

SUMÁRIO

Capítulo 1 – Compreendendo a Inteligência Artificial e a Necessidade de Regulamentação	17
1.1. Introdução	19
1.2. O universo da inteligência artificial	21
I. O conceito	21
II. Os componentes fundamentais da IA	22
III. Principais modelos	22
IV. Aplicações práticas	23
1.3. Viés em modelos, falha ou necessidade?	24
I. A origem do viés: a interação entre dados e algoritmos	24
II. O papel da seleção de conteúdos na amplificação do viés	25
III. O viés como elemento de decisão	25
IV. O viés é necessário	26
1.4. Da necessidade da regulamentação	26
I. Da criação de uma lei brasileira	26
II. O cenário americano	27
III. Do histórico e argumentos para o <i>AI Act</i>	29
IV. Da razão dos riscos	31
V. Dos riscos	31
a) Riscos relacionados à segurança de dados	32
b) Riscos relacionados à privacidade de dados	35
c) Riscos operacionais	38

d) Riscos éticos	40
e) Riscos de transparência	41
f) Propriedade intelectual	42
g) Risco na escolha do fornecedor	43
VI. Das consequências	44
a) Legais	45
b) Reputacionais	45
c) Financeiros	46
Capítulo 2 – AI Act, o Regulamento Europeu	47
2.1. AI Act, entendendo o regulamento	49
2.2. Definição de Inteligência Artificial	50
2.3. Classificação de riscos	51
I. Sistemas de risco inaceitável	51
a) Técnicas de manipulação subliminar	52
b) Exploração de vulnerabilidades	53
c) Classificação social e impactos na personalidade	53
d) Perfilização e avaliação de risco criminal	54
e) Limitação ao reconhecimento facial sem justificativa	55
f) Proibição da análise de emoções no trabalho e na educação	55
g) Categorização biométrica e suas restrições	56
h) Identificação biométrica em tempo real e a proteção da privacidade	57
II. Sistemas de Alto Risco	57
III. Sistemas de risco limitado	61
a) Sistemas de IA que interagem com pessoas	61
b) Geração de conteúdo digital	62
c) Reconhecimento de emoções e categorização biométrica	62
d) Deepfakes e conteúdos sintéticos avançados	63
e) Por que a transparência é essencial?	63
IV. Sistemas de risco mínimo	64

2.4.	Classificação dos operadores.....	65
I.	Provedores	65
II.	Implementadores.....	65
III.	Fabricante de produto	66
IV.	Mandatário	66
V.	Importador.....	67
VI.	Distribuidor	68
Capítulo 3 – Regulamento em Prática.....		69
3.1.	Das principais obrigações para provedores.....	71
I.	Obrigações para qualquer sistema independentemente do risco	71
a)	Transparência com os usuários.....	71
b)	Transparência e educação.....	72
c)	Manutenção de documentação técnica.....	73
d)	Explicações claras.....	75
e)	Colaboração com autoridades.....	75
II.	Obrigações para sistemas de alto risco.....	76
a)	Classificação de risco: o primeiro passo para a confor- midade.....	77
b)	Gestão de risco: garantindo segurança e conformidade contínua.....	79
c)	Governança de dados: a base para a confiabilidade e a equidade em sistemas de IA de alto risco	81
d)	Documentação técnica: o alicerce da conformidade e transparência em sistemas de IA de alto risco	84
e)	Registro de eventos (Logs): a base para transparência e rastreamento contínuo	88
f)	Transparência ampliada.....	89
g)	Supervisão humana: garantindo o controle e a segurança em sistemas de IA	91
h)	Robustez e cibersegurança: protegendo sistemas de IA com eficiência	93
i)	Correção e notificação.....	94

j)	Cooperação com autoridades competentes	96
k)	Marcação CE	97
l)	Registro	98
m)	Monitoramento pós-mercado	99
III.	Obrigações para modelos de uso geral	101
IV.	Modelos de uso geral sem risco sistêmico	102
V.	Modelos de uso geral com risco sistêmico	102
VI.	A necessidade da classificação	103
a)	Documentação técnica	104
b)	Gerenciando riscos sistêmicos	106
c)	Participação em práticas recomendadas	108
VII.	Obrigações para desenvolvedores de fora da UE	109
a)	Conformidade com as regras de segurança e transparência	110
b)	Avaliação e gestão de riscos para sistemas de alto risco	112
c)	Designação de um representante legal	113
3.2.	Das principais obrigações para implementadores	114
I.	Obrigações para qualquer sistema independentemente do risco	115
a)	Transparência e educação em IA	115
b)	Medidas organizacionais	116
II.	Obrigações para sistema de alto risco	117
a)	Medidas organizacionais	117
b)	Supervisão humana	118
c)	Avaliação de impacto	120
3.3.	Das principais obrigações para os adquirentes de IA	121
I.	Aquisição de modelos independentemente do risco	122
a)	Transparência	122
b)	Governança e normas	123
c)	Comunicação e contratos	123
d)	Treinamento e suporte	124
e)	Cibersegurança	124
f)	Explicabilidade	125

II.	Aquisição de modelos de alto risco	127
a)	Certificações e relatórios de conformidade	127
b)	Gestão de riscos	127
c)	Dados utilizados	128
d)	Monitoramento pós-mercado	129
e)	Supervisão humana	130
f)	Análise de impacto	130
3.4.	Regulamentações além do AI/Act	131
I.	Leis de privacidade de dados	131
a)	Decisões automatizadas	132
b)	Base legal	132
II.	Leis de direitos autorais	135
III.	Leis Antitruste	137
IV.	Leis de responsabilidade civil	138
Capítulo 4 –	Governança de Inteligência Artificial	141
4.1.	Governança de Inteligência Artificial	143
4.2.	Da necessidade de governança de IA	143
I.	Mitigação de riscos	144
II.	Construção de confiança	144
III.	Conformidade legal e regulamentar	144
IV.	Promoção da inovação responsável	145
4.3.	Princípios fundamentais da governança de Inteligência Artificial	145
I.	Credibilidade (<i>Trustworthiness</i>)	145
II.	Transparência	146
III.	Responsabilidade	147
IV.	Supervisão humana	147
V.	Equidade	148
VI.	Segurança da informação	149

VII.	Privacidade de dados	149
4.4.	Das frentes impactadas pela governança.....	150
I.	Uso de IA.....	151
II.	Aquisição de modelos.....	152
III.	Desenvolvimento	153
4.5.	Dos principais <i>frameworks</i> de governança de IA.....	154
I.	NIST <i>AI risk management framework</i>	155
a)	Principais características do AI RMF	155
b)	Pilares deste <i>framework</i>	156
c)	Benefícios da implementação do AI RMF	158
d)	Desafios e limitações do AI RMF	159
II.	ISO/IEC 42001:2023	159
a)	Principais características e pilares da ISO/IEC 42001	160
b)	Benefícios da implementação da ISO/IEC 42001	161
III.	ISO/IEC 42001 vs. NIST AI RMF	161
4.6.	Estruturação de um programa de governança de IA	162
I.	Organização.....	162
II.	Diagnóstico	163
a)	Desenvolvimento	164
b)	Aquisição	165
c)	Uso	166
III.	Adequação.....	168
IV.	Melhoria contínua.....	168
	Referências	169