 Parlamento Europeu. “O que é a inteligência artificial e como funciona?” (2023)

11 Souza, C.; Padrão, V. IA transformará o Direito, mas o Direito transformará IA?

12 Comissão Europeia. “Livro branco sobre a inteligência artificial - uma abordagem europeia virada para a excelência e a confiança”. Bruxelas 2020.

13 Parlamento Europeu/Conselho. Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da União, 2021.

### 3. INTELIGÊNCIA ARTIFICIAL E DIREITO PENAL

#### 3.1. RELEVÂNCIA DA IA NO DIREITO PENAL

Juliano Maranhão, Juliana Florêncio e Marco Almada, afirmam que “de formas visíveis ou invisíveis, a inteligência artificial já afeta as vidas de milhões de brasileiros, suscitando perguntas a respeito de como o Direito deve lidar com essas novas tecnologias.”<sup>14</sup>

Dessa forma, é inegável que o Direito está intimamente conectado com a sociedade, e que, portanto, deve acompanhar os avanços em todas as áreas que ele sofre intervenção.

Consoante com essa idéia, Rui Ferreira e Marina Pais entendem que essa relação de ia e direito se dá principalmente pelo fato dos “efeitos da Inteligência Artificial fazem e far-se-ão cada vez mais sentir não apenas no cotidiano mas também no Direito, que não pode ficar indiferente à evolução da sociedade em que se insere”<sup>15</sup>.

Serena Quattrocolo afirma que, apesar de “no senso comum ‘direito penal’ e ‘tecnologia’ são considerados, tradicionalmente, termos não conciliáveis”, diante de todas as relações e do cenário no mundo atual, “urge iniciar uma reflexão jurídica sobre os efeitos a curto e longo prazo desta tecnologia, que está a remodelar todos os aspetos da nossa existência social, incluindo a justiça”<sup>16</sup>.

Por consequência, diante do atual cenário que a sociedade como um todo vive, com a ia afetando a vida das pessoas, a privacidade, os direitos fundamentais, surge a necessidade do direito penal intervir.

Apesar do direito penal ser regido pelo princípio da *ultima ratio*, quando bens jurídicos tutelados pelo direito penal são violados, há necessidade do direito penal intervir para a proteção destes direitos. É isso o que ocorre quando há violações de direitos fundamentais pela utilização de sistemas de ia.

Por outro lado, sabe-se que a ia também pode auxiliar questões ligadas ao direito penal, principalmente no âmbito das investigações criminais e nas questões processuais. Entretanto, Rui Ferreira e Marina Pais salientam que, o fato do “direito penal ser uma área particularmente sensível na ciência jurídica e precisamente por isso, é também aquela em que a evolução através das novas tecnologias

---

14 Maranhão, J.; Florêncio, J.; Almada, M. Suprema: Revista de Estudos Constitucionais, vol.1, no.1 (2021).”Artificial intelligence applied to the law and the law of artificial intelligence”, 3

15 Ferreira, R.; Pais, M. “Os desafios da Inteligência Artificial no Direito Penal”, 2

16 Quattrocolo, S. “An introduction to ai and criminal justice in Europe”. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, 1519

tem de ser introduzida com enormes cautelas, com maior cuidado, com melhor critério e profunda e ponderada reflexão.”<sup>17</sup>

Nessa mesma perspectiva, Serena Quattrocolo explica que as mudanças advindas pela sociedade digital no âmbito do direito penal não são somente no que concerne as novas maneiras de ocorrência de crime, mas também, em “como as investigações podem ser conduzidas. Nesse contexto, afirma que “fazer justiça é uma tarefa humana e a súbita mudança digital no estilo de vida dos indivíduos está afetando a maneira como essa tarefa é realizada”<sup>18</sup>.

Dessa forma, a relação entre ia e o direito já é uma realidade. A intenção já não é discutir se devemos ser a favor ou contra essa relação, mas analisar possíveis impactos e a necessidade ou não de se regular. É nesse pensamento que Floridi esclarece que “o facto de a ia estar tendo um grande impacto na sociedade já não é questionável. O debate atual centra-se antes em saber até que ponto será positivo ou negativo, para quem, de que forma, em que locais e a que prazo. E são esses aspectos que o PE, juntamente com o Conselho, buscou esclarecer nas normas previstas na proposta do regulamento.”<sup>19</sup>

### 3.2. *NECESSIDADES E DESAFIOS NA REGULAÇÃO*

Com a ia cada vez mais presente no cotidiano das pessoas, nas empresas e na sociedade em geral, é possível denotar os benefícios que ela traz, como celeridade, contribuição em para a diminuição de problemas climáticos/ambientais como a poluição, auxiliar no combate ao crime e terrorismo, otimizar as operações, melhorar as previsões. Entretanto, a utilização da IA também traz sérios riscos, devido sua opacidade, complexidade, enviesamentos e graus de imprevisibilidade, riscos esses principalmente na violação de direitos fundamentais e proteção de dados.

Floridi e Strait analisam que “nos últimos anos, as empresas de tecnologia e os laboratórios de investigação têm procurado cada vez mais implementar várias formas de análise ética dos seus produtos, serviços e investigação.”<sup>20</sup>

Marcos Soares explica que “as novas tecnologias devem ser vistas não unicamente por uma perspectiva de utilidade individual, é necessário um enfoque que compreenda o seu impacto na vida coletiva”.<sup>21</sup>

---

17 Ferreira, R.; Pais, M. “Os desafios da Inteligência Artificial no Direito Penal”, 3

18 Quattrocolo, S. “An introduction to ai and criminal justice in Europe”. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1522

19 Floridi, L., et al. AI4People: an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds and Machines, v. 28, 2018, 690

20 Floridi, L.; Strait, A.; Ethical foresight analysis: what it is and why it is needed? Minds and Machines, v. 30, n. 1, 2020, 80

21 Soares, M. “Impacto da evolução tecnológica no reconhecimento de novos direitos: proteção dos dados pessoais e uso adequado da inteligência artificial”. Revista de Direito e as Novas Tecnologias. vol. 15. ano 5. São Paulo: Ed. RT, abr.-jun. 2022

Apesar de haver legislações sobre proteção de dados, sobre crimes cibernéticos, sobre direitos fundamentais, é necessário que haja uma regulamentação específica para a IA, pois estas legislações não conseguem abarcar a especificidade e complexidade destes sistemas.

Anabela Rodrigues reforça a necessidade de se regular quando diz que: “novas soluções de IA entraram e começaram a difundir-se nos sistemas de justiça penal sem terem sido pensadas e desenhadas para ser utilizadas neste domínio”.<sup>22</sup>

Destarte, é indispensável que haja um quadro regulatório para , evitar usos maliciosos não obstruir seu progresso e para que as pessoas possam confiar na IA, além de assegurar um desenvolvimento e implementação de uma IA que seja ética e respeite os direitos fundamentais.

A falta de um quadro regulatório eficaz ou até mesmo uma regulamentação inadequada, além de trazer grande insegurança para os utilizadores, pode trazer danos irreparáveis, dificultando o uso da IA.

Diante da certeza de que é necessário haver uma regulamentação no que concerne ao desenvolvimento, inserção no mercado e ao uso da IA, é imprescindível que essa regulamentação tenha uma preocupação acerca da responsabilidade ética, conforme defende Luciano Floridi<sup>23</sup>, filósofo italiano e um dos principais teóricos que tem se dedicado a estudar os desafios éticos relacionados à IA.

Com a necessidade de se regulamentar, surgem inúmeros desafios, como, qual a melhor forma de se regular, como fazer uma regulamentação a nível da UE que tenha o mesmo grau de eficácia em todos os países (considerando aqui que há países com ordenamentos jurídicos diferentes e com aplicação de sistemas de IA de diferentes formas).

Existe também a discussão acerca do dilema que concerne entre haver uma regulamentação para garantir a não violação dos direitos fundamentais, mas de outro lado, essa regulamentação acabar atrapalhando o desenvolvimento dos sistemas de IA.

Nesse viés, “há uma preocupação que uma eventual regulação excessiva possa inibir a inovação por parte das empresas, mas, ao mesmo tempo deixe de prevenir e mitigar danos que possam ser causados pelo uso indevido da IA”<sup>24</sup>.

Karen Almeida, Margareth Zaganelli e Maria Gonçalves, descrevem que “os inúmeros benefícios possíveis trazidos pela IA a diversas atividades e a muitas

---

22 Rodrigues, A. et al. A Inteligência Artificial no Direito Penal. Coimbra: Grupo Almedina, Março de 2022, 12

23 Floridi, L. *Etica dell'intelligenza artificiale: sviluppi, opportunità, sfide*. Milano: Raffaello Cortina Editore, 2022, 68

24 ENAP - Escola Nacional de Administração Pública. (2022). “Regulação da Inteligência Artificial - benchmarking de países selecionados”.

áreas de estudo requerem uma regulamentação que, em primeiro lugar, evite usos maliciosos e, em segundo lugar, não obstrua seu progresso”.<sup>25</sup>

Ressalta-se que, a grande necessidade e preocupação de criar meios regulatórios para a utilização da ia se dá porque os seres humanos devem controlá-la, e não o contrário.

Sob essa perspectiva, o PE, ao redigir a Resolução de 06 de outubro de 2021, considerou que “a IA não deve ser vista como um fim em si, mas como um instrumento ao serviço das pessoas, com o objetivo último de aumentar o bem-estar, as capacidades e a segurança dos seres humanos”.<sup>26</sup>

Nessa ótica, o PE reconhece que “a falta de regulamentação e as diferenças regulamentares que possibilitam ou interditam a utilização de IA para determinadas finalidades”<sup>27</sup>, acaba justificando a diferença no sistema judicial do recurso a aplicações e sistemas integrados de IA.

A nível da UE, um dos principais desafios é conseguir uma abordagem europeia comum da ia para atingir todos os Estados-Membros e evitar a fragmentação do mercado único interno, conforme descrito no livro branco<sup>28</sup>, buscando sempre garantir a segurança jurídica para os operadores que desenvolvem, e também, utilizam os sistema de ia.

## **4. ANÁLISE DA PROPOSTA DE REGULAMENTO DE IA NO ÂMBITO DA UE**

### *4.1. SÍNTESE SOBRE A PROPOSTA*

A presente proposta de Regulamento<sup>29</sup> tem como principal objetivo, conforme disposto na página 3 do documento, garantir a segurança jurídica dos sistemas de ia, para que, eles sejam seguros e respeitem a legislação no que concerne os direitos fundamentais e valores da União, mas, ao mesmo tempo, facilitar os investimentos e a inovação no domínio da ia.

Através da leitura da proposta, é possível perceber que, a UE, além de sentir necessidade de ter um quadro regulatório acerca do assunto, tem total interesse e se empenha, em ser pioneira no desenvolvimento de uma ia que seja

---

25 Almeida, K.; Zaganelli M.; Gonçalves. M.C. “Artificial intelligence: Reflections about emerging regulatory frameworks on its applications – The brazilian case and international trends”. Humanidades e tecnologia (FINOM), vol.26, n.1 (2020).

26 European Parliament.(2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))

27 European Parliament.(2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))

28 Comissão Europeia. “Livro branco sobre a inteligência artificial - uma abordagem europeia virada para a excelência e a confiança”. Bruxelas 2020

29 Parlamento Europeu/Conselho. Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da União, 2021



segura, ética e de confiança, e por isso, tem avançado com pesquisas e projetos de regulamentação.

O próprio livro branco reconhece o interesse da UE em ser precursora de um quadro regulamentar, dispondo que “a Europa pode combinar os seus pontos fortes tecnológicos e industriais com uma infraestrutura digital de elevada qualidade e um quadro regulamentar baseado nos seus valores fundamentais para se tornar um líder mundial na inovação na economia dos dados e nas suas aplicações.”<sup>30</sup>

A proposta de regulamento, “visa padronizar as estratégias regulatórias entre os Estados-Membros visto que a supervisão regulatória autónoma colocaria em risco o ecossistema sinérgico do mercado interno da UE.”<sup>31</sup>

Em suma, a proposta é dividida em 13 títulos, sendo que o título I trata sobre o âmbito e definições, o título II sobre as práticas de ia proibidas, título III sobre os sistemas de ia de risco elevado, título IV sobre as obrigações de transparência aplicáveis a alguns sistemas de ia, título V sobre medidas de apoio à inovação, títulos VI, VII e VIII trata sobre a governação e execução, título IX sobre os códigos de conduta, e, por fim, os títulos X, XI e XII trata das disposições finais.

As normas indicadas pela proposta do Regulamento são baseadas em princípios éticos, como transparência, responsabilidade, privacidade e segurança. Nesse viés, a proposta do Regulamento está intimamente relacionada com a Ética de Luciano Floridi, que, em síntese, é uma ética baseada em quatro pilares: bem-estar, autonomia, justiça e veracidade. Floridi defende que esses pilares devem se aplicar tanto para quem desenvolve os sistemas de IA, quanto para quem os utilizam/são afetados por eles.

Demócrito Filho ressalta a preocupação que o PE e o Conselho da UE tiveram ao redigir a proposta no que concerne ao equilíbrio entre os benefícios e os riscos: “a proposta de regulamento europeu leva em conta esses dois aspectos distintos e aparentemente antagônicos das ferramentas artificialmente inteligentes. Por essa razão, procura encontrar o equilíbrio normativo, para fomentar e promover o desenvolvimento de tecnologias “AI-driven” sem esquecer a necessidade de construir um “human-centric” quadro regulatório”.<sup>32</sup>

Importante ressaltar que a proposta realiza uma hierarquização dos riscos dos sistemas de IA. A proposta considera, em síntese, 03 tipos de sistemas de

---

30 Comissão Europeia. “Livro branco sobre a inteligência artificial - uma abordagem europeia virada para a excelência e a confiança”. Bruxelas 2020

31 ENAP - Escola Nacional de Administração Pública. (2022). “Regulação da Inteligência Artificial - benchmarking de países selecionados”

32 Filho, D. “A proposta regulatória da União Europeia para a inteligência artificial (1ª parte) - a hierarquização dos riscos”. Juristas (2021).

acordo com os riscos que eles podem trazer, principalmente, para os direitos fundamentais, havendo: sistemas proibidos, sistemas de alto risco e sistemas de risco mínimo.

Demócrito Filho explica que “a concepção regulatória baseada nos níveis de riscos dos sistemas de IA tem um caráter de proporcionalidade, no sentido de que as restrições mais graves e exigências mais onerosas somente se aplicam a programas e aplicações que oferecem maiores riscos à segurança e direitos fundamentais das pessoas. Para os demais, são reservadas poucas obrigações de transparência”<sup>33</sup>.

Sendo assim, os sistemas de ia de uso proibido são completamente vedados, em razão do elevado potencial de vulneração de direitos fundamentais. Eles compreendem os seguintes sistemas de ia: sistemas que manipulam o comportamento humano e que seja suscetível/cause danos físicos ou psicológicos; sistemas que explore a vulnerabilidade de um grupo específico, de forma prejudicial associado a idade ou deficiência física/mental; sistemas que são utilizados para efeitos de avaliação ou classificação da credibilidade de pessoas com base no comportamento social ou características de personalidade, conhecido como sistemas de “pontuação social”; e, por último, sistemas de identificação biométrica à distância em tempo real em espaços acessíveis ao público para efeitos de manutenção de ordem pública, sendo que neste, há previsão de algumas exceções, quando for estritamente necessário para cumprir os objetos dispostos no art. 1, ‘d’ da Proposta.

Já os sistemas de risco elevado, compreendem os sistemas elencados em uma lista no anexo III, podendo essa lista ser alargada, e possuem como principais requisitos a obrigação de documentação, rastreabilidade, transparência, supervisão humana, exatidão, solidez e cibersegurança para mitigar consequências danosas aos usuários. A título de exemplo, no âmbito da manutenção de ordem pública, são considerados de risco elevado os sistemas de IA concebidos para serem utilizados por autoridades policiais como polígrafos e instrumentos similares ou para detetar o estado emocional de uma pessoa singular.

Para os sistemas de risco mínimo, são propostas obrigações de transparência mínimas, permitindo que os indivíduos que interagem com o conteúdo tomem decisões informadas e tenham a opção de continuar ou parar de usar a aplicação.<sup>34</sup>

---

33 Filho, D. “A proposta regulatória da União Europeia para a inteligência artificial (1ª parte) - a hierarquização dos riscos”. *Juristas* (2021).

34 ENAP - Escola Nacional de Administração Pública. (2022). “Regulação da Inteligência Artificial - benchmarking de países selecionados”.

Por fim, caso as regras estipuladas não forem seguidas, a proposta prevê sanções que vão de 10 milhões de euros ou 2% do volume de negócios anual global do exercício anterior até 30 milhões de euros ou 6% do volume de negócios anual global do ano financeiro anterior.

#### *4.2. PRINCIPAIS ASPECTOS NO ÂMBITO DO DIREITO PENAL*

Os principais pontos tratados pela proposta que se refere a proteção dos direitos fundamentais e proteção de dados – no âmbito do direito penal, é a identificação das categorias dos sistemas de IA, fazendo assim uma análise de quais sistemas e o quão prováveis (de acordo com uma análise de riscos) eles podem violar direitos fundamentais e a proteção de dados, e, após a identificação da categoria, a proposta estabelece requisitos legais (como transparência, supervisão humana, exatidão, segurança, solidez) que devem ser cumpridos desde o desenvolvimento até a implementação, e, pós-implementação no mercado.

Dessa forma, o âmbito principal da proposta concerne a estabelecer regras claras e harmonizadas para os sistemas de IA de risco elevado.

O PE ressalta a importância do respeito à garantia dos direitos fundamentais, enfatizando que “os direitos e as liberdades fundamentais consignados na Carta devem ser garantidos ao longo de todo o ciclo de vida da IA e respetivas tecnologias, nomeadamente no momento da conceção, do desenvolvimento, da implantação e utilização, e devem ser tidos em conta no quadro da aplicação da lei em todas as circunstância.”<sup>35</sup>

Além disso, a proposta exige que haja um consentimento por parte dos usuários para que os dados pessoais sejam utilizados, sendo que esse consentimento deve ser explícito e tratar de todos os dados, até mesmo os mais sensíveis.

A proposta também exige que os fornecedores de sistemas de IA<sup>36</sup> adotem medidas técnicas e organizacionais para garantir a segurança de dados pessoais.

O grande problema dos sistemas de ia que interfere nos direitos fundamentais e na proteção de dados é a opacidade, ou seja, a falta de transparência. Dessa forma, a proposta prevê uma série de regras desde o desenvolvimento até a colocação da ia no mercado para que a ia seja transparente e combata a opacidade, estabelecendo regras específicas para fabricantes, distribuidores, fornecedores, importadores e utilizadores dos sistemas de ia.

---

35 European Parliament.(2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))

36 Fornecedores deverão ser entendidos conforme o art.28º da Proposta como sendo: “qualquer distribuidor, importador, utilizador ou outro terceiro que: coloca no mercado um sistema de IA de alto risco sob seu nome/marca, modifica no mercado um sistema de IA de risco elevado já colocado no mercado, introduz uma modificação substancial no sistema de IA de risco elevado”.

Nesse sentido, o PE e o CE, através da proposta de regulamento, demonstrou uma preocupação nos acompanhamentos até mesmo pós comercialização/aplicação dos sistemas.

A título de exemplos, a proposta prevê a proibição de determinados sistemas de IA que viola os direitos fundamentais, como a proibição da utilização de pontuação social, por violar direitos e garantias fundamentais as sociedades democráticas.

Exemplo contrário é o que ocorre no Governo da China, que utiliza um sistema tecnológico para monitoramento digital do comportamento dos cidadãos, o chamado sistema de “crédito social”, permitindo a valorização e avaliação exaustiva das pessoas de acordo com a conduta social e vida cotidiana, atribuindo pontuação que gera uma espécie de ranking entre os chineses, conforme explica Demócrito Filho.<sup>37</sup>

A proposta também proíbe sistemas de identificação biométrica à distância em tempo real, com algumas exceções (a) busca de vítimas de crimes e crianças desaparecidas; b) reprimir uma ameaça séria e iminente à vida ou integridade física de uma pessoa ou para prevenir ataques terroristas; ou c) localizar indivíduos que tenham praticado crimes graves - ainda precisam cumprir uma série de requisitos.

Há também, no nível da proposta, uma exigência de consentimento dos usuários para utilização de dados pessoais, consentimento este que deve ser explícito e tratar de todos os dados, até mesmo os mais sensíveis.

Ness viés, Juliano Maranhão, Juliana Florêncio e Marco Almada, explicam que “um dos principais focos de atenção para o Direito está na coleta e tratamento de dados pessoais para perfilamento, sendo entendido como, qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com desempenho profissional, situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocções.”<sup>38</sup>

Matthias Risse, esclarece que “os algoritmos podem fazer qualquer coisa que possa ser codificada, desde que tenham acesso aos dados de que precisam, na velocidade exigida, e sejam colocados em um quadro de projeto que permita a execução das tarefas assim determinadas. Em todos esses domínios, o progresso

---

37 Filho, D. “A proposta regulatória da União Europeia para a inteligência artificial (2ª parte) - a hierarquização dos riscos”. *Juristas* (2021).

38 Maranhão, J.; Florêncio, J.; Almada, M. *Suprema: Revista de Estudos Constitucionais*, vol.1, no.1 (2021). “Artificial intelligence applied to the law and the law of artificial intelligence”, 5

tem sido enorme. A eficiência dos algoritmos é cada vez mais aprimorada através do Big Data: a disponibilidade de uma enorme quantidade de dados sobre toda a atividade humana e outros processos no mundo que permitem que um tipo particular de IA conhecido como “aprendizado de máquina” (machine learning) faça inferências sobre o que acontecerá com base na detecção de padrões.”<sup>39</sup>

Os sistemas de ia devem ser desenvolvidos e utilizados, como bem esclarece o PE, de forma antropocêntrica, no sentido de ser “digno de confiança pública e estar sempre ao serviço dos seres humanos.”<sup>40</sup>

Nesse viés, o PE esclarece que os “sistemas de ia devem ser concebidos para proteção e benefício de todos os membros da sociedade (tendo, nomeadamente, em conta as populações vulneráveis e marginalizadas na sua conceção), ser não discriminatórios e seguros, e que as suas decisões devem ser explicáveis e transparentes, respeitar a autonomia humana e os direitos fundamentais.”<sup>41</sup>

A carta europeia reforça a necessidade de garantia dos direitos humanos previstos no Estado de direito, prescrevendo que “Longe de ser um simples instrumento para melhorar a eficiência dos sistemas judiciais, a ia deve reforçar as garantias do Estado de direito, bem como a qualidade da justiça pública”<sup>42</sup>.

Ademais, a proposta prevê a criação de um novo órgão de supervisão, o Comitê Europeu de ia, sendo que este terá como principal objetivo monitorar a aplicação da regulamentação e tomar as devidas medidas em caso de violações<sup>43</sup>. Este órgão tem como principal função fiscalizar e vigiar o mercado a nível nacional e a nível da UE acerca do cumprimento das regras previstas no regulamento.

#### *4.3. IMPACTOS MAIS RELEVANTES DA PROPOSTA*

Caso a proposta de Regulamento seja aprovada, é necessário que se cumpra todos os pontos propostos, para que seja realmente eficaz e proteja os direitos fundamentais. O impedimento de sistemas de IA de uso proibido, as exigências para os sistemas de IA de risco elevado e os requisitos de transparência para os sistemas de IA de risco mínimo, garantem, em mínimo, se for aplicado as propostas do regulamento, que haja uma inovação da IA, mas que, ao mesmo tempo, seja respeitado os direitos fundamentais e que a IA tenha um viés ético.

---

39 Risse, M. Direitos Humanos e Inteligência Artificial: Uma Agenda Urgentemente Necessária. Revista Publicum, v. 4, n. 1, 18 jun. 2018, 3

40 European Parliament.(2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))

41 European Parliament.(2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))

42 Comissão Europeia para a Eficácia da Justiça (CEPEJ). “Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente”. Dezembro de 2018.

43 O capítulo I do Título IV da Proposta do Regulamento, a partir do seu artigo 56º, trata sobre o Comitê Europeu para a IA.

De outro lado, há lacunas e alguns desafios que devem ser analisados referente a proposta.

O artigo 5º da Proposta define as práticas de IA proibidas, porém nas definições eles utilizam o termo “danos”: “(...) cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa” (destacado), sendo que o termo “danos” está sujeito à diversas interpretações.

Outro desafio enfrentado diz respeito a complexidade da proposta. Algumas pessoas podem ter dificuldade em entender e implementar em sua totalidade, principalmente pelo fato de algumas exigências serem extremamente técnicas.

Flavio Lobo explica que “no atual estágio do projeto de lei, segundo a MIT Technology Review , há previsões de transparência e prestação de contas que, de acordo com especialistas ouvidos pelo veículo, são na prática inviáveis. É o caso, por exemplo, da aplicação de tecnologias de “redes neurais”, cujos processos de processamento de dados são tão complexos que se torna impossível demonstrar exatamente como certos resultados e conclusões são produzidos”.<sup>44</sup>

Há também, uma possível dificuldade no controle de dados pessoais referente a empresas que desenvolvem e usam os sistemas de ia e que estão localizadas em um espaço diferente da UE.

Outrossim, existe o desafio de que as regras propostas pelo Regulamento atendam a necessidade e realidade dos diversos ordenamentos jurídicos dos Estados-Membros, pois deve se considerar que há países com diversas culturas, que já possuem algum nível de regulamentação sobre o uso de ia, além de que, há países com mais recursos e outros com menos recursos com sistemas de ia. Nesse aspecto, se faz necessário uma cautela para que seja possível uma efetiva harmonização das normas.

Por fim, sabe-se que a ia é dinâmica e então há um novo problema: a dificuldade de atualizar a regulamentação. Como os sistemas de ia estão e estarão em constante desenvolvimento e evolução, dificilmente a regulamentação irá acompanhar essa evolução. Isso pode levar a problemas de adaptação e atualização da regulamentação, tornando-a desatualizada e ineficaz.

## 5. CONCLUSÃO

Diante de todo o exposto, visou-se fazer uma abordagem do que é ia, quais as repercussões entre ia e Direito, aqui especificamente no direito penal, analisar

---

44 Lobo, F. “Lei europeia poderá ser marco global para regulação da inteligência artificial”. IPEA Centro de Pesquisa em Ciência, Tecnologia e Sociedade (2022).

a necessidade e os desafios de se regularizar o tema, promover uma reflexão de como a atuação da ia pode repercutir na tutela dos direitos humanos.

Ademais, foi feita uma análise da Proposta de Regulamento, abordando, em síntese, os principais pontos e os impactos mais relevantes que interferem no direito penal, especificamente nos direitos fundamentais e proteção de dados.

Portanto, conclui-se que é necessário haver uma regulamentação, para que haja um desenvolvimento ético e baseado em princípios básicos, dos sistemas de ia, mas que, haja também o respeito aos direitos fundamentais e proteção de dados.

Apesar de já haver, em diversos ordenamentos jurídicos, leis que regulam sistemas complexos de tecnologia, crimes cibernéticos, protejam direitos fundamentais e tratam da proteção de dados, com o rápido desenvolvimento e inserção no cotidiano da ia, é necessário que haja uma regulamentação específica para o uso da ia, a fim de suprir lacunas e tratar de questões que não foram abordadas nos outros quadros regulatórios.

Desse modo, foi possível verificar que não se deve ignorar a aplicação de sistemas de ia no Direito, mas sim estudar e regulamentar de forma mais específica questões pontuais em que os direitos fundamentais e proteção de dados estejam com maiores chances de serem violados.

Por conseguinte, é imprescindível que haja um equilíbrio para garantir a proteção dos direitos fundamentais e a não violação da proteção de dados e, de outro lado, garantir o desenvolvimento dos sistemas de ia.

## REFERÊNCIAS BIBLIOGRÁFICAS

Almeida, K.; Zaganelli M.; Gonçalves. M.C. “**Artificial intelligence: Reflections about emerging regulatory frameworks on its applications – The brazilian case and international trends**”. Humanidades e tecnologia (FINOM), vol.26, n.1 (2020). Disponível em: [http://revistas.icesp.br/index.php/FINOM\\_Humanidade\\_Tecnologia/article/view/1322/966](http://revistas.icesp.br/index.php/FINOM_Humanidade_Tecnologia/article/view/1322/966)

Floridi, L. et al. **AI4People: an ethical framework for a good AI society: opportunities, risks, principles, and recommendations**. Minds and Machines, v. 28, 2018.

Floridi, L. **Etica dell'intelligenza artificiale: sviluppi, opportunità, sfide**. Milano: Raffaello Cortina Editore, 2022.

Floridi, L.; Strait, A.; **Ethical foresight analysis: what it is and why it is needed?** Minds and Machines, v. 30, n. 1, p. 77-97, 2020.

Maranhão, J.; Florêncio, J.; Almada, M. “**Artificial intelligence applied to the law and the law of artificial intelligence**”. Suprema: Revista de Estudos Constitucionais, vol.1, no.1 (2021). Disponível em: <https://suprema.stf.jus.br/index.php/suprema/article/view/20>

Quattrococo, S. “**An introduction to ai and criminal justice in Europe**”. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1519-1554, set./dez. 2019. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/290>

Risse, M. **Direitos Humanos e Inteligência Artificial: Uma Agenda Urgentemente Necessária**. Revista Publicum, v. 4, n. 1, p. 17-33, 18 jun. 2018. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/publicum/article/view/35098/25126>

Rodrigues, A. et al. **A Inteligência Artificial no Direito Penal**. Coimbra: Grupo Almedina, Março de 2022.

Soares, M. “**Impacto da evolução tecnológica no reconhecimento de novos direitos: proteção dos dados pessoais e uso adequado da inteligência artificial**”. Revista de Direito e as Novas Tecnologias. vol. 15. ano 5. São Paulo: Ed. RT, abr.-jun. 2022.

Sousa, Susana. (2020). **Um direito penal desafiado pelo desenvolvimento tecnológico: alguns exemplos a partir das neurociências e da inteligência artificial**. Revista Da Defensoria Pública Da União, (14), 21-37. Disponível em: <https://doi.org/10.46901/revistadadpu.i14.p21-37>

#### Documentos e instrumentos normativos:

Comissão Europeia. **Livro branco sobre a inteligência artificial - uma abordagem europeia virada para a excelência e a confiança**. Bruxelas 2020. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0065&qid=1637746594462>

Comissão Europeia. **Orientações éticas para uma inteligência artificial de confiança**. 2019. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF>

Comissão Europeia para a Eficácia da Justiça (CEPEJ). **Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente**. Dezembro de 2018. Disponível em: <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>

European Parliament.(2021). **European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)**. Disponível em: [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html)

Parlamento Europeu/Conselho. **Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da União, 2021**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206>.

Parlamento Europeu. “**O que é a inteligência artificial e como funciona?**” (2023). Disponível em: <https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona>

#### Outros

ENAP - Escola Nacional de Administração Pública. (2022). “**Regulação da Inteligência Artificial - benchmarking de países selecionados**”. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/7419/1/2022.12.08%20-%20Regula%3a7%3a3o%20da%20Intelig%3aancia%20Artificial.pdf>

Ferreira, R.; Pais, M. “**Os desafios da Inteligência Artificial no Direito Penal**”. Disponível em: [https://carlospintodeabreu.com/wp-content/uploads/2019/01/inteligencia\\_artificial\\_direito\\_penal.pdf](https://carlospintodeabreu.com/wp-content/uploads/2019/01/inteligencia_artificial_direito_penal.pdf)

Filho, D. “**A proposta regulatória da União Europeia para a inteligência artificial (1ª parte) - a hierarquização dos riscos**”. Juristas (2021). Disponível em: <https://juristas.com.br/2021/05/21/a-proposta-regulatoria-da-uniao-europeia-para-a-inteligencia-artificial-1a-parte-a-hierarquizacao-dos-riscos/>

Filho, D. “**A proposta regulatória da União Europeia para a inteligência artificial (2ª parte) - a hierarquização dos riscos**”. Juristas (2021). Disponível em: <https://juristas.com.br/2021/05/21/a-proposta-regulatoria-da-uniao-europeia-para-a-inteligencia-artificial-2a-parte-a-hierarquizacao-dos-riscos/>

Floridi, L. (s.d.). “**Ser humano e inteligência artificial: os próximos desafios do Onlife [Entrevista com Luciano Floridi]**”. Instituto Humanitas Unisinos (2020). Disponível em: <https://www.ihu.unisinos.br/categorias/604136-ser-humano-e-inteligencia-artificial-os-proximos-desafios-do-onlife-entrevista-com-luciano-floridi>



Lobo, F. **“Lei europeia poderá ser marco global para regulação da inteligência artificial”**. IPEA Centro de Pesquisa em Ciência, Tecnologia e Sociedade (2022). Disponível em: <https://www.ipea.gov.br/cts/pt/central-de-conteudo/noticias/noticias/313-lei-europeia-podera-ser-marco-global-para-regulacao-da-inteligencia-artificial>

Souza, C.; Padrão, V. **IA transformará o Direito, mas o Direito transformará IA?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/ia-transformara-o-direito-mas-o-direito-transformara-ia-26092017>

# INTELIGÊNCIA ARTIFICIAL NOS PROCESSOS JUDICIAIS: ANÁLISE SOBRE A DISCRIMINAÇÃO ALGORÍTMICA

RENATA AKEMI OTAKE<sup>1</sup>

## 1. INTRODUÇÃO

Inovações tecnológicas fazem parte do dia das pessoas, seja por meio dos celulares, ou em suas casas com os assistentes pessoais, como o Google Home, a Siri ou a Alexa, é difícil não se ter uma interação com essas tecnologias, e o mesmo vem acontecendo quando tratamos das Inteligências Artificiais (*Artificial Intelligence* ou IA), estão presentes em todas as áreas, desde a Medicina até a Agronomia, é possível encontrar avanços tecnológicos.

Essas mudanças demonstram-se como disruptivas, e o sistema judiciário vem acompanhando as inovações, buscando um aprimoramento em sua performance, contudo, até o momento as IA se restringem no sistema Brasileiro a seleções e redirecionamentos de processos, para promover agilidade e celeridade processual, para população que busca a proteção judiciária.

Nesse sentido, avaliando a frequente evolução dos sistemas, se chega à questão, as inteligências artificiais podem efetuar sentenças? E caso efetuem, como formulariam essas decisões? São questões que perfazem o sistema, tendo em vista que não é possível interromper os avanços tecnológicos que acontecem diariamente, e a produtividade que a utilização dessas IA trazem.

Com esse intuito, a análise é facilitada com a exemplificação proporcionada pelos Estados Unidos, o qual já utiliza o sistema COMPAS (Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativas), que se compreende com um algoritmo, possuindo o objetivo de calcular as probabilidades que o indivíduo possui para a reincidência.

Desta forma, a um potencial de expansão gigantesco, o qual levanta os questionamentos supracitados e nos remete a esse estudo, para que possamos

---

1 Mestranda do Programa de Pós-Graduação em Fronteiras e Direitos Humanos pela Universidade Federal da Grande Dourados – UFGD. Bacharel em Direito (UNIPAR). Pesquisadora do Grupo de Pesquisa CNPq “Democracia, Constituição e Direitos Humanos-fundamentais”. E-mail: renataakemi97@hotmail.com. Lattes: <http://lattes.cnpq.br/0332803653673456> Orcid: <https://orcid.org/0009-0006-4328-8560>.

levar em consideração questionamentos que nos estimulem ao pensamento das contradições que encontraremos no futuro.

Ademais, como metodologia a pesquisa parte do Método hipotético-dedutivo, o qual, conforme estipula Marina de Andrade Marconi e Eva Maria Lakatos<sup>2</sup>, trata-se pela percepção de uma lacuna nos conhecimentos, através da qual levanta-se uma fórmula hipótese e, pelo processo de inferência dedutiva, se testará a predição da ocorrência dos fenômenos estabelecidos pela hipótese. Quanto aos procedimentos técnicos, parte-se por meio da pesquisa bibliográfica, principalmente por teses, artigos científicos, publicações e livros.

Para o segundo tópico executou-se uma análise das inteligências artificiais, com o intuito de compreender seus conceitos, e avaliar qual a forma utilizada por esses sistemas para que possam efetuar decisões autônomas. Assim como, questiona-se se esses mecanismos poderiam realmente ser substitutos em decisões judiciais.

No terceiro tópico, trata-se da utilização do Sistema COMPAS, e os resultados obtidos através de pesquisas realizadas, no quarto tópico discute-se a existência das discriminações algorítmicas, resultado das análises desses sistemas de inteligência artificial, e por fim, antes das considerações finais, no quinto tópico avalia-se a controle e exclusão nos meios digitais.

## 2. AS INTELIGÊNCIAS ARTIFICIAIS APRENDEM PARA QUE TOMEM DECISÕES?

O Direito está em uma constante evolução, e se utiliza das novas tecnologias para sua atualização, todavia, assim como o Direito se utiliza das inovações, estas também necessitam dele para sua regularização, para o controle do comportamento humano, e de suas relações.

Como bem traz, Brad Smith e Carol Ann Browne<sup>3</sup>:

A percepção humana é a habilidade dos computadores de perceber o que está acontecendo no mundo da forma como os humanos percebem por intermédio da visão e da audição. Por um lado, as máquinas conseguem “ver” o mundo, desde que a câmera foi inventada na década de 1830. Mas sempre era necessário um ser humano para compreender o que estava sendo retratado em uma fotografia. Da mesma forma, as máquinas podem ouvir desde que Thomas Edison inventou o fonógrafo, em 1877. Contudo, nenhuma máquina poderia entender e transcrever com a mesma precisão que um ser humano.

---

2 MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 9. ed. atual São Paulo: Atlas, 2021. Livro digital. ISBN 9788597026580, p. 103.

3 SMITH, Brad; BROWNE, Carol Ann.. **Armas e ferramentas: o futuro e o perigo da era digital**. Rio de Janeiro: Alta Books, 2021. E-book. (1 recurso online). ISBN 9788550817026, p. 56. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9788550817026>. Acesso em: 29 Abr. 2023.

Completando esta explanação, a IA pode ser vista, como um ramo da computação, o qual tem como objetivo a interação multidisciplinar de outras áreas do conhecimento, buscando a reprodução de ações que são tidas como humanos<sup>4</sup>.

Nesse contexto, a anos as IA vem sendo utilizadas nos sistemas judiciários para a organização dos processos, e até mesmo para despachos de mero expediente, o programa estipula as citações, sem que seja necessária a intervenção humana, otimizando a tramitação de processos que não estejam requisitando medidas liminares, a máquina efetua sua atribuição e já estipula o seu primeiro ato com o despacho da citação<sup>5</sup>.

No entanto, ao tratar-se das IA, é necessário compartimentar sua beneficias e os problemas que o uso indiscriminado podem gerar, como dispõe Finger<sup>6</sup>, existe um interesse das mídias não especializadas que nos trazem diversas informações, contudo, por muitas vezes são sensacionalistas, não tratando dos pontos relevantes.

Polêmicas envolvendo as IA não são novidades, já nos anos 1960, Norbert Wiener<sup>7</sup> em sua uma entrevista na revista Science advertia dos riscos: *“It is my thesis that machines can and do transcend some of the limitations of their designers, and that in doing so they may be both effective and dangerous”*.

Para alguns essa ideia demonstra-se muito à frente de seu tempo, contudo, em países como o Estados Unidos essas tecnologias já são utilizadas para a determinação do cumprimento da pena, e em outro como a Estônia, realmente já existe o robô juiz, que efetua decisões em processos com valor abaixo de € 7.000,00 (sete mil euros).

Esses sistemas inteligentes, são feitos a partir da utilização de uma base de conhecimento, na qual replicam a mesma resposta para lidar com situações que consideram idênticas ou parecidas, de certa forma os sistemas partem de padrões que são identificados e reutilizados em outras decisões.

Castilho, *et al.*<sup>8</sup>, estabelece um sistema para a construção desse sistema de aprendizado, o qual se divide em quatro partes:

- 
- 4 HARTMANN PEIXOTO, Fabiano. **Direito e Inteligência Artificial**. Coleção Inteligência Artificial e Jurisdição. Volume 2. DR.IA. Brasília, 2020. <https://orcid.org/0000-0002-6502-9897>. ISBN nº 978-65-00-08585-3, p. 17. Disponível em: [www.dria.unb.br](http://www.dria.unb.br). doi: 10.29327/521174. Acesso em 22 Maio 2023.
  - 5 SOARES, Marcelo Negri; KAUFFMAN, Marcos Eduardo; CHAO, Kuo-Ming. (2020). INTELIGÊNCIA ARTIFICIAL: IMPACTOS NO DIREITO E NA ADVOCACIA. **Direito Público**, 17(93), p. 111. Disponível em: <https://www.portalde-periodicos.idp.edu.br/direitopublico/article/view/3555>. Acesso em: 25 Abr. 2023
  - 6 FINGER, Marcelo. Quando se compra Inteligência Artificial, o que de fato se leva para casa? Além do “oba-oba”. **Inteligência artificial [livro eletrônico]: avanços e tendências** / organizadores Fabio G. Cozman, Guilherme Ary Plonski, Hugo Neri. -- São Paulo : Instituto de Estudos Avançados, 2021. Pag. 98.
  - 7 WIENER, Norberto. **Some Moral and Technical Consequences of Automation**. **Science**, New Series, Vol. 131, No. 3410 (May 6, 1960), pp. 1355-1358. Published by: American Association for the Advancement of Science, p.02.
  - 8 CASTILHO, Richard Eckart; MARGONI, Thomas; LABROPOULOU, Penny; GUREVYCH, Iryna. **A Legal Perspective on Training Models for Natural Language Processing**. In Proceedings of the Eleventh International Conference on Lan-

In general, constructing a model consists of the following steps: (1) corpus compilation, (2) corpus pre-processing, (3) corpus annotation, and (4) training of the model. Depending on the availability of an annotated corpus, one or more of these steps can be skipped. We briefly describe all of these steps here and elaborate on the training step in the main parts of our investigation.

Pode-se observar em síntese que o sistema segue etapas, partindo da compilação de seus dados, processamento, anotação e treinamento. Ou seja, os sistemas das IA apreendem conforme recebem informações que analisam através de seus algoritmos, para que possam replicar em outras situações.

Esse processo, também é conhecido como *Machine Learning*, que seria o aprendizado da máquina por meio da programação, com objetivo de treiná-la para que responda coerentes com as informações e comandos aplicados.

Como transpõe Nilsson<sup>9</sup>, as máquinas aprendem conforme as mudanças das estruturas, programas ou dados, com base nas entradas ou respostas as informações externas, citando como exemplo o desempenho no reconhecimento da fala de uma pessoa, que após receber várias amostras passa a identificá-la e pode-se dizer que a máquina aprendeu.

A autora Cathy O’Neil, em seu livro *Algoritmos de Destruição em Massa* (2020), destaca que a construção dos algoritmos tem como meta modelar a realidade a partir de seus dados, dando respostas ao que seus criadores desejam. Contudo, como a autora pontua, essa programação não se importa com os resultados, as consequências dessa decisão não lhe geram nenhum abalo, e apenas de se dizerem “imparciais”, os algoritmos refletem ideologias.

Nas palavras de Diego Carneiro Costa ao tratar-se das IA<sup>10</sup>:

Assim, para além dos inegáveis ganhos de eficiência para o agente de tratamento de dados, a utopia de que as decisões tomadas através dos algoritmos eliminariam os vieses e a subjetividade do ser humano, aumentando significativamente a precisão de julgamento, foi a grande jogada de marketing das empresas desenvolvedoras dos softwares modernos. Na prática, porém, tem-se verificado que IA e o processo algorítmico não apenas são incapazes de evitar o erro humano derivado de seus preconceitos, como também podem reforçar as discriminações já existentes na sociedade.

Portanto, a preocupação no que se refere ao aprendizado das inteligências artificiais, é a reprodução dos conteúdos a qual está exposta, sem que exista uma análise de cunho ético, as decisões formuladas pelos algoritmos não são perfeitas

---

guage Resources and Evaluation (LREC 2018), Miyazaki, Japan. European Language Resources Association (ELRA), p. 01. Disponível em: <https://aclanthology.org/L18-1202/>. Acesso em: 25 Abr. 2023.

9 NILSSON, Nills J. **Introduction to Machine Learning**. Department of Computer Science, Stanford University, Stanford, 2005, Online. Disponível em: <https://ai.stanford.edu/~nilsson/MLBOOK.pdf>. Acesso em: 27 Abr. 2023.

10 COSTA, Diego Carneiro. **O viés do algoritmo e a discriminação por motivos relacionados á sexualidade**. Dissertação Mestrado em Direito, Universidade Federal da Bahia, Salvador, 2020, p.85.

e podem apresentar vícios presentes nos criadores do algoritmo ou por meio dos dados ao qual são exposto para seu aprendizado.

Um exemplo dessas situações, foi o ocorrido no ano de 2015, quando o Google etiquetou uma foto de duas pessoas negras como “gorilas”. O erro foi rapidamente verificado e corrigido pela plataforma, contudo, demonstrou novamente que esses erros, sendo intencionais ou não, podem ocorrer na análise de dados provenientes de algoritmos.

Outro exemplo é o Tay, desenvolvido pela Microsoft, para conversas informais e quanto mais você conversa-se com a IA, mais inteligente ela ficaria, porém, em pouco tempo, Tay passou a receber conteúdos de cunho racista, preconceituosos, e os reproduziu demonstrando que sua fala estava propagando discursos de ódio.

Publicando em seu perfil do Twitter, frases como: “*Nós vamos construir uma muralha, e o México vai pagar por ela.*” e “*O Bush arquitetou o 11/9 e Hitler teria feito um trabalho melhor do que o macaco que temos agora. Donald Trump é a única esperança que temos*”, referindo-se ao então presidente dos Estados Unidos, Barack Obama. Esse efeito se dá pela forma como os sistemas se baseiam, utilizando-se as informações repassadas, sem que façam distinções éticas sobre o assunto.

Em vista dos argumentos apresentados, pode-se observar que as IA não são neutras, uma vez que necessitam do sistema de aprendizado para tomada de decisões, e esse sistema se baseia na compreensão de determinados dados, para que seus algoritmos reproduzam uma resposta.

### **3. ANÁLISE DE RESULTADOS DO SISTEMA COMPAS (*CORRECTIONAL OFFENDER MANAGEMENT PROFILING FOR ALTERNATIVE SANCTIONS*)**

Dessa forma, ao trazer-se o assunto para a baía do direito, destaca-se estudos como o realizado pela Berkman Klein Center, na Universidade de Harvard<sup>11</sup>, o qual possibilitou a verificação de uma discriminação não intencional das inteligências artificiais, em razão dos algoritmos que seriam criados de forma justa e de acordo com o ordenamento jurídico, ampliarem a discriminação nas decisões e o racismo.

O Sistema COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), utilizado pelos Estados Unidos com base na ideia de que seu uso possibilitaria a redução dos gastos do sistema prisional, reduzindo o nú-

---

11 RASO, Filippo; HILLIGOSS, Hannah; KRISHNAMURTHY, Vivek; BAVITZ, Christopher; KIM, Levin. **Artificial Intelligence & Human Rights: Opportunities & Risks**. Berkman Klein Center, 25 de Setembro de 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstractid=3259344>. Acesso em: 23 de Abr. de 2023.

mero de pessoas encarceradas, mantendo no sistema prisional apenas aqueles de demonstrassem risco a sociedade, através da análise dos dados fornecidos se estabeleceria o regime do cumprimento da pena, com um *score* de pontuação.

Contudo, no uso da IA pode-se observar pelo estudo realizado pela Berkman Klein Center, que sua atuação não trazia eficácia, trazendo imparcialidade em suas decisões, sendo que os infratores afro-americanos foram classificados como de “alto risco”, duas vezes mais do que outras pessoas caucasianas.

Nesta análise, quando comparado as porcentagens, o sistema considerou 45% (quarenta e cinco por cento) dos condenados afro-americano como “alto risco”, e apenas 23% (vinte e três por cento) dos caucasianos em situação semelhante<sup>12</sup>.

Pelos resultados obtidos pela Revista ProPublica<sup>13</sup>, foram examinados dez mil réus criminais no condado de Broward, Flórida e comparados os resultados das avaliações das taxas de reincidência em um período de dois anos. E ao compararmos resultados do sistema COMPAS, evidenciaram que os réus negros tinham 45% mais probabilidade de receber pontuações de risco mais altas do que os réus brancos.

Portanto, novamente evidencia-se uma questão racial que está atingindo aqueles que necessitam do sistema judiciário, desta vez ultrapassando os juízes e se estabelecendo nas decisões formuladas pela IA.

Nas palavras de O’neil<sup>14</sup>, esses sistemas de pontuações estão presentes em diversas áreas e podem ser danosos universalmente, pois podem levar alguém a arranjar empréstimos baratos, bons empregos, e chegando ao caso da redução do tempo de prisão, mas o que deve ser analisado é os danos que esses algoritmos causam a aqueles que não são considerados “sortudos”, a essas pessoas, não restam recursos.

Nessa discussão para a utilização das IA, algumas entidades já se voltam a este estudo, entre elas o IBM (*International Business Machines Corporation*), uma das maiores empresas quando se refere a concepção das inteligências artificiais. Em seu site, a empresa prega a ideia de uma IA explicável, “Ela ajuda a caracterizar a precisão, a imparcialidade, a transparência e os resultados na tomada de decisão

---

12 RASO, Filippo; HILLIGOSS, Hannah; KRISHNAMURTHY, Vivek; BAVITZ, Christopher; KIM, Levin. **Artificial Intelligence & Human Rights: Opportunities & Risks**. Berkman Klein Center, 25 de Setembro de 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstractid=3259344>. Acesso em: 23 de Abr. de 2023.

13 LARSON, Jeff; MATTU, Surya; KICHENER, Lauren; ANGWIN, Julia. **How We Analyzed the COMPAS Recidivism Algorithm**. ProPublica, 2016. Disponível em: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. Acesso em: 29 Abr. 2023.

14 O’NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. 1ª edição. Ed.: Rua do Sabão, São Paulo, 2020, p. 31-32.

*desenvolvida com IA. A IA explicável é crucial para uma organização em gerar confiança e convicção ao colocar modelos de IA em produção.”*

Por mais que a IBM se afirme como explicável, assim como afirma Henrique Alves Pinto<sup>15</sup>, somente na prática pode-se descobrir esse nível de comprometimento, e além, nota-se a solidificação de um discurso objetivo, sem abertura para falhas, considerando o sistema como algo isento de críticas.

Observando o cenário, não se nega a utilidade dos sistemas de IA, como tratado anteriormente, eles possibilitam a otimização do tempo com despachos já programados, organização de informações, entre outras várias funcionalidades. Todavia, não é possível assumir que as IA conseguem efetuar decisões em equivalência a um juiz, e não possuem o discernimento para aplacar as desigualdades de nosso sistema.

Nesse sentido, Jordi Nieva Fenoll<sup>16</sup>, suscita quatro fatores que não podem ser esquecidos: *a) La motivación de la valoración probatoria; b) La resignificación de la fase de admisión y de la impugnación de la valoración de la prueba; c) La aplicación de estándares probatorios; d) En particular, la apreciación de la presunción de inocencia.*

Como exposto por Fenoll, esses fatores não podem ser efetuados pelas IA, e estas não podem atuar em todas as partes, pois são ferramentas de auxílio, no entanto, não possuem a elaboração da motivação, um trabalho que reflita a convicção de um juiz, um caráter eminentemente humano.

#### 4. DISCRIMINAÇÃO ALGORÍTMICA

Até o momento se trabalhou-se a ideia dos algoritmos sendo a ferramenta para que as inteligências artificiais pudessem criar caminhos de uma forma de aprendizagem, mas para adentrar a questão da discriminação algorítmica, é necessária uma contextualização do que eles seriam.

Conceituando, os algoritmos podem ser entendidos com conjunto de instruções, que por meio de formas sequenciais organizadas, determinam como deve ser feito, no entanto, ressalta-se que este conceito depende do uso, pois existem algoritmos que auxiliam na escolha de roupas, para não perder um ônibus, para uma receita, deste modo, a diversos modos de utilização de um algoritmo, já que ele é a fórmula usada para atingir o objetivo de seu programador<sup>17</sup>.

---

15 PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária accountability. *Revista de Informação Legislativa*, v. 57, n. 225, p. 43-60, 2020, p.51.

16 FENOLL, Jordi Nieva. *Inteligencia Artificial y Proceso Judicial*. Editora Marcial Pons: Madrid, 2018. p. 101-115.

17 MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, v. 16, n. 90, 2019, p.03.



Entretanto, neste momento analisasse a discriminação exercida por estes algorítmicos. Segundo Mendes e Mattiuzzo<sup>18</sup>, quando se pensa no conceito da discriminação, a ideia que se vem em mente é de uma certa pessoa, a qual é excluída de um grupo por possuir determinadas características que não são aceites.

Todavia, a análise deste estudo foca-se nos casos de discriminação algorítmica, trata-se do resultado discriminatório devido ao pertencimento a uma determinada categoria, a partir das características apresentadas pelo grupo que o indivíduo pertence, ou seja, nesse caso, o indivíduo é discriminado devido ao pertencimento a um grupo, a um conjunto de pessoas.

A vários exemplos do dia a dia que podem ser utilizados, como seguros automobilísticos, para jovens do sexo masculino, o valor é superior do que para jovens mulheres, aqui a questão do género é levada ao algorítmico para se estabelecer as taxas de acidentes de trânsito, e a partir desses dados efetuar essa diferenciação. E esses raciocínios por mais que estatisticamente consistentes, generalizam as pessoas a um grupo, sem o estudo do indivíduo.

Deste modo, um dos maiores problemas dos algoritmos é a falsa concepção de que eles seriam neutros, que não se vinculariam a decisões de viés discriminatórios como os humanos, e com essa percepção as pessoas passam a confiar plenamente nos resultados de suas análises algorítmicas.

Nesse sentido, as palavras Frank Pasquale e Danielle Keats Cidra<sup>19</sup>, fundamentam a argumentação nos dizeres:

Advocates applaud the removal of human beings and their flaws from the assessment process. Automated systems are claimed to rate all individuals in the same way, thus averting discrimination. But this account is misleading. Because human beings program predictive algorithms, their biases and values are embedded into the software's instructions, known as the source code and predictive algorithms. Scoring systems mine datasets containing inaccurate and biased information provided by people.

Como afirmado pelos autores, comemoram-se como boa notícia a ideia pontuação, aplaudindo a substituição dos seres humanos e suas falhas, para a inclusão de um sistema automatizado que classifica as pessoas sem discriminação, mas essa ideia é enganosa, pois os sistemas que deveriam ser supostamente “sem falhas”, trazem as concepções de seus programadores em seus códigos fontes, além de efetuarem uma avaliação baseada apenas em seus algoritmos.

Não somente pela simplificação apresentada, mas as IA se apresentam em tantas áreas no dia a dia da atual sociedade que para seus indivíduos, a confiança

---

18 MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, v. 16, n. 90, 2019, p.09.

19 CITRON, Danielle. Keats; PASQUALE, Frank. **The scored society: Due process for automated predictions**. *Wash. L. Rev.*, v. 89:1, 2014. p. 4. Disponível em: <https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2/>. Acesso em: 03 de Maio de 2023.

nela passou a ser algo simples, desde a opções de filmes pela Netflix, o melhor caminha a seguir por Apps como Maps e Waze, até o presente momento, no qual passa-se a avaliar a possibilidade da inteligência artificial efetuarem decisões judiciais, em substituições aos juízes humanos, e portanto, necessário trazer a discussão os resultados destas aplicações, e as discriminações que acontecem nos grupos minoritários.

## 5. CONCLUSÃO

No discorrer do artigo, buscou-se a análise dos sistemas de inteligência artificial no judicial, e a incidência da discriminação algorítmica em sua utilização. Levantando-se os seguintes questionamentos: Essas inteligências artificiais podem tomar decisões sem qualquer interferência, e existe a incidência de uma discriminação algorítmica? Como elas poderiam aprender sobre algo para que discorram sobre o assunto? Sua utilização poderia gerar danos?

Com intuito de realizar uma averiguação quanto a incidência de uma discriminação algorítmica, na utilização destes sistemas, trouxe-se a baia o resultado obtido pelo sistema COMPAS, o qual já vem a ser utilizado para o exame de pessoas encarceradas, mantendo no sistema prisional apenas aqueles de demonstrassem risco a sociedade, através da análise dos dados fornecidos se estabeleceria o regime do cumprimento da pena, com um score de pontuação.

Desta forma, respondendo os questionamentos inicialmente levantados, sobre a interferência em decisões efetuadas pela IA, constatou-se que não seria um sistema neutro, a concepção de suas decisões pode apresentar vieses discriminatórios, conforme as informações que foram captados ou repassados no seu aprendizado, pelo *machine learning*.

Esse processo, possibilita que as IA aprendam, e a partir deste aprendizado efetuem decisões as situações a ela apresentadas, contudo, como discutidos, esses processos não são verdadeiramente autônomos, e trazem os vieses, valores, já enraizadas nas informações processadas.

Contudo, observou-se pelos resultados dos estudos realizados que em suas respostas, o sistema apresentava decisões com vieses discriminatórios, o sistema considerou 45% (quarenta e cinco por cento) dos condenados afro-americano como “alto risco”, e apenas 23% (vinte e três por cento) dos caucasianos em situação semelhante<sup>20</sup>. Nesse sentido, o presente estudo buscou a discussão desses resultados, frente a discriminação algorítmica.

---

20 RASO, Filippo; HILLIGOSS, Hannah; KRISHNAMURTHY, Vivek; BAVITZ, Christopher; KIM, Levin. **Artificial Intelligence & Human Rights: Opportunities & Risks**. Berkman Klein Center, 25 de Setembro de 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstractid=3259344>. Acesso em: 23 de Abr. de 2023

Portanto, confirma-se a hipótese levantada, o uso das inteligências artificiais para efetuação de decisões, pode resultar em discriminações algorítmicas que caso não sejam devidamente regulamentadas, resultará nesta incidência. Não olvidando-se que as IA apresentam um grande desenvolvimento para a humanidade, e seu está cada vez mais intrincado a sociedade, no entanto, o estudo de seus resultados é necessário para que não seus avanços não signifiquem um retrocesso aos direitos dos cidadãos.

## REFERÊNCIAS BIBLIOGRÁFICAS

- CASTILHO, Richard Eckart; MARGONI, Thomas; LABROPOULOU, Penny; GUREVYCH, Iryna. **A Legal Perspective on Training Models for Natural Language Processing**. In Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018), Miyazaki, Japan. European Language Resources Association (ELRA), p. 01. Disponível em: <https://aclanthology.org/L18-1202/>. Acesso em: 25 set. 2023.
- CITRON, Danielle. Keats; PASQUALE, Frank. **The scored society: Due process for automated predictions**. Wash. L. Rev., v. 89:1, 2014. p. 4. Disponível em: <https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2/>. Acesso em: 03 de Maio de 2023.
- COSTA, Diego Carneiro. **O viés do algoritmo e a discriminação por motivos relacionados à sexualidade**. Dissertação Mestrado em Direito, Universidade Federal da Bahia, Salvador, 2020, p.85.
- FENOLL, Jordi Nieva. **Inteligencia Artificial y Proceso Judicial**. Editora Marcial Pons: Madrid, 2018. p. 101-115.
- FINGER, Marcelo. Quando se compra Inteligência Artificial, o que de fato se leva para casa? Além do “oba-oba”. **Inteligência artificial [livro eletrônico]: avanços e tendências** / organizadores Fabio G. Cozman, Guilherme Ary Plonski, Hugo Neri. -- São Paulo : Instituto de Estudos Avançados, 2021. Pag. 98.
- HARTMANN PEIXOTO, Fabiano. **Direito e Inteligência Artificial**. Coleção Inteligência Artificial e Jurisdição. Volume 2. DR.IA. Brasília, 2020. <https://orcid.org/0000-0002-6502-9897>. ISBN nº 978-65-00-08585-3, p. 17. Disponível em: [www.dria.unb.br](http://www.dria.unb.br). doi: 10.29327/521174. Acesso em 22 set. 2023.
- LARSON, Jeff; MATTU, Surya; KICHENER, Lauren; ANGWIN, Julia. **How We Analyzed the COMPAS Recidivism Algorithm**. *ProPublica*, 2016. Disponível em: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. Acesso em: 29 set. 2023.
- MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 9. ed. atual São Paulo: Atlas, 2021. Livro digital. ISBN 9788597026580, p. 103.
- MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, v. 16, n. 90, 2019, p.03.
- NILSSON, Nils J. **Introduction to Machine Learning**. Department of Computer Science, Stanford University, Stanford, 2005, Online. Disponível em: <https://ai.stanford.edu/~nilsson/MLBOOK.pdf>. Acesso em: 27 set. 2023.
- O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. 1ª edição. Ed.: Rua do Sabão, São Paulo, 2020, p. 31-32.
- PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária accountability. *Revista de Informação Legislativa*, v. 57, n. 225, p. 43-60, 2020, p.51.
- RASO, Filippo; HILLIGOSS, Hannah; KRISHNAMURTHY, Vivek; BAVITZ, Christopher; KIM, Levin. **Artificial Intelligence & Human Rights: Opportunities & Risks**. *Berkman Klein Center*, 25 de Setembro de 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstractid=3259344>. Acesso em: 23 de set. 2023.

SMITH, Brad; BROWNE, Carol Ann. **Armas e ferramentas: o futuro e o perigo da era digital**. Rio de Janeiro: Alta Books, 2021. E-book. (1 recurso online). ISBN 9788550817026, p. 56. Disponível em: <https://integrada.minhabiblioteca.com.br/bo oks/9788550817026>. Acesso em: 29 set. 2023.

SOARES, Marcelo Negri; KAUFFMAN, Marcos Eduardo; CHAO, Kuo-Ming. (2020). INTELIGÊNCIA ARTIFICIAL: IMPACTOS NO DIREITO E NA ADVOCACIA. **Direito Público**, 17(93), p. 111. Disponível em: <https://www. portaldeperiodicos.idp.e du.br/direitopublico/article/view/3555>. Acesso em: 25 set. 2023.

WIENER, Norberto. **Some Moral and Technical Consequences of Automation**. **Science**, New Series, Vol. 131, No. 3410 (May 6, 1960), pp. 1355-1358. Published by: American Association for the Advancement of Science, p.02.

# GOVERNANÇA DE DADOS, AUDITORIA E DIREITOS FUNDAMENTAIS NO USO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

MARCELO FONSECA SANTOS<sup>1</sup>

## 1. PROBLEMA

O tratamento de dados pessoais – e sua Governança - em sistemas de inteligência artificial pode gerar impactos negativos para os titulares de dados e outros agentes de mercado caso não sejam cuidadosamente analisadas na parte concernente aos riscos desde a concepção, e o famoso *risk-based* approach é o mais utilizado pelos times de privacidade e proteção de dados nas instituições, e ganha novos desafios com ferramentas de aprendizado de máquinas?

Tal problema é relevante porque nem sempre os sistemas de inteligência artificial são auditáveis, transparentes ou capazes de prover explicações significativas de suas decisões (problema da *Black Box*). Situações como negativa de crédito, avaliação de riscos securitários, fraude, perda da autodeterminação informativa - ou diagnósticos incorretos - são exemplos de prejuízos concretos às liberdades individuais dos cidadãos.

Para maximizar as garantias a proteção desses titulares de dados, o relatório de impacto à proteção de dados pode ser uma ferramenta valiosa em um framework de governança dentro de uma instituição (pública ou privada) que tenha como parte de seu *core business* o tratamento de dados para finalidades comerciais ou institucionais.

Entretanto, para mitigar riscos é preciso entender o que está sendo objeto de tratamento desde a concepção de um sistema de Inteligência Artificial.

O presente artigo buscará explorar *frameworks* existentes de governança, e entender como é possível endereçar riscos para os Direitos Constitucionais e Fundamentais – o que poderá violar valores e preceitos Democráticos - à privacidade e proteção de dados no contexto de uma auditoria que pretenda reforçar princípios como explicabilidade, transparência. Essas são as possíveis violações que podem surgir no contexto de tratamento de dados pessoais utilizados por

---

1 Mestrando em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie

(e para) sistema de Inteligência Artificial que aprendem de forma autônoma e decidem.

## 2. HIPÓTESE

A hipótese a ser trabalhada pelos autores no presente artigo é a de que o relatório de impacto à proteção de dados pessoais pode ser uma ferramenta valiosa para analisar e mitigar riscos relacionados à privacidade e proteção de dados, o qual pode ser instrumento de prova em eventual auditoria pela Autoridade Nacional de Proteção de Dados, por parceiros de negócio, ou mesmo em caso de ação judicial.

A documentação pode contribuir para o princípio de *accountability* que obriga os controladores de dados pessoais a demonstrarem as medidas necessárias e o cumprimento de Boas Práticas de Governança de Dados e Compliance, bem como efetivas tomadas de decisão e execução de meios que visem proteger direitos e liberdades individuais (e coletivos) dos titulares de dados pessoais.

No sentido de proteger os Direitos Fundamentais no contexto da Sociedade movida a dados, cujo Constitucionalismo Digital proposto no artigo escrito por Henry L. Moses, *Professor of Law and International Organization*, Columbia Law School, chamado de “**Europe’s Digital Constitution**”.<sup>2</sup>

Mas não é só, o papel da constituição em proteger os indivíduos da interferência do poder público, mas a capacidade das empresas digitais – principalmente plataformas que controlam mídias com vídeos, redes sociais e outras formas de expressão de terceiros para todos que estejam em ambientes virtuais que ameaçam Direitos Fundamentais e Humanos, cuja reação por meio da regulação constitucional e infraconstitucional (regulatória) se faz necessária, não mais deixando aos atores e agentes de mercado simplesmente se auto regularem, mas migrando para o sistema de correção (Estado e Agentes de Mercado) como forma de mitigar riscos.<sup>3</sup>

A pesquisa para elaboração do artigo pretende sugerir meios de mitigação de riscos aos Direitos Constitucionais.

---

2 Verbis: “*escreve: “This constitution engrains Europe’s human-centric, rights-preserving, democracy-enhancing, and redistributive vision for the digital economy into binding law. This vision stands in stark contrast to the United States, which has traditionally placed its faith in markets and tech companies’ self-regulation”* (MOSES, 2023)”, cuja tradução livre dos autores é: “Esta constituição consagra em lei vinculativa a visão antropocêntrica, preservadora de direitos, fortalecedora da democracia e redistributiva da Europa para a economia digital. Esta visão contrasta fortemente com a dos Estados Unidos, que tradicionalmente têm colocado sua fé nos mercados e na auto-regulação das empresas de tecnologia.”

3 De Gregorio, Giovanni. **The rise of digital constitutionalism in the European Union**, publicado no International Journal of Constitutional Law 19 (1), 41-70. Acesso: <https://ssrn.com/abstract=3506692> em 11 de junho de 2.203

Centrado no humano e na sociedade democrática para reforço de legitimação de poder Constitucional e de suas Garantias.

### 3. MARCO TEÓRICO

O primeiro Marco Teórico é Luciano Floridi<sup>4</sup> é o principal expoente no estudo de frameworks relacionados à governança em sistemas de inteligência artificial. É Professor de Filosofia e Ética da Informação do OII na Universidade de Oxford, onde também é Diretor do Laboratório de Ética Digital do Oxford Internet Institute. Cuja obra “*Etica dell’intelligenza artificiale. Sviluppo, opportunità, sfide.*”. A obra trata de ética no uso e aplicação dos sistemas de Inteligência Artificial e sua usabilidade no desenvolvimento dos negócios, comércio, indústrias e sociedade.

O segundo Marco Teórico será o, e o Prof. Frank Pascale<sup>5</sup>, autor do livro: “*Black Box Society*”, cuja obra aborda a questão da ausência de transparência em algoritmos utilizados por agentes de mercado para análises que poderão segregar indivíduos ou tratá-los de forma desigual.

### 4. METODOLOGIA

A pesquisa será fundamentada em análise de artigos científicos e bibliografia, ou seja, metodologia utilizar-se-á o método Hipotético-Dedutivo “o pesquisador elege o conjunto de proposições hipotéticas que acredita serem viáveis como estratégia de abordagem para se aproximar de seu objeto.”<sup>6</sup>

Desse modo, a presente pesquisa pretende fazer uso do método teórico e referencial dogmático (artigos científicos e livros) de abordagem sobre Direito Constitucional, Direitos Fundamentais, Direitos Humanos, Proteção de Dados no contexto brasileiro e Europeu.

### 5. CONCLUSÃO OU RESULTADOS ESPERADOS

Concluiu-se da leitura do material prévio que é um grande desafio de implementação de políticas (privadas e públicas) afirmativas.

---

4 Floridi, Luciano. *Etica dell’intelligenza artificiale. Sviluppo, opportunità, sfide.* Milão-Itália. Raffaello Cortina Editore (3 março 2022). Professor da Universidade de Oxford na Inglaterra.

5 Pasquale, Frank. *The black Box Society. The secret algorithms that control money and information.* Cambridge: Harvard University Press, 2015 – Professor da Brooklyn Law School – New York/USA. Professor da Lwa School of Brooklyn – New York/USA

6 MEZZARROBA, Orides; MONTEIRO, Cláudia S. *Manual de Metodologia da Pesquisa no Direito.* [Digite o Local da Editora]: Editora Saraiva, 2019. *E-book.* ISBN 9788553611560. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553611560/>. Acesso em: 01 mai. 2023. p. 90.

A execução dessas políticas acima tem como objetivo a procura por possíveis de respostas que garantam maior transparência e seu dever de proteção dos cidadãos e /ou grupos de cidadãos.

A governança (de dados e corporativa) e o Compliance são capazes de endereçar e reforçar a proteção de Direitos Fundamentais e Liberdades Individuais relacionados à privacidade e personalidade nas instituições privadas e públicas que têm como objeto da Sociedade da Informação os dados (pessoais, mas também corporativos).

Espera-se com o artigo que sejam propostas medidas para assegurar maior explicabilidade e transparência dos sistemas de IA e suas decisões, pois a robusta documentação para lastrear escolhas éticas, e de design, dos sistemas de Inteligência Artificial e sua constante análise, atualização e monitoramento por comitê especializado pode prover elementos de *accountability*, bem como a produção do Relatório de Auditoria de Algoritmos, em eventual verificação (extrajudicial ou judicial) podem comprovar o respeito à Constituição e da Democracia.

## REFERÊNCIAS BIBLIOGRÁFICAS

ABRUSIO, Juliana e Raiz, Diogo. Privacidade, mercado e cidadania: uma conexão a partir da IA. São Paulo. Revista dos Tribunais. 2022.

BAGNOLI, Vicente. **Direito Econômico e Concorrencial**. São Paulo. Revista dos Tribunais. 2023.

BIONI, Bruno Ricardo. Regulação e Proteção de Dados Pessoais - O Princípio da Accountability. São Paulo. Forense. 2022.

CASTRO, Catarina Sarmiento. **Direito da informática, Privacidade e Dados Pessoais**. Coimbra. Almedina. 2005.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro. Renovar. 2006.

DUBBER, Markus R. PASQUALE, Frank e DAS, Sunit. **The Oxford Handbook os Ethics of AI**. Oxford, UK. Oxford University Press. 2020.

FLORIDI, Luciano. **Etica dell'intelligenza artificiale. Sviluppo, opportunità, sfide**. Milão-Itália. Raffaello Cortina Editore (3 março 2022).

FLORIDI, Luciano and Holweg, Matthias and Taddeo, Mariarosaria and Amaya Silva, Javier and Mökander, Jakob and Wen, Yuni, capAI - **A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act** (March 23, 2022). Available at SSRN: <https://ssrn.com/abstract=4064091> or <http://dx.doi.org/10.2139/ssrn.4064091>

FRAZÃO, Ana e Mulholland, Caitlin. **Inteligência Artificial e Direito – Ética, Regulação e Responsabilidade**. São Paulo. Revista dos Tribunais. 2019.

KLEINBERG, Jon. Sunstein, Cass R., Ludwig, Jens. Sunstein. Discrimination in the Age of Algorithms, 2019. Journal of Legal Analysis, Volume 10, 2018, Pages 113–174, <https://doi.org/10.1093/jla/laz001>. Published: 22 April 2019 – Acesso: <https://academic.oup.com/jla/article/doi/10.1093/jla/laz001/5476086> - Acesso em: 01.05.2023

MAGALHÃES, Guilherme Martins, João Victor Rozatti Longhi, e outros. Comentários à Lei Geral de Proteção de Dados Pessoais: Lei 13.709/2018. São Paulo. Foco. 2022.

LAGE, Fernanda Carvalho. **Manual de Inteligência Artificial**. São Paulo. Juspodivm. 2021.



MEZZAROBA, Orides; MONTEIRO, Cláudia S. Manual de Metodologia da Pesquisa no Direito. Editora Saraiva, 2019. E-book. ISBN 9788553611560. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553611560/>. Acesso em: 01 mai. 2023.

MOREIRA, Adilson José. Tratado de Direito Antidiscriminatório (Volume 1). São Paulo. Contra-Corrente. 2020.

O'NEIL, Cathy. **Algoritmos de Destruição em Massa**. São Paulo. Rua do Sabão. 2021.

PASQUALE, Frank. The black box society. **The secret algorithms that control money and information**. Cambridge: Harvard University Press. New York. 2015.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro. Renovar. 2008

RUSSELL, Stuart e Norvig, Peter. **Inteligência Artificial, Uma Abordagem Moderna**. São Paulo. LTC GEN. 2022.

SAAVEDRA, Giovanni Agostini. **Governança Corporativa, Compliance e Proteção de Dados - volume 1**. São Paulo. Esseni. 2021.

TEFFÉ, Chiara Spadaccini de Tefé. **Dados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas**. São Paulo. Foco. 2023.

inteligência artificial, RECRIAÇÃO DIGITAL E O CASO ELIS REGINA: UMA ANÁLISE À LUZ DO PL 2.338/2023 E DOS DIREITOS DA PERSONALIDADE

# ARTIFICIAL INTELLIGENCE, DIGITAL RECREATION, AND THE ELIS REGINA CASE: AN ANALYSIS IN THE CONTEXT OF BILL 2,338/2023 AND PERSONALITY RIGHTS

RENATA BRAGA KLEVENHUSEN<sup>1</sup>  
ELIEL VITOR DE SOUSA VITÓRIO<sup>2</sup>

## 1. INTRODUÇÃO

A Inteligência Artificial (IA) tem se tornando cada vez mais presente na sociedade, impactando diversos aspectos da vida cotidiana, desde a forma como as pessoas consomem informações até como interagem com a tecnologia. Kissinger, Schmidt e Huttenlocher (2023, p. 11) já externavam que a tecnologia está a mudar o nosso pensamento, o conhecimento, a percepção e a realidade – e ao fazê-lo, está a mudar o curso da história humana<sup>3</sup>. Na indústria do entretenimento, a IA desempenha um papel significativo, expandindo as possibilidades criativas e inovadoras. No entanto, com o rápido avanço da IA, surgem questões éticas complexas e desafios regulatórios que exigem análise aprofundada.

Um caso emblemático que gerou debates intensos no cenário midiático e jurídico brasileiro foi a utilização da IA na recriação digital da cantora Elis Regina, falecida em 1982. Nesse caso, uma versão digitalmente recriada de Elis Regina foi usada em um comercial de televisão para promover um produto, levantando questões éticas e jurídicas sobre o uso da imagem de personalidades falecidas por meio da IA.

Este artigo tem como objetivo analisar o “Caso Elis Regina” como um estudo de caso relevante para explorar as implicações éticas e jurídicas da utili-

---

1 Pós-Doutora pelo IFCS-UFRJ/Universidade de Coimbra/IMS-UERJ. Doutora em Direito pela UFSC. Mestre em Direito Civil pela UERJ. Professora adjunta do Curso de Direito da UFF – Volta Redonda. Coordenadora dos Grupos do Observatório Direito e Tecnologia/UFF – Volta Redonda e do Grupo de Estudos e Pesquisas em Métodos Consensuais de Solução de Conflitos/UFF – Volta Redonda. E-mail: renatabragak@terra.com.br. Currículo Lattes: <http://lattes.cnpq.br/4668232703577152>

2 Graduando em direito pela UFF e membro no Grupo Observatório de Direito e Tecnologia/UFF – Volta Redonda. E-mail: elielvitor@id.uff.br

3 KISSINGER, H. A.; SCHMIDT, E.; HUTTENLOCHER, D. A Era da IA: e o nosso futuro como humanos. Califórnia, EUA: Alta Cult, 15 de junho de 2023.

zação da Inteligência Artificial na recriação de figuras públicas, além de discutir a necessidade de regulamentação específica para essas situações. O texto começa com uma revisão da base teórica da IA e suas aplicações na indústria do entretenimento, contextualizando o cenário atual da tecnologia.

Em seguida, o artigo analisa detalhadamente o caso Elis Regina, descrevendo o comercial de televisão em questão e destacando as reações do público, da indústria e dos juristas diante dessa inovação tecnológica. São abordadas as questões éticas relacionadas à utilização da imagem de personalidades falecidas e feita uma comparação com casos similares em nível internacional.

Posteriormente, o texto entra no contexto regulatório da Inteligência Artificial no Brasil, apresentando um panorama atual das leis e regulamentos pertinentes. São discutidos os desafios legais e éticos específicos relacionados à recriação de personalidades por meio da IA, e argumenta-se a favor da necessidade de regulamentação mais precisa e abrangente para situações como a do “Caso Elis Regina”.

Por fim, o artigo discute as implicações mais amplas do uso da IA na recriação de personalidades para o direito e a sociedade em geral, refletindo sobre o impacto na indústria do entretenimento, nos princípios da liberdade de expressão e nos direitos autorais.

Por meio dessa análise crítica e multidisciplinar, busca-se contribuir para o entendimento das complexas questões legais e éticas que envolvem a utilização da IA na recriação de figuras públicas, bem como para o desenvolvimento de políticas e regulamentações que garantam um uso ético e responsável dessa tecnologia no Brasil.

## **2. FUNDAMENTAÇÃO TEÓRICA**

### *2.1. CONCEITO DE INTELIGÊNCIA ARTIFICIAL*

O conceito de IA é fundamental para contextualizar a tecnologia que está no centro deste estudo. Segundo Russell e Norvig<sup>4</sup>, a IA refere-se ao estudo de agentes racionais capazes de perceber o ambiente que os cerca, raciocinar sobre esse ambiente e tomar ações que maximizem suas chances de alcançar objetivos. Essa definição ressalta a capacidade da IA de simular processos cognitivos humanos, como o aprendizado e a tomada de decisões, por meio de algoritmos e modelos computacionais. A IA abrange uma série de técnicas, incluindo o apren-

---

4 Russell S, Norvig P. Artificial intelligence: a modern approach, Hoboken. USA: Pearson; 2020.

dizado de máquina, redes neurais artificiais e processamento de linguagem natural, que desempenham um papel crucial na recriação digital de personalidades.

O Aprendizado de Máquina permite que os sistemas de IA identifiquem padrões complexos nos dados, habilitando-os a tomar decisões embasadas sem requerer uma programação explícita. Esse aspecto é particularmente relevante na recriação digital de personalidades, onde a captura de nuances comportamentais e estilísticas é essencial. Algoritmos de aprendizado de máquina, como as Redes Neurais Artificiais (RNAs), destacam-se nesse contexto.

As RNAs são modelos computacionais inspirados na estrutura e funcionamento do cérebro humano, compostas por camadas de unidades interconectadas (neurônios artificiais) que processam informações em paralelo. No contexto da recriação de personalidades, as RNAs têm um papel fundamental na análise de características vocais, expressões faciais e comportamentos característicos da personalidade a ser emulada. Através do treinamento com grandes volumes de dados contendo informações sobre a personalidade original, as RNAs capacitam-se para reproduzir essas características com alta precisão.

No contexto da IA, o uso de RNAs e técnicas de aprendizado de máquina se revela imprescindível para a recriação digital de personalidades com alto grau de fidelidade. Essas técnicas possibilitam a modelagem de comportamentos complexos e uma adaptação contínua com base em dados disponíveis, resultando na criação de representações digitais mais autênticas e realistas das personalidades em questão.

Dessa forma, o processo de aprendizado de máquina, especialmente através das RNAs, desempenha um papel crucial na recriação digital de personalidades, permitindo a análise e replicação de características e comportamentos essenciais, como a voz, o estilo de interpretação e a expressão facial.

### **2.1.1. Aplicação da IA na Indústria do Entretenimento**

A Inteligência Artificial (IA) tem desempenhado um papel transformador na indústria do entretenimento, moldando a criação de conteúdo, o entretenimento digital e a interação do público com as mídias. Uma aplicação notável e, ao mesmo tempo, controversa da IA é a tecnologia de Deep Fake, que permite a reconstrução digital de artistas e personalidades em cenários fictícios. Esse fenômeno representa uma fronteira fascinante e desafiadora no mundo do entretenimento, com implicações profundas para a representação visual e a narrativa artística.

### 2.1.2. Reconstrução de Artistas e Personalidades com Deep Fake

O Deep Fake é uma técnica de IA que utiliza redes neurais profundas para criar vídeos e imagens extremamente realistas, nos quais uma pessoa parece estar dizendo ou fazendo algo que nunca aconteceu. Essa tecnologia baseia-se no treinamento de algoritmos com grandes volumes de dados, incluindo imagens e vídeos da personalidade a ser recriada. A IA aprende a replicar minuciosamente traços faciais, movimentos labiais, expressões e até mesmo a voz da pessoa.

Um caso emblemático de aplicação do Deep Fake na indústria do entretenimento ocorreu no filme “Rogue One: Uma História Star Wars” (2016). Neste filme, a tecnologia foi empregada para recriar digitalmente o personagem Grand Moff Tarkin, originalmente interpretado por Peter Cushing, que havia falecido. O resultado foi uma representação virtualmente indistinguível do personagem, que permitiu a continuidade da história e a homenagem ao legado do ator.

No campo da música, o Deep Fake tem sido empregado para criar novas performances de artistas icônicos. Por exemplo, algoritmos de IA foram utilizados para imitar a voz e o estilo musical de Elvis Presley, possibilitando a criação de faixas que parecem autênticas, mas foram geradas digitalmente. Esse uso da tecnologia permite a revitalização da música de artistas do passado, abrindo portas para novas colaborações e experiências musicais.

### 2.1.3. Desenvolvimento da IA na Recriação de Personalidades

A área da Inteligência Artificial (IA) voltada para a recriação de personalidades tem avançado notavelmente, e pesquisadores como Fei-Fei Li, Ian Goodfellow e Kate Crawford têm contribuído significativamente para essa evolução. Kate Crawford, em particular, é reconhecida como uma voz proeminente na ética da IA e tem desempenhado um papel fundamental na conscientização sobre as implicações éticas e sociais da recriação digital de figuras públicas.

Em seu livro “Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence,”<sup>5</sup> publicado em 2021, Crawford apresenta um argumento central sobre a IA como um sistema complexo permeado por questões de poder, política e impactos ambientais. Ela destaca como as decisões relacionadas a algoritmos e modelos de IA frequentemente refletem preconceitos e desigualdades existentes na sociedade, levando a preocupações significativas sobre discriminação algorítmica. Além disso, Crawford ressalta como a corrida pelo avanço da IA tem implicações ambientais substanciais, dada a intensa demanda energética necessá-

---

5 CRAWFORD, K. ATLAS OF AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven, CT: Yale University Press, 2021.

ria para treinar modelos de IA. Seu argumento central enfatiza a importância de uma abordagem crítica para a IA, que considere não apenas seus benefícios, mas também suas implicações sociais, políticas e ambientais. Isso inclui a necessidade de regulamentações e políticas públicas que garantam o desenvolvimento e uso ético, responsável e consciente da IA, não apenas na recriação de personalidades, mas em todas as suas aplicações.

Essa perspectiva crítica de Kate Crawford tem influenciado de forma significativa o debate sobre a ética e a governança da IA moldando a forma como pesquisadores, legisladores e a indústria abordam questões relacionadas à recriação de personalidades e outras aplicações da tecnologia.

## 2.2. RECRIAÇÃO DIGITAL E O CASO ELIS REGINA

O comercial de televisão da montadora de carros Volkswagen apresentou a recriação digital da icônica cantora brasileira Elis Regina por meio da Inteligência Artificial (IA). Nesse anúncio, a IA foi empregada para replicar a imagem e a voz de Elis Regina, permitindo que a cantora dirigisse um modelo da marca, ao lado de sua filha Maria Rita e performando a canção do compositor brasileiro Belchior. A tecnologia avançada utilizada para essa recriação foi capaz de reproduzir detalhes minuciosos da performance e da aparência da artista, buscando capturar sua essência única.

As reações ao comercial foram diversas e abrangentes. Enquanto alguns espectadores expressaram admiração pela habilidade da IA em recriar uma figura tão querida e carismática como Elis Regina, outros levantaram questões críticas em relação à ética envolvida na recriação de uma personalidade falecida. Muitos fãs da cantora foram emocionalmente afetados pela experiência de ver Elis Regina “de volta” em uma apresentação, enquanto outros questionaram se a IA poderia verdadeiramente transmitir a autenticidade e a alma de uma artista tão singular.

A discussão sobre a ética envolvida nesse caso inclui considerações sobre consentimento pós-morte, preservação da identidade e os limites da representação digital de figuras públicas. A ausência de autorização por parte de Elis Regina para a utilização de sua imagem e voz após sua morte levanta questões sobre a integridade da recriação e os direitos de imagem. Além disso, a recriação de personalidades por meio da IA levanta discussões mais amplas sobre o impacto cultural e artístico dessa tecnologia e sobre como ela pode ser usada de maneira responsável e respeitosa.

Em busca de casos semelhantes que possam auxiliar na compreensão dessas questões, é possível explorar outras situações em que a IA foi utilizada para recriar figuras públicas ou históricas, tanto no campo do entretenimento quanto em

outras esferas. Esses casos proporcionam um contexto mais amplo para avaliar as implicações éticas e culturais da recriação de personalidades por meio da IA.

**Figura 1 – Comercial da Marca de carros Volkswagen que recriou digitalmente a cantora Elis Regina, falecida em 1982**



Fonte: Veja (2023)

### *2.3. REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL*

A partir do exemplo mencionado anteriormente e dessa nova realidade, surge a questão sobre qual será o impacto nos direitos da personalidade do indivíduo. Inicialmente, observa-se que há um uso significativo dos direitos relacionados aos dados pessoais, privacidade, imagem e voz, uma vez que o fulcro de tais propaganda midiáticas é justamente o uso da imagem como um todo de personalidades históricas de sucesso.

Mesmo com a existência da Lei Geral de Proteção de Dados, do Marco Civil da Internet e dos projetos de lei que visam regulamentar a inteligência artificial no Brasil, este assunto ainda carece de políticas claras sobre como a imagem e dados daqueles já falecidos serão tratados. Outro aspecto relevante é que a imagem e os direitos autorais para fins de uso comercial tornam-se bens tuteláveis a quem o direito lhe conferir o poder de fazê-lo, o que resulta no uso da personalidade como bem entender o herdeiro, posto a lacuna que há sobre a regulamentação do tema abordado neste artigo.

No Código Civil, observamos a disposição que autoriza os herdeiros a agir em defesa dos Direitos da Personalidade do indivíduo falecido. Entretanto, essa norma carece de especificação quanto à natureza precisa dos direitos protegidos.

Portanto, a projeção da identidade do indivíduo no mundo virtual deve ser acompanhada de uma proteção efetiva dos direitos da personalidade. Como afirma Tepedino e Oliva<sup>6</sup>, a personalidade é considerada um conjunto de características e atributos da pessoa humana, que é objeto de proteção prioritária pelo ordenamento jurídico. Assim, a identidade de uma pessoa não se limita apenas ao seu nome, imagem e voz, mas abrange um conjunto de características, o que demonstra a necessidade de tutela contra possíveis violações de seus direitos personalíssimos. Pietro Perlingieri<sup>7</sup> também destaca que a pessoa se realiza por meio de uma complexidade de situações que podem ser consideradas como poder jurídico, interesse legítimo, direito subjetivo, faculdade e poderes, reforçando a importância de proteger esses aspectos da personalidade no ambiente virtual.

Outro ponto que merece melhor atenção é que não se confunde os direitos autorais, aqueles que incidem sobre as criações produzidas em vida por determinado artista, com os direitos da personalidade, que segundo Caio Mário da Silva Pereira, estão intrinsecamente ligados à própria dignidade da pessoa humana, sendo ainda inalienáveis, irrenunciáveis e imprescritíveis, em outras palavras, não podem ser vendidos, renunciados ou perdidos ao longo do tempo.

Além disso, o jurista também argumentou que os direitos da personalidade abrangem uma ampla gama de aspectos da vida de uma pessoa, incluindo sua integridade física, moral, intelectual e emocional, podendo ser invocados em ações judiciais para proteger a pessoa contra invasões ilegais ou violações por terceiros, enfatizando sua relação intrínseca com a dignidade da pessoa humana.

Neste sentido, alguns telespectadores argumentaram que o uso da imagem da Cantora no comercial era discrepante, posto que, tanto Elis Regina, quanto o compositor Belchior se posicionavam veemente contra o Regime Militar que ocorreu no Brasil entre 1964 a 1984<sup>8</sup>, e, paralelo a isso a montadora alemã atuou como financiadora do regime na época.

A controvérsia central na regulamentação da Inteligência Artificial no contexto da recriação digital de indivíduos falecidos está ancorada na disposição do artigo 6º do Código Civil de 2002. Esse artigo estabelece que a personalidade de um indivíduo tem início com seu nascimento e se encerra com sua morte. No entanto, essa interpretação rígida levanta questões significativas em um cenário em que a sociedade demonstra uma crescente habilidade de recriar digitalmente personalidades após sua morte.

---

6 TEPEDINO, Gustavo. OLIVA, Milena Donato. **Fundamentos do direito civil**: Teoria Geral do Direito Civil. Rio de Janeiro: Forense, 2021.

7 PERLINGIERI, Pietro. Perfis de direito civil: introdução ao direito civil constitucional. Rio de Janeiro: Renovar, 2002. p 155.

8 BASUALDO, Victoria; CAMPOS, Pedro Henrique Pedreira (Orgs.). Ditaduras, empresas e transformações econômicas e trabalhistas na América do Sul durante a Guerra Fria [Dossiê]. Revista Continentes, ano 8, n. 16, jan.-jun. 2020.



Ademais, no que tange sobre os direitos autorais, O dispositivo legal em destaque, o Artigo 5º, inciso XXVII da Constituição Federal de 1988, estabelece que os autores detêm o direito exclusivo de utilizar, publicar e reproduzir suas obras, com a possibilidade de transmitir esses direitos aos herdeiros, pelo período determinado por lei. Nesse contexto, conforme Silva destaca, o direito do autor, também conhecido como direito autoral, compreende um conjunto de normas destinadas a conceder proteção a obras criadas de maneira original, independentemente de sua natureza artística ou intelectual<sup>9</sup>. Essas obras podem ser apresentadas em diversos meios, como livros, revistas, internet, entre outros, e fixadas em suportes tangíveis ou intangíveis, abrangendo qualquer forma de reprodução que possa infringir os direitos dos legítimos autores.

#### 2.4. O PL 2.338/2023

Atualmente o mais promissor das tentativas de regulamentação da IA no Brasil, o projeto de lei em questão tem como objetivo primordial estabelecer direitos e regulamentações relacionados ao uso da Inteligência Artificial (IA) no Brasil. Em sua essência, busca a proteção do indivíduo, que é afetado cotidianamente pelos sistemas de IA em várias esferas, desde recomendações online até avaliações para crédito e políticas públicas. O texto é fruto de outras três propostas sobre o tema :PL 21/2020<sup>10</sup>, PL 5051/19<sup>11</sup> e PL 872/21<sup>12</sup>. De fato, o PL 2338/2023 teve como ponto de partida o relatório concebido por um grupo de juristas que se congregou em 2022. Este comitê identificou a necessidade de introduzir ajustes nos projetos previamente em andamento. A coordenação da Comissão ficou sob a responsabilidade do Ministro Ricardo Villas Bôas Cuevas, do Superior Tribunal de Justiça (STJ).

Paralelamente, visa criar um arcabouço de governança e supervisão que assegure a previsibilidade na interpretação das normas, contribuindo para a segurança jurídica e o desenvolvimento tecnológico. A proposição parte do pressuposto de que não há conflito entre a proteção dos direitos fundamentais e a inovação tecnológica, mas sim uma harmonização desses interesses, em conformidade com a Constituição Federal.

---

9 SILVA, Ricardo Gaiotti. As novas tecnologias e os novos desafios para os direitos autorais. **Conteúdo Jurídico**, Brasília-DF: 09 nov. 2016

10 BRASIL. Câmara dos Deputados. **Projeto de Lei 21/2020, de 04 de fevereiro de 2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Câmara dos Deputados, 2020.

11 BRASIL. Câmara do Deputados. **Projeto de Lei nº 5051, de 2019**. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. 2019. Autoria: Deputado Styvenson Valentim.

12 BRASIL. Câmara dos Deputados. **Projeto de Lei Nº 872, DE 2021**. Dispõe sobre o uso da Inteligência Artificial. 2021. Autoria: Senador Veneziano Vital do Rêgo.

A estrutura do projeto é delineada por princípios gerais que orientam todas as disposições subsequentes. É dedicado um capítulo específico à salvaguarda dos direitos das pessoas afetadas por sistemas de IA, assegurando o acesso à informação, a compreensão das decisões automatizadas, o direito de contestação e intervenção humana, bem como a proibição de discriminação e correção de vieses discriminatórios. Tais direitos são aplicados de forma proporcional aos contextos de risco envolvidos, com maior ênfase em sistemas de alto risco.

O projeto estabelece medidas de governança tanto para sistemas de IA de qualquer grau de risco quanto para sistemas classificados como de alto risco. A categorização de riscos é detalhada, incluindo avaliações preliminares e aplicações vedadas devido a riscos extremos. A responsabilidade civil é abordada de forma diferenciada, com responsabilidade objetiva para sistemas de alto risco e inversão do ônus da prova para outros casos. Também é enfatizada a proteção contra a discriminação, com definições claras e direitos específicos de correção de vieses discriminatórios.

O texto prevê fiscalização por parte do Poder Executivo, com a designação de uma autoridade para supervisionar o cumprimento das normas e a imposição de sanções administrativas. Além disso, incentiva a inovação em IA incluindo um ambiente regulatório experimental (sandbox regulatório). O texto busca conciliar direitos autorais e de propriedade intelectual com a circulação de dados para treinamento de máquinas e desenvolvimento de sistemas de IA, em conformidade com padrões internacionais.

Em suma, o PL propõe uma abordagem abrangente e equilibrada para regulamentar a IA no Brasil, protegendo os direitos individuais, promovendo a inovação e estabelecendo critérios de acordo com o grau de risco. Seu enfoque em direitos, governança e supervisão visa assegurar que a IA seja utilizada de forma ética e responsável, considerando os interesses da sociedade como um todo.

No entanto, a ausência de disposições relacionadas à proteção póstuma da imagem de indivíduos é uma lacuna significativa, considerando a crescente utilização de IA para recriar digitalmente personalidades já falecidas.

Estudiosos contemporâneos, como Kate Crawford, têm enfatizado a importância de considerar a ética e os direitos individuais na aplicação da IA, especialmente quando se trata da recriação de figuras públicas após sua morte.

Somente ao desenvolvermos uma compreensão mais profunda dos sistemas de IA à medida que eles atuam no mundo, podemos garantir que essa nova infraestrutura nunca se torne tóxica. É uma falha de imaginação e metodologia afirmar que é necessário experimentar com milhões de pessoas sem o seu consentimento para produzir uma boa ciência de dados.

A ausência de regulamentação específica sobre esse assunto deixa uma lacuna que pode ser explorada de maneira inadequada, levando a questões éticas e

legais não resolvidas. É fundamental lembrar que a proteção póstuma da imagem de uma pessoa falecida envolve questões de consentimento, dignidade e respeito pelos direitos da personalidade, que merecem atenção adequada.

## *2.5. PROPOSTAS DE TRATAMENTO DO DIREITO À IMAGEM EM RECRIAÇÕES DIGITAIS COM O USO DE INTELIGÊNCIA ARTIFICIAL*

### **2.5.1. Incorporação de Disposições Específicas sobre autorização póstuma no Código Civil Brasileiro**

Incorporar disposições específicas no Código Civil Brasileiro de 2015 que se assemelham às práticas legais da França pode ser uma estratégia promissora para regulamentar o uso da Inteligência Artificial na recriação de figuras públicas póstumas. Inspirado pelo artigo 63 da *Loi pour une République Numérique*<sup>13</sup>, que permite que os usuários determinem diretrizes relativas ao armazenamento, apagamento e comunicação de seus dados pessoais após a morte, o código brasileiro poderia estabelecer mecanismos semelhantes. Essas disposições permitiriam que os usuários definissem claramente as diretrizes relativas à recriação digital de suas imagens após o falecimento, bem como estabelecessem limites sobre o que pode ser feito com seus dados pessoais.

No âmbito das disposições relativas ao gerenciamento de acervos digitais de indivíduos falecidos, é estabelecido que apenas pessoas jurídicas (sejam elas entidades coletivas ou familiares) e terceiros, bem como entidades despersonalizadas que detenham acesso a esses acervos digitais, terão o direito de administrar os ativos digitais que se relacionem com a privacidade do falecido. Este direito é condicionado à manifestação expressa do indivíduo falecido, a qual pode ser realizada por meio de um instrumento público ou particular, incluindo a utilização de campos designados para tal finalidade em plataformas de redes sociais. Essa manifestação pode ocorrer sem a necessidade de testemunhas e também por meio de comportamentos concludentes que evidenciem a vontade do falecido nesse sentido. No caso de conflitos entre herdeiros ou terceiros, é possível utilizar meios de prova admitidos pelo Direito para demonstrar o conteúdo do comportamento concludente.

Em situações em que a declaração expressa ou os comportamentos que indiquem a vontade do falecido não tenham ocorrido, ou estejam afetados por questões como inexistência, anulabilidade, nulidade ou ineficácia, é estabelecido que nenhum acervo digital que represente a personalidade do falecido deverá sofrer alterações, ser acessado ou compartilhado por qualquer pessoa.

---

13 FRANÇA. Assembleia Nacional. *Loi pour une République Numérique*. “Lei para uma República Digital”. 2016.

### **2.5.2. Implementação de um Órgão Regulatório Especializado em IA**

A criação de um órgão regulatório especializado em IA é uma medida crucial para a eficaz regulamentação do uso dessa tecnologia, especialmente na recriação de personalidades históricas. Esse órgão teria a responsabilidade de elaborar diretrizes claras para o uso ético da IA nesse contexto. Para fundamentar essa proposta, é importante examinar experiências internacionais de órgãos regulatórios de IA, como a Comissão Europeia, pioneira no mundo na regulamentação da Inteligência artificial.

### **2.5.3. Criação de um “Fundo de Preservação da Memória”**

Inspirado na prática de estabelecimento de fundos de preservação da memória em outros países, o Brasil poderia criar um “Fundo de Preservação da Memória” financiado por empresas que utilizam a IA para recriações digitais. Este fundo seria dedicado à preservação e promoção da memória de figuras públicas já falecidas. Além disso, o fundo poderia apoiar projetos culturais, educacionais e de preservação histórica relacionados a essas personalidades. Isso garantiria que as recriações digitais não fossem apenas lucrativas, mas também benéficas para a cultura e a história do país, respeitando os direitos da personalidade póstuma.

Essas práticas, baseadas em leis e decisões judiciais de diferentes países, como o “Memorial Fund” da Fundação Elvis Presley, demonstram a importância de garantir que os direitos de testar dos usuários sobre o destino de seus bens digitais sejam respeitados, evitando restrições indevidas impostas unilateralmente por provedores de aplicação. Incorporar essas práticas à regulamentação brasileira da IA é fundamental para equilibrar a inovação tecnológica com a proteção dos direitos da personalidade e da memória das figuras públicas, mesmo após suas mortes.

### **2.5.4. Ênfase na Transparência na Criação de Conteúdo Gerado por IA**

A regulamentação da IA no Brasil deve estabelecer requisitos de transparência na criação de conteúdo gerado por IA. Isso garantiria que os consumidores estejam cientes quando estão interagindo com sistemas automatizados. Para fundamentar essa proposta, é fundamental explorar diretrizes internacionais de proteção ao consumidor, como as orientações da União Europeia sobre IA, que enfatizam a importância da transparência para proteger os direitos dos usuários e promover a confiança no uso da IA.

Nesse contexto, as propostas apresentadas neste capítulo são sólidas e embasadas em práticas legais e regulatórias internacionais, com o objetivo de equi-

librar a inovação tecnológica com a proteção dos direitos da personalidade e da dignidade humana, mesmo após a morte das figuras públicas.

### 3. CONSIDERAÇÕES FINAIS

No contexto da crescente utilização da Inteligência Artificial (IA) para recriar personalidades históricas e figuras públicas, a necessidade de uma regulamentação ética e eficaz torna-se evidente. A rápida evolução tecnológica exige uma abordagem que concilie a inovação com a preservação dos direitos da personalidade e a dignidade humana, mesmo após o falecimento.

Uma proposta consiste na criação de uma agência regulatória especializada em IA, incumbida de monitorar e regular o uso da tecnologia em suas diversas aplicações. Tal agência estabeleceria diretrizes claras para áreas sensíveis, como a recriação de personalidades falecidas. Adicionalmente, poderia ser implementado um sistema de autorização póstuma, no qual herdeiros ou detentores dos direitos de imagem de pessoas falecidas concederiam permissão para a recriação digital dessas personalidades, respeitando, assim, as vontades das famílias, bem como os ideais defendidos pelo falecido em vida e garantindo a integridade da memória das figuras em questão.

Uma vez que, a morte de um indivíduo não deve ser considerada um ponto final absoluto no que tange à proteção de sua personalidade e dos interesses e causas que ele defendia durante sua vida. À medida que a tecnologia avança, a capacidade de recriar figuras públicas falecidas por meio de IA nos força a repensar e revisar concepções tradicionais de personalidade e direitos. A recriação digital de pessoas falecidas apresenta desafios éticos e legais significativos, incluindo a necessidade de preservar o legado, a imagem e os princípios dessas personalidades. Portanto, é imperativo que se reavalie a interpretação do início e fim da personalidade à luz da era digital e da IA, a fim de garantir a continuidade da proteção da personalidade e dos valores defendidos pelas pessoas, mesmo após sua morte.

Outra proposta sugere a criação de um “Fundo de Preservação da Memória”, financiado por empresas que lucram com a IA. Esse fundo seria destinado à preservação e promoção da memória de personalidades falecidas, apoiando projetos culturais, educacionais e de preservação histórica. Além disso, a regulamentação poderia estabelecer requisitos de transparência na criação de conteúdo gerado por IA, garantindo que os consumidores estejam cientes quando estão interagindo com sistemas automatizados.

Portanto, é imperativo que a legislação considere essas preocupações éticas e legais e estabeleça diretrizes claras para o uso da IA na recriação de personalidades, mesmo após suas mortes. Essas diretrizes devem incluir a obtenção de auto-

rização prévia dos herdeiros ou detentores dos direitos de imagem, bem como a definição de limites claros para evitar o uso inadequado ou desrespeitoso da imagem de pessoas já falecidas. A inclusão dessas disposições no projeto de lei contribuiria para uma regulamentação mais completa e ética do uso da IA no Brasil, assegurando a proteção adequada dos direitos individuais mesmo após a morte.

Em suma, o Brasil tem a oportunidade de liderar a busca por uma regulamentação ética da IA, assegurando a proteção dos direitos da personalidade, a dignidade da pessoa humana e a preservação da memória de figuras históricas, bem como daqueles já falecidos. As propostas apresentadas visam a encontrar o equilíbrio entre a inovação tecnológica e o respeito pelos valores éticos e legais que fundamentam nossa sociedade. Esta busca por harmonia pode moldar de forma significativa o futuro da IA no Brasil e servir como um modelo global para o uso responsável e respeitoso da tecnologia.

## REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Câmara do Deputados. **Projeto de Lei nº 5051, de 2019.** Estabelece os princípios para o uso da Inteligência Artificial no Brasil. 2019. Autoria: Deputado Styvenson Valentim. Disponível em: < [https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1679601537015&disposition=inline&\\_gl=1\\*17d-4tyd\\*\\_ga\\*MjUxMTY1ODU4LjE2ODM4Mjk5Mjc.\\*\\_ga\\_CW3ZH25XMK\\*MTY4NDM2NjI3My42LjEuMTY4NDM2NjM1NC4wLjAuMA...](https://legis.senado.leg.br/sdleg-getter/documento?dm=8009064&ts=1679601537015&disposition=inline&_gl=1*17d-4tyd*_ga*MjUxMTY1ODU4LjE2ODM4Mjk5Mjc.*_ga_CW3ZH25XMK*MTY4NDM2NjI3My42LjEuMTY4NDM2NjM1NC4wLjAuMA...) > . Acesso em: 11 nov. 2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei 21/2020, de 04 de fevereiro de 2020.** Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Câmara dos Deputados, 2020. Disponível em: < <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340> > . Acesso em: 15 oct. 2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei Nº 872, DE 2021.** Dispõe sobre o uso da Inteligência Artificial. 2021. Autoria: Senador Veneziano Vital do Rêgo. Disponível em: < [https://legis.senado.leg.br/sdleg-getter/documento?dm=8940096&ts=1679602030034&disposition=inline&\\_gl=1\\*uww20\\*\\_ga\\*MjUxMTY1ODU4LjE2ODM4Mjk5Mjc.\\*\\_ga\\_CW3ZH25XMK\\*MTY4NDM2NjI3My42LjEuMTY4NDM2NjM1NC4wLjAuMA](https://legis.senado.leg.br/sdleg-getter/documento?dm=8940096&ts=1679602030034&disposition=inline&_gl=1*uww20*_ga*MjUxMTY1ODU4LjE2ODM4Mjk5Mjc.*_ga_CW3ZH25XMK*MTY4NDM2NjI3My42LjEuMTY4NDM2NjM1NC4wLjAuMA) > . Acesso em: 10 nov. 2022.

BRASIL. Senado Federal. **Projeto de Lei 2338/2023, de 03 de maio de 2023.** Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. Autoria: Senador Rodrigo Pacheco. Disponível em: < [https://legis.senado.leg.br/sdleg-getter/documento?dm=9347593&ts=1683827933930&disposition=inline&\\_gl=1\\*eriu1\\*\\_ga\\*MjUxMTY1ODU4LjE2ODM4Mjk5Mjc.\\*\\_ga\\_CW3ZH25XMK\\*MTY4NDI0ODg3OC40LjAuMTY4NDI0ODg3OC4wLjAuMA.>](https://legis.senado.leg.br/sdleg-getter/documento?dm=9347593&ts=1683827933930&disposition=inline&_gl=1*eriu1*_ga*MjUxMTY1ODU4LjE2ODM4Mjk5Mjc.*_ga_CW3ZH25XMK*MTY4NDI0ODg3OC40LjAuMTY4NDI0ODg3OC4wLjAuMA.>) . Acesso em: 01 out. 2023.

OSIJEK, Dubrawka. Digital Inheritance – Conference Paper – November 2018. In: [https://www.researchgate.net/publication/329124760\\_Digital\\_inheritance](https://www.researchgate.net/publication/329124760_Digital_inheritance). Acesso em 13 de out de 2023.

PEREIRA, Caio Mário da Silva; TEPEDINO, Gustavo. Responsabilidade Civil. 12. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2018. PERLINGIERI, Pietro. **Perfis do direito civil.** Rio de Janeiro: Renovar, 1999.

SILVA, Ricardo Gaiotti. As novas tecnologias e os novos desafios para os direitos autorais. **Conteúdo Jurídico**, Brasília-DF: 09 nov. 2016. Disponível em: <<http://www.conteudojuridico.com.br/?artigos&ver=2.57017&seo=1>>. Acesso em: 03 de Outubro de 2023.

TEPEDINO, Gustavo. OLIVA, Milena Donato. **Fundamentos do direito civil: Teoria Geral do Direito Civil.** Rio de Janeiro: Forense, 2021.

Transmissibilidade do Acervo Digital de Quem Falece: efeitos dos direitos da personalidade projetados *post mortem*. In: <http://abdconst.com.br/revista20/acervoPablo.pdf>. Acesso em 13 de out de 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6022**: informação e documentação: artigo em publicação periódica técnica e/ou científica: apresentação. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6023**: informação e documentação: referências: elaboração. Rio de Janeiro: ABNT, 2018.

## **AGRADECIMENTOS**

Expressamos nossos sinceros agradecimentos a Deus pela orientação e inspiração que permearam a jornada deste trabalho. É com profundo apreço que agradeço a contribuição da Professora Renata Braga, que, muito enriqueceu este artigo com sua sabedoria e dedicação.

A pesquisa e elaboração deste estudo nos desafiaram e, ao mesmo tempo, reforçaram nossa convicção de que nosso propósito transcende a mera busca pelo conhecimento. Trabalhos como este nos recordam a importância de perseverar firmes no propósito que há em nossos corações e de nunca desistir do sonho de fazer uma diferença significativa no mundo.

À medida que navegamos pelas complexas questões envolvendo a inteligência artificial, ética e direito, mantemos nosso compromisso de contribuir para a sociedade, deixando uma marca relevante. Esta jornada acadêmica é mais do que um caminho pessoal; é um esforço coletivo que, por meio de pesquisas e colaborações, pode moldar positivamente o futuro.



**tirant**  
lo blanch

[editorial.tirant.com/br/](http://editorial.tirant.com/br/)



O Congresso Sociedade Digital e Inteligência Artificial : Desafios da Democracia foi organizado em conjunto pela Faculdade de Direito da Universidade de Coimbra – Portugal e pela Faculdade de Direito da Universidade Presbiteriana Mackenzie – Brasil, por meio de seu curso de Graduação em Direito e Programa de Pós-Graduação em Direito Político e Econômico com apoio das Subseções, Santo Amaro, Tatuapé, Jabaquara e Itaquera da Ordem dos Advogados do Brasil Seção de São Paulo, procura discutir os efeitos para o direito da inteligência artificial na sociedade digital. O principal tema discutido foram os desafios à democracia neste contexto.

Para isso contamos com palestrantes de ambas as Universidades, experts na área, e com a apresentação de trabalhos de pesquisadores nos grupos de trabalho: GT1 Cidadania, democracia e inteligência artificial, GT2 Proteção de dados e democracia, GT3 Economia, democracia e inteligência artificial. Tais grupos se inserem nas investigações dos grupos de pesquisa Laboratório de Direito Digital e Democracia e Estado e Economia no Brasil, ambos registrados no Diretório de Grupos de Pesquisa Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq, do Brasil. Os trabalhos foram submetidos ao sistema duplo cego de avaliação, sendo que 60% dos avaliadores são mulheres. Os trabalhos vieram de Portugal, de Angola e de diversos Estados brasileiros, como São Paulo, Minas Gerais, Mato Grosso do Sul e Sergipe

O evento foi organizado para discutir estes temas a partir de uma perspectiva inclusiva quanto ao gênero, começando pelas comissões organizadoras e científica, paritárias entre homens e mulheres, do mesmo modo que os palestrantes. Também foi paritária a participação de brasileiros e portugueses em todos esses casos.

O tema da democracia foi abordado em diversas dimensões, tanto nas palestras quanto nos trabalhos apresentados, buscando mapear potencialidades e riscos da utilização das novas tecnologias para a efetivação dos direitos fundamentais. Esperamos que os leitores possam tirar proveito desses anais para suas próprias pesquisas.

São Paulo/Coimbra, Janeiro de 2023

Felipe Chiarello de Souza Pinto

Ricardo Libel Waldman

Sandra Passinhas

João Pinto Monteiro

ISBN 978-655908764-8



9

786559

087648

+ ACESSO À VERSÃO DIGITAL GRÁTIS NA NOSSA PLATAFORMA DE LEITURA