

SUMÁRIO

Introdução.....	37
Preâmbulo.....	45
Parte I – A era da Guerra Informacional.....	47

Capítulo 1

A REVOLUÇÃO DOS DADOS E O NASCIMENTO DO PODER ALGORÍTMICO	49
1.1. DA INFORMAÇÃO AO DADO: A NOVA MATÉRIA-PRIMA DO PODER	49
1.2. DADOS COMO CAPITAL E INSTRUMENTO DE DOMINAÇÃO	50
1.2.1. Capital informacional e concentração de poder	51
1.2.2. O dado como instrumento de governança comportamental.....	51
1.2.3. Colonialismo digital e vulnerabilidade soberana	52
1.2.4. Síntese interpretativa.....	52
1.3. INTELIGÊNCIA ARTIFICIAL E A CONCENTRAÇÃO ALGORÍTMICA DE PODER	53
1.3.1. O ato algorítmico como ato jurídico relevante	53
1.3.2. Governança técnica: validação, drift e explicabilidade.....	54
1.3.3. Responsabilidade institucional e trilhas de auditoria.....	54
1.3.4. Convergência regulatória: prudência, proteção de dados e PLD/FT	54
1.3.5. Síntese interpretativa.....	54
1.4. O SISTEMA FINANCEIRO COMO CAMPO DE BATALHA DA GUERRA INFOR- MACIONAL	55
1.4.1. A coordenação interinstitucional como escudo regulatório.....	56
1.4.2. Síntese interpretativa.....	57
1.5. CONCLUSÃO: O DADO COMO ARMA E A URGÊNCIA DA SOBERANIA INFOR- MACIONAL.....	57

Capítulo 2

A GEOPOLÍTICA DOS DADOS FINANCEIROS.....	59
2.1 BIG TECHS, FINTECHS E O NOVO COLONIALISMO DIGITAL.....	59
2.1.1. Dependência tecnológica e risco de jurisdição	60
2.1.2. Plataformas, interoperabilidade e captura regulatória informacional	60

2.1.3.	Dados como infraestrutura crítica e assimetria de poder	60
2.1.4.	Terceirização crítica, IA e governança de modelos.....	61
2.1.5.	Diretrizes de cibergovernança soberana	61
2.1.6.	Síntese interpretativa.....	62
2.2.	DEPENDÊNCIA TECNOLÓGICA, INFRAESTRUTURAS CRÍTICAS E RISCO DE SOBERANIA ALGORÍTMICA.....	62
2.2.1.	Infraestrutura crítica informacional	62
2.2.2.	Dependência tecnológica e vulnerabilidade soberana	63
2.2.3.	Soberania algorítmica: o novo paradigma de controle estatal.....	63
2.2.4.	Políticas de mitigação e resiliência soberana.....	64
2.2.5.	Síntese interpretativa.....	64
2.3.	INFRAESTRUTURAS CRÍTICAS: DATA CENTERS, APIS E O REAL DIGITAL	65
2.3.1.	Data centers e soberania informacional.....	65
2.3.2.	APIs e o ecossistema de interoperabilidade do open finance.....	66
2.3.3.	O Real Digital e a soberania monetária informacional	66
2.3.4.	Integração normativa e defesa institucional	67
2.3.5.	Síntese interpretativa.....	67
2.4.	O PAPEL DO ESTADO BRASILEIRO NA DEFESA INFORMACIONAL.....	68
2.4.1.	O Banco Central do Brasil e a soberania monetária informacional	68
2.4.2.	O COAF e a inteligência financeira como instrumento de defesa	69
2.4.3.	A CVM, a ANPD e a CGU na governança da informação sensível.....	69
2.4.4.	O GSI e a defesa cibernética como política de Estado.....	70
2.4.5.	O Estado informacional regulador	70
2.4.6.	Síntese interpretativa.....	70
2.5.	SÍNTESE INTERPRETATIVA – GEOPOLÍTICA E AUTONOMIA DOS DADOS	71

Capítulo 3

A GUERRA DOS DADOS NO SISTEMA FINANCEIRO NACIONAL	73
3.1. O SISTEMA BANCÁRIO COMO ALVO: CIBERATAQUES, VAZAMENTOS E SABOTAGEM DIGITAL	73
3.1.1. Tipologia das ameaças informacionais.....	74
3.1.2. Vazamentos de dados e responsabilidade institucional.....	74
3.1.3. Sabotagem digital e manipulação algorítmica	75
3.1.4. Resposta soberana e estrutura de contenção	75
3.1.5. Síntese interpretativa.....	76
3.2. RESPONSABILIDADE DOS BANCOS E FINTECHS NA PROTEÇÃO INFORMACIONAL.....	76
3.2.1. A responsabilidade regulatória: dever de governança e diligência reforçada	76

3.2.2.	A responsabilidade civil e a proteção de dados	77
3.2.3.	A responsabilidade solidária e o papel dos provedores tecnológicos.....	77
3.2.4.	Responsabilidade em incidentes de integridade algorítmica	78
3.2.5.	A integração do SBIF e a <i>accountability</i> soberana	78
3.2.6.	Síntese interpretativa.....	79
3.3.	INTERAÇÃO BACEN–ANPD–GSI–COAF: MODELO DE DEFESA REGULATÓRIA	79
3.3.1.	O Banco Central do Brasil: regulação prudencial e segurança cibernética.....	79
3.3.2.	A ANPD e a proteção de dados sensíveis.....	80
3.3.3.	O GSI e a ciberdefesa de infraestruturas críticas.....	80
3.3.4.	O COAF e a supervisão digital responsiva.....	81
3.3.5.	O modelo de defesa regulatória integrada.....	81
3.3.6.	Síntese interpretativa.....	81
3.4.	ARQUITETURA DE MATURIDADE INSTITUCIONAL E CULTURA DE INTEGRIDADE DIGITAL	82
3.4.1.	Síntese interpretativa.....	83
3.5.	SÍNTESE INTERPRETATIVA – O SISTEMA FINANCEIRO COMO FRONTEIRA ESTRATÉGICA.....	83

Parte II – Ciber governança financeira e integridade digital 85

Capítulo 4

CIBERGOVERNANÇA: DA SEGURANÇA TÉCNICA À INTEGRIDADE INSTITUCIONAL	87
4.1. O CONCEITO JURÍDICO DE CIBERGOVERNANÇA E SUA EVOLUÇÃO NORMATIVA	87
4.1.1. Natureza jurídica da ciber governança	88
4.1.2. A passagem da segurança técnica à integridade institucional.....	88
4.1.3. Ciber governança como instrumento de soberania financeira.....	88
4.1.4. Síntese interpretativa.....	89
4.2. O ESTADO COMO ENTE DE DEFESA DIGITAL	89
4.2.1. Da proteção passiva à defesa informacional ativa.....	90
4.2.2. A função soberana do Estado informacional.....	90
4.2.3. Estrutura institucional da defesa digital brasileira	91
4.2.4. Cooperação público-privada e dever de defesa compartilhada	91
4.2.5. Síntese interpretativa.....	92
4.3. ESTRUTURA BACEN–COAF–CVM–TCU–CGU: O SISTEMA NERVOSO DA GOVERNANÇA	92
4.3.1. O Banco Central do Brasil: o centro regulatório e prudencial	92
4.3.2. O COAF: inteligência financeira e supervisão digital responsiva.....	93

4.3.3.	A CVM e a integridade dos mercados de capitais	93
4.3.4.	O TCU e o controle de integridade das políticas públicas digitais	94
4.3.5.	A CGU e o eixo ético da governança	94
4.3.6.	Integração sistêmica e inteligência de governança	94
4.3.7.	Síntese interpretativa	95
4.4.	A ÉTICA COMO BLINDAGEM INFORMACIONAL	95
4.4.1.	Fundamentos jurídicos da ética digital	95
4.4.2.	Ética como camada de defesa	96
4.4.3.	A cultura de integridade digital	96
4.4.4.	A responsabilidade ética do decisor público e privado	97
4.4.5.	Síntese interpretativa	97
4.5.	SÍNTESE INTERPRETATIVA – O ESTADO COMO ENTE DE DEFESA DIGITAL	97

Capítulo 5

REGULAÇÃO PRUDENCIAL E RESILIÊNCIA CIBERNÉTICA	99
5.1. O RISCO CIBERNÉTICO COMO CATEGORIA PRUDENCIAL	99
5.1.1. A definição jurídica do risco cibernético	99
5.1.2. O enquadramento normativo brasileiro	100
5.1.3. A integração do risco cibernético ao capital regulatório	101
5.1.4. Supervisão baseada em risco e resposta prudencial	101
5.1.5. Síntese interpretativa	102
5.2. REQUISITOS PRUDENCIAIS, SEGURANÇA CIBERNÉTICA E GOVERNANÇA DE RISCOS: ESCOPOS NORMATIVOS APLICÁVEIS	102
5.2.1. Política de segurança cibernética, nuvem e continuidade: normas específicas por escopo	103
5.2.2. Responsabilidade da alta administração e delimitação do escopo da PRSAC	103
5.2.3. Convergência normativa e complementaridade estrutural	103
5.2.4. Mecanismos de conformidade e sanções	104
5.2.5. Síntese interpretativa	104
5.3. SUPERVISÃO INTEGRADA E PROTOCOLOS DE RESPOSTA A INCIDENTES	105
5.3.1. A supervisão integrada: fundamentos e arquitetura	105
5.3.2. O ciclo de resposta regulatória	106
5.3.3. O papel dos órgãos na coordenação de incidentes	106
5.3.4. O dever de defesa informacional	107
5.3.5. Protocolos nacionais e aprendizado sistêmico	107
5.3.6. Síntese interpretativa	107
5.4. FRAMEWORK DE MATURIDADE CIBERNÉTICA INSTITUCIONAL	108
5.4.1. Estrutura conceitual do framework	108

5.4.2.	Níveis de maturidade e critérios de avaliação	109
5.4.3.	Avaliação regulatória de maturidade	109
5.4.4.	A maturidade como instrumento de soberania	109
5.4.5.	Síntese interpretativa.....	110
5.4.6.	Resiliência cibernética e ciclo prudencial do dado	110
5.5.	SÍNTESE INTERPRETATIVA FINAL – A PRUDÊNCIA COMO ESCUDO DA SOBERANIA	110

Capítulo 6

A INTEGRIDADE DOS DADOS FINANCEIROS	113
6.1. O DADO COMO ATIVO JURÍDICO E ELEMENTO DE INTEGRIDADE FINANCEIRA	113
6.1.1. A natureza jurídica do dado financeiro	113
6.1.2. Integridade como princípio regulatório.....	114
6.1.3. A integridade na arquitetura do Sistema Financeiro Nacional.....	114
6.1.4. A integridade como fator de estabilidade sistêmica	115
6.1.5. Síntese interpretativa.....	115
6.2. DUE DILIGENCE DIGITAL E RASTREABILIDADE DE FONTES	116
6.2.1. Fundamentos jurídicos da due diligence digital	116
6.2.2. O ciclo da diligência digital: verificação, rastreamento e certificação.....	116
6.2.3. Due diligence digital e prevenção à lavagem de dinheiro	117
6.2.4. Auditoria digital e responsabilidade institucional	117
6.2.5. Síntese interpretativa.....	118
6.3. O CICLO DA INTEGRIDADE ALGORÍTMICA NO SISTEMA FINANCEIRO NACIONAL.....	118
6.3.1. Conceito e fundamentos da integridade algorítmica	118
6.3.2. Estrutura do ciclo da integridade algorítmica	119
6.3.3. Supervisão e responsabilidade regulatória.....	119
6.3.4. O papel do SBIF e da cooperação interinstitucional.....	120
6.3.5. A dimensão ética e soberana da integridade algorítmica	120
6.3.6. Síntese interpretativa.....	121
6.4. SÍNTESE FINAL – O PAPEL DO CAPÍTULO 6 NA DOCTRINA DA INTEGRIDADE...	121

Capítulo 7

SEGURANÇA INFORMACIONAL E SOBERANIA ECONÔMICA	123
7.1. O DADO FINANCEIRO COMO PATRIMÔNIO ESTRATÉGICO NACIONAL	123
7.1.1. Fundamentos jurídicos da proteção estratégica dos dados financeiros....	123
7.1.2. A lógica estratégica da soberania informacional financeira.....	124
7.1.3. O papel do Estado e das instituições financeiras na defesa informacional.....	124

7.1.4.	Segurança informacional e estabilidade macroeconômica.....	125
7.1.5.	Síntese interpretativa.....	125
7.2.	DEFESA NACIONAL E INFRAESTRUTURA CRÍTICA DO SISTEMA FINANCEIRO	126
7.2.1.	O enquadramento jurídico da infraestrutura crítica financeira.....	126
7.2.2.	O papel das instituições de Estado na ciberdefesa financeira.....	126
7.2.3.	Mecanismos de proteção e resposta.....	127
7.2.4.	Vulnerabilidades e riscos sistêmicos.....	128
7.2.5.	Defesa financeira como pilar da soberania nacional.....	128
7.2.6.	Síntese interpretativa.....	128
7.3.	COOPERAÇÃO INTERNACIONAL E COORDENAÇÃO MULTILATERAL NA DEFESA INFORMACIONAL	129
7.3.1.	A dimensão jurídica da cooperação internacional.....	129
7.3.2.	O papel do COAF e da Rede Egmont.....	130
7.3.3.	A atuação do SBIF e do BACEN em fóruns multilaterais.....	130
7.3.4.	Cooperação tecnológica e inteligência compartilhada.....	131
7.3.5.	A diplomacia de dados e a soberania informacional compartilhada	131
7.3.6.	Síntese interpretativa.....	131
7.4.	SÍNTESE FINAL – DEFESA, ECONOMIA E SOBERANIA.....	132

Capítulo 8

A EXTRATERRITORIALIDADE ALGORÍTMICA.....	133
8.1. A EXPANSÃO DO PODER TECNOLÓGICO E O CONFLITO DE JURISDIÇÕES DIGITAIS	133
8.1.1. A natureza jurídica da extraterritorialidade algorítmica	133
8.1.2. A tensão entre soberania e interoperabilidade.....	134
8.1.3. O impacto da IA estrangeira sobre a regulação financeira nacional	134
8.1.4. O direito emergente da soberania digital	135
8.1.5. Síntese interpretativa.....	135
8.2. RESPONSABILIDADE DE PROVEDORES ESTRANGEIROS E JURISDIÇÃO SOBRE ALGORITMOS EXTERNOS	136
8.2.1. A base legal da responsabilidade extraterritorial.....	136
8.2.2. A doutrina da responsabilidade compartilhada.....	136
8.2.3. A supervisão prudencial da tecnologia importada.....	137
8.2.4. Responsabilidade administrativa e sanções.....	137
8.2.5. A responsabilização indireta e o princípio da soberania derivada.....	138
8.2.6. Síntese interpretativa.....	138
8.3. DISPUTA REGULATÓRIA GLOBAL E O PAPEL DO BRASIL NA GOVERNANÇA DA IA FINANCEIRA	138
8.3.1. O modelo europeu: regulação ética e centralizada	139

8.3.2.	O modelo norte-americano: flexibilidade e inovação controlada	139
8.3.3.	O modelo chinês: controle e soberania tecnológica absoluta	140
8.3.4.	O modelo brasileiro: soberania informacional cooperativa	140
8.3.5.	O papel do Brasil na governança global da IA financeira	141
8.3.6.	A doutrina brasileira de regulação algorítmica soberana	141
8.3.7.	Síntese interpretativa	141
8.4.	MECANISMOS DE MITIGAÇÃO E CONTROLE DA EXTRATERRITORIALIDADE ALGORÍTMICA	142
8.4.1.	Mecanismos jurídicos de mitigação	142
8.4.2.	Mecanismos técnicos de controle e prevenção	143
8.4.3.	Mecanismos cooperativos e diplomáticos	143
8.4.4.	Governança e resposta a incidentes extraterritoriais	143
8.4.5.	A soberania regulatória operacional	144
8.4.6.	Síntese interpretativa	144
8.5.	SÍNTESE CONCLUSIVA: EXTRATERRITORIALIDADE, SOBERANIA E GUERRA DOS DADOS	145

Parte III – Defesa Nacional e regulação internacional 147

Capítulo 9

DIPLOMACIA DE DADOS E REGULAÇÃO GLOBAL	149
9.1. A EMERGÊNCIA DA DIPLOMACIA DE DADOS NO SÉCULO XXI	149
9.1.1. A transição do poder econômico para o poder informacional	150
9.1.2. A diplomacia digital brasileira	150
9.1.3. O conceito de diplomacia de dados	150
9.1.4. O papel do SBIF e da coordenação BACEN–COAF–ANPD–Itamaraty	151
9.1.5. Síntese interpretativa	151
9.2. COOPERAÇÃO MULTILATERAL E O PAPEL DOS ORGANISMOS INTERNACIONAIS NA REGULAÇÃO DA IA FINANCEIRA	152
9.2.1. O GAFI e a governança financeira baseada em risco	152
9.2.2. O papel do Egmont Group e a integração das Unidades de Inteligência Financeira (UIFs)	153
9.2.3. A OCDE e o marco ético da inteligência artificial	153
9.2.4. O BIS e a governança financeira digital	153
9.2.5. A ONU e o regime emergente de cibersegurança internacional	154
9.2.6. Síntese interpretativa	154
9.3. HARMONIZAÇÃO REGULATÓRIA INTERNACIONAL E O PAPEL DO <i>SOFT LAW</i> DIGITAL	154
9.3.1. O que é <i>soft law</i> digital e por que ela vincula na prática	155
9.3.2. Arquitetura internacional de harmonização (mapa funcional)	155

9.3.3.	Método brasileiro de internalização: equivalência, proporcionalidade e SBR	156
9.3.4.	Da <i>guideline</i> ao mandatório: trilha de conformidade prática	156
9.3.5.	Métrica de harmonização: indicadores e evidências	156
9.3.6.	Riscos da harmonização e como mitigá-los	157
9.3.7.	Síntese interpretativa	157
9.4.	PROPOSTA BRASILEIRA DE QUADRO GLOBAL DE CIBERGOVERNANÇA FINANCEIRA	157
9.4.1.	Fundamentos da proposta brasileira	158
9.4.2.	Estrutura institucional sugerida	158
9.4.3.	Cláusulas-modelo do Tratado-Quadro	159
9.4.4.	Papel do Brasil no processo de construção	160
9.4.5.	Benefícios estratégicos e desafios de adesão	160
9.4.6.	Síntese interpretativa	160
9.5.	SÍNTESE CONCLUSIVA: DIPLOMACIA DE DADOS COMO EIXO DA SOBERANIA INFORMACIONAL	161

Parte IV – Modelos, Defesa e Responsabilidade 163

Capítulo 10

INCIDENTES CIBERNÉTICOS E RESPONSABILIDADE REGULATÓRIA	165
10.1. O INCIDENTE CIBERNÉTICO COMO EVENTO JURÍDICO-REGULATÓRIO	165
10.1.1. Tipologia dos incidentes cibernéticos no SFN	166
10.1.2. O dever de reporte e comunicação regulatória	166
10.1.3. Responsabilidade regulatória: conceito e natureza	167
10.1.4. Interação entre BACEN, COAF, ANPD e CVM	167
10.1.5. Síntese interpretativa	168
10.2. TIPOLOGIA JURÍDICA DOS INCIDENTES: INTERNOS, EXTERNOS, ALGORÍTMICOS E HÍBRIDOS	168
10.2.1. Incidentes internos: falhas de governança e negligência operacional	169
10.2.2. Incidentes externos: ataques, invasões e sabotagens digitais	169
10.2.3. Incidentes algorítmicos: falhas de IA e automação decisória	170
10.2.4. Incidentes híbridos: confluência de falhas humanas, técnicas e algorítmicas	171
10.2.5. Síntese interpretativa	171
10.3. PLANOS DE RESPOSTA E MITIGAÇÃO: O MODELO PPRIF (PLANO DE PREVENÇÃO E RESPOSTA A INCIDENTES FINANCEIROS)	172
10.3.1. Estrutura normativa e fundamentos do PPRIF	172
10.3.2. Estrutura funcional do PPRIF	172
10.3.3. Responsabilidades institucionais e fluxos de decisão	173

10.3.4. O ciclo jurídico de resposta: do evento ao restabelecimento	173
10.3.5. Integração entre PPRIF e regulação internacional.....	174
10.3.6. Síntese interpretativa.....	174
10.4. RESPONSABILIDADE E SANÇÕES: GRADAÇÃO, MITIGAÇÃO E RESPOSTA JURÍDICA REGULATÓRIA	175
10.4.1. Estrutura das responsabilidades	175
10.4.2. Gradação das sanções regulatórias	176
10.4.3. Tipologia das sanções aplicáveis	176
10.4.4. Circunstâncias atenuantes e agravantes	177
10.4.5. A dimensão internacional da responsabilidade	177
10.4.6. Síntese interpretativa.....	178
10.5. SÍNTESE CONCLUSIVA: DO INCIDENTE TÉCNICO À RESPONSABILIDADE SOBERANA	178

Capítulo 11

AUDITORIA E CERTIFICAÇÃO DE SOBERANIA DIGITAL	181
11.1 AUDITORIA DIGITAL SOBERANA: FUNDAMENTOS E FINALIDADE JURÍDICA	181
11.1.1. Natureza jurídica e função pública da auditoria.....	182
11.1.2. Tipos de auditoria digital aplicáveis ao Sistema Financeiro Nacional	182
11.1.3. Fluxo jurídico-operacional da auditoria soberana.....	183
11.1.4. A auditoria como instrumento de soberania.....	184
11.2. CERTIFICAÇÃO DE SOBERANIA INFORMACIONAL E COMPLIANCE SOBERANO	184
11.2.1. Natureza jurídica e finalidade da certificação soberana	185
11.2.2. Estrutura e níveis da certificação.....	185
11.2.3. O <i>compliance</i> soberano: a nova fronteira da regulação	186
11.2.4. Mecanismos de emissão e controle da certificação.....	186
11.2.5. Síntese interpretativa.....	187
11.3. METODOLOGIA DE AVALIAÇÃO DE MATURIDADE DIGITAL E GOVERNANÇA ALGORÍTMICA	187
11.3.1. Estrutura geral do modelo MNMD-S	188
11.3.2. Níveis de maturidade digital soberana.....	188
11.3.3. Governança algorítmica e mensuração de integridade de IA.....	189
11.3.4. Aplicação do INSI: mensuração e classificação nacional.....	189
11.3.5. Síntese interpretativa.....	190
11.4. ROTEIRO DE IMPLEMENTAÇÃO INSTITUCIONAL DA AUDITORIA E CERTIFICAÇÃO SOBERANA	190
11.4.1. Fase 1 – Diagnóstico e mapeamento de riscos.....	191
11.4.2. Fase 2 – Planejamento de adequação e estruturação do PPRIF.....	191
11.4.3. Fase 3 – Auditoria interna e validação cruzada regulatória	191

11.4.4. Fase 4 – Emissão da certificação soberana e registro no CNII	192
11.4.5. Fase 5 – Monitoramento contínuo e reavaliação de soberania	192
11.4.6. Modelo de governança recomendada.....	193
11.4.7. Síntese interpretativa.....	193
11.5. SÍNTESE CONCLUSIVA DO CAPÍTULO 11	194

Capítulo 12

A NOVA CIDADANIA INFORMACIONAL	195
12.1. DIREITOS FUNDAMENTAIS DIGITAIS NO AMBIENTE FINANCEIRO	195
12.1.1. O cidadão como titular e fiscal do dado financeiro	196
12.1.2. A proteção de dados como elemento de cidadania econômica	196
12.1.3. O papel do Estado e das instituições na efetivação da cidadania digital..	197
12.1.4. Síntese interpretativa.....	197
12.2. TRANSPARÊNCIA E AUTODETERMINAÇÃO INFORMATIVA.....	198
12.2.1. Fundamento constitucional da transparência informacional.....	198
12.2.2. A autodeterminação informativa como expressão da liberdade contemporânea	198
12.2.3. Transparência algorítmica e dever de explicabilidade.....	199
12.2.4. A transparência como dever de integridade e legitimidade	200
12.2.5. Síntese interpretativa.....	200
12.3. O CIDADÃO COMO AGENTE DE INTEGRIDADE INFORMACIONAL	200
12.3.1. A cidadania fiscalizadora: do controle político ao controle digital.....	201
12.3.2. A responsabilidade compartilhada na integridade digital.....	201
12.3.3. Mecanismos jurídicos de participação e denúncia	202
12.3.4. Cultura de integridade e ética digital participativa.....	202
12.3.5. Síntese interpretativa.....	203
12.4. EDUCAÇÃO CÍVICO-FINANCEIRA E CULTURA DA CONFIANÇA DIGITAL.....	203
12.4.1. A educação cívico-financeira como instrumento de soberania.....	203
12.4.2. O papel institucional da educação digital.....	204
12.4.3. A cultura da confiança digital e o pacto de integridade social.....	204
12.4.4. Educação, ética e democracia informacional.....	205
12.4.5. Síntese interpretativa.....	205

Capítulo 13

ENSAIO FINAL: SOBERANIA INFORMACIONAL NAS PLATAFORMAS DIGITAIS.....	207
13.1. O PODER ALGORÍTMICO, A REGULAÇÃO DAS PLATAFORMAS E A SOBERANIA DO ESTADO NA ERA DIGITAL	207

13.2. PLATAFORMAS COMO INFRAESTRUTURAS PRIVADAS DE PODER DURANTE MUITO TEMPO, PLATAFORMAS FORAM TRATADAS COMO “SERVIÇOS” OU “APLICATIVOS”	208
13.3. O CIDADÃO-USUÁRIO: ENTRE DIREITOS FUNDAMENTAIS E MÉTRICAS DE ENGAJAMENTO	208
13.4. PODER ALGORÍTMICO E JURISDIÇÃO INVISÍVEL.....	209
13.5. CONFLITO DE SOBERANIAS: ESTADO, MERCADO E ARQUITETURAS DIGITAIS...	210
13.6. UM CONVITE AO PRÓXIMO CAMPO DE BATALHA: DAS FINANÇAS ÀS PLATAFORMAS	211
SÍNTESE FINAL – A SOBERANIA DIGITAL COMO NOVA FRONTEIRA CONSTITUCIONAL.....	212
DO DEBATE TEÓRICO À PRÁTICA – GUIA DE USO DOS APÊNDICES	215
QUEM DEVE USAR OS APÊNDICES.....	215
COMO NAVEGAR PELOS APÊNDICES	216
TEORIA E PRÁTICA EM CAMADAS.....	217
CADERNO DE APÊNDICES TÉCNICOS E NORMATIVOS.....	219
APÊNDICE A – MAPA REGULATÓRIO DA CIBERGOVERNANÇA (BACEN, COAF, CVM, ANPD, GSI E REFERÊNCIAS CORRELATAS).....	219
1. OBJETIVO E USO PRÁTICO	219
2. ARQUITETURA REGULATÓRIA EM CAMADAS	220
3. MAPA POR ÓRGÃO – FUNÇÕES CENTRAIS EM CIBERGOVERNANÇA	220
4. FLUXOS TÍPICOS DE INTERAÇÃO NA GUERRA DOS DADOS.....	222
5. MATRIZ REGULATÓRIA SINTÉTICA	223
6. REFERÊNCIAS NORMATIVAS E INSTITUCIONAIS (NÃO EXAUSTIVAS).....	224
APÊNDICE B – TIPOLOGIAS DE INCIDENTES E VAZAMENTOS (2018–2025)	227
1. OBJETIVO E USO PRÁTICO	227
2. DIMENSÕES BÁSICAS DE CLASSIFICAÇÃO	227
3. TIPOLOGIAS PRINCIPAIS (2018–2025)	228
4. MATRIZ DE CLASSIFICAÇÃO OPERACIONAL.....	229
5. REFERÊNCIAS NORMATIVAS E INSTITUCIONAIS (NÃO EXAUSTIVAS).....	230
APÊNDICE C – QUADRO COMPARATIVO (AI ACT × LGPD × RESOLUÇÃO BCB Nº 205/2022).....	231
1. OBJETIVO E USO PRÁTICO	231
2. QUADRO COMPARATIVO SINTÉTICO.....	231
3. USO INTEGRADO EM CIBERGOVERNANÇA FINANCEIRA.....	233
4. REFERÊNCIAS NORMATIVAS E INSTITUCIONAIS (NÃO EXAUSTIVAS).....	233

APÊNDICE D – MINUTA-MODELO DE POLÍTICA INSTITUCIONAL DE CIBERGOVERNANÇA.....	235
1. OBJETIVO E USO PRÁTICO	235
2. ESTRUTURA SUGERIDA (MODELO AUDITÁVEL).....	235
3. CONTEÚDO MÍNIMO POR SEÇÃO	235
4. PAPÉIS E RESPONSABILIDADES	236
5. GESTÃO DE RISCOS, CONTROLES E INCIDENTES.....	237
6. TREINAMENTO, CULTURA E REVISÃO	238
7. REFERÊNCIAS NORMATIVAS E INSTITUCIONAIS (NÃO EXAUSTIVAS).....	238
APÊNDICE E – GLOSSÁRIO TÉCNICO-JURÍDICO DA GUERRA INFORMACIONAL	239
1. OBJETIVO.....	239
2. TERMOS E DEFINIÇÕES (SELEÇÃO).....	239
3. REFERÊNCIAS NORMATIVAS E INSTITUCIONAIS (NÃO EXAUSTIVAS).....	241
GUIA DE USO DOS APÊNDICES	243
ARSENAL PRÁTICO DA “GUERRA DOS DADOS”	243
1. POR QUE ESTES APÊNDICES EXISTEM	243
2. COMO OS APÊNDICES SE CONECTAM ENTRE SI.....	244
3. QUEM DEVE USAR O QUÊ (MAPA POR FUNÇÃO).....	245
4. TABELA RÁPIDA – “SE ACONTECER X, USE Y”.....	247
5. COMO IMPLANTAR NA PRÁTICA: ESTRATÉGIA DE ONDAS	248
6. COMO ADAPTAR SEM PERDER A ESSÊNCIA.....	249
7. MENSAGEM FINAL: SOBERANIA INFORMACIONAL COMO PRÁTICA DIÁRIA.....	251
APÊNDICE I – MODELOS DE DEFESA E COMUNICAÇÃO À ANPD	253
PARTE 1/2 – COMUNICAÇÃO DE INCIDENTE + CASO FICTÍCIO	253
1. OBJETIVO E USO PRÁTICO	253
2. DIRETRIZES GERAIS DE UTILIZAÇÃO	254
3. MODELO 1 – COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA À ANPD	255
4. CASO FICTÍCIO – INCIDENTE EM FINTECH (EXEMPLO PREENCHIDO).....	262
PARTE 2/2 – RESPOSTA, DEFESA, RIPD E CHECKLIST	264
1. MODELO 2 – OFÍCIO DE RESPOSTA E COMPLEMENTAÇÃO DE INFORMAÇÕES À ANPD.....	265
2. MODELO 3 – DEFESA ADMINISTRATIVA EM PROCESSO SANCIONADOR PERANTE A ANPD	270
3. ESTRUTURA SIMPLIFICADA DE RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD)	275
4. CHECKLIST PÓS-INCIDENTE – ROTEIRO MÍNIMO DE VERIFICAÇÃO INTERNA	278

APÊNDICE II – MODELOS DE ATENDIMENTO A TITULARES (ART. 18 LGPD)	281
PARTE 1/2 – RESPOSTAS PADRÃO E COMUNICAÇÕES EXTERNAS.....	281
1. OBJETIVO E USO PRÁTICO	281
2. DIRETRIZES GERAIS DE UTILIZAÇÃO	282
3. MODELO 1 – CONFIRMAÇÃO DE RECEBIMENTO E QUALIFICAÇÃO DO PEDIDO.....	283
4. MODELO 2 – RESPOSTA A PEDIDO DE ACESSO / COMPROVAÇÃO DE TRATAMENTO.....	285
5. CASO FICTÍCIO – MARKETPLACE “CONEXÃO LOCAL”	288
PARTE 2/2 – ELIMINAÇÃO, NEGATIVA FUNDAMENTADA, REGISTRO INTERNO E CHECKLIST	290
1. MODELO 3 – RESPOSTA A PEDIDO DE ELIMINAÇÃO / OPOSIÇÃO.....	290
2. MODELO 4 – COMUNICAÇÃO DE PRORROGAÇÃO DE PRAZO (PEDIDO COMPLEXO).....	292
3. MODELO 5 – REGISTRO INTERNO DE SOLICITAÇÃO DE TITULAR	293
4. CHECKLIST PRÁTICO – FLUXO DE ATENDIMENTO A DIREITOS (ART. 18)	295
5. CASO FICTÍCIO – CLÍNICA “VIDA PLENA 2.0” (ELIMINAÇÃO X OBRIGAÇÃO LEGAL)	297
APÊNDICE III – MODELOS CONTRATUAIS DE PROTEÇÃO DE DADOS	299
PARTE 1/2 – CLÁUSULAS-BASE PARA OPERADORES E PARCEIROS	299
1. OBJETIVO E USO PRÁTICO	299
2. DIRETRIZES GERAIS DE UTILIZAÇÃO	300
3. MODELO 1 – CLÁUSULAS ESSENCIAIS PARA CONTRATOS COM OPERADORES	301
4. CASO FICTÍCIO – FINTECH “BANCO DIGITAL ÓRBITA” E PROVEDOR DE NUVEM.....	306
PARTE 2/2 – ADITIVO ENXUTO, CO-CONTROLADORIA E DUE DILIGENCE	308
1. OBJETIVO E VISÃO GERAL.....	308
2. MODELO 2 – ADITIVO LGPD ENXUTO PARA CONTRATOS EXISTENTES.....	309
3. MODELO 3 – CLÁUSULAS PARA COMPARTILHAMENTO ENTRE CONTROLADORES/CO-CONTROLADORIA.....	313
4. CHECKLIST DE DUE DILIGENCE DE FORNECEDORES (FOCO LGPD).....	317
5. CASO FICTÍCIO – ECOSISTEMA “CARTÃO VIZINHO” (PARCERIA + ADITIVO + DUE DILIGENCE).....	319
APÊNDICE IV – PROGRAMA DE GOVERNANÇA EM PRIVACIDADE E MATRIZ DE RISCOS	321
PARTE 1/2 – PROGRAMA, POLÍTICAS, GOVERNANÇA E CHECKLIST INICIAL.....	321
1. OBJETIVO E USO PRÁTICO	321
2. DIRETRIZES GERAIS PARA MONTAR UM PROGRAMA DE PRIVACIDADE.....	322

3.	MODELO 1 – ATO/RESOLUÇÃO DA ALTA ADMINISTRAÇÃO INSTITUINDO O PROGRAMA E DESIGNANDO O DPO	323
4.	MODELO 2 – POLÍTICA CORPORATIVA DE PRIVACIDADE E PROTEÇÃO DE DADOS (ESQUELETO PRÁTICO)	327
5.	MODELO 3 – REGULAMENTO DO COMITÊ DE PRIVACIDADE, SEGURANÇA DA INFORMAÇÃO E DADOS.....	333
6.	CHECKLIST INICIAL – DIAGNÓSTICO RÁPIDO DO PROGRAMA DE PRIVACIDADE	335
	PARTE 2/2 – MATRIZ DE RISCOS, INTEGRAÇÃO COM RISCO CIBERNÉTICO E PLANO ANUAL DO DPO	338
1.	MODELO 4 – MATRIZ DE RISCOS DE PRIVACIDADE E PROTEÇÃO DE DADOS	338
2.	MODELO 5 – INTEGRAÇÃO PRIVACIDADE X RISCO CIBERNÉTICO X PLD/FT	341
3.	MODELO 6 – PLANO ANUAL DE TRABALHO DO DPO (ROTEIRO 12 MESES)	342
4.	CHECKLIST DE REVISÃO PERIÓDICA E REPORTE À ALTA ADMINISTRAÇÃO	344
	APÊNDICE V – DADOS, ANALYTICS, PERFILIZAÇÃO E INTELIGÊNCIA ARTIFICIAL.....	347
	PARTE 1/2 – PROJETOS DE ANALYTICS, PERFILIZAÇÃO E DECISÕES AUTOMATIZADAS.....	347
1.	OBJETIVO E USO PRÁTICO	347
2.	DIRETRIZES GERAIS PARA PROJETOS DE ANALYTICS, PERFILIZAÇÃO E IA.....	348
3.	MODELO 1 – TERMO / FORMULÁRIO DE ABERTURA DE PROJETO DE ANALYTICS/IA	349
4.	MODELO 2 – PARECER DE PRIVACIDADE/DPO PARA PROJETOS DE ANALYTICS/IA	353
5.	CASO FICTÍCIO – FINTECH “CRÉDITO NEXO” (SCORING, MARKETING E IA).....	357
	PARTE 2/2 – TRANSPARÊNCIA, DECISÃO AUTOMATIZADA, REVISÃO E CHECKLIST DE IA	358
1.	MODELO 3 – AVISO / CLÁUSULA DE TRANSPARÊNCIA SOBRE USO DE ANALYTICS, PERFILIZAÇÃO E IA.....	358
2.	MODELO 4 – CHECKLIST DE AVALIAÇÃO DE RISCO EM ANALYTICS/IA.....	359
3.	MODELO 5 – RESPOSTA A PEDIDO DE REVISÃO DE DECISÃO AUTOMATIZADA	361
4.	CASOS FICTÍCIOS – ANÁLISE CRUZADA	363
5.	CHECKLIST FINAL – MATURIDADE EM ANALYTICS, PERFILIZAÇÃO E IA SOB LGPD	364

APÊNDICE VI – DADOS DE COLABORADORES, RH E MONITORAMENTO NO AMBIENTE DE TRABALHO.....

	PARTE 1/2 – AVISOS, POLÍTICAS E FLUXOS DE RH.....	367
1.	OBJETIVO E USO PRÁTICO	367

2.	DIRETRIZES GERAIS PARA DADOS DE COLABORADORES E MONITORAMENTO.....	368
3.	MODELO 1 – AVISO GERAL DE PRIVACIDADE PARA COLABORADORES E CANDIDATOS.....	369
4.	MODELO 2 – CLÁUSULAS DE PROTEÇÃO DE DADOS EM CONTRATO DE TRABALHO / PRESTAÇÃO DE SERVIÇOS.....	373
5.	CASO FICTÍCIO – EMPRESA “INDÚSTRIA NOVO ELO” (RH, MONITORAMENTO E LGPD NA PRÁTICA)	376
	PARTE 2/2 – POLÍTICA INTERNA, DIREITOS DE COLABORADORES E CHECKLIST DE RH.....	377
1.	MODELO 3 – POLÍTICA INTERNA DE USO ACEITÁVEL E MONITORAMENTO.....	377
2.	MODELO 4 – FLUXO E ROTEIRO PARA ATENDIMENTO DE DIREITOS (COLABORADORES E EX-COLABORADORES).....	380
3.	MODELO 5 – CHECKLIST DE CONFORMIDADE EM RH E DADOS DE COLABORADORES	382
4.	CASOS FICTÍCIOS – RH EM CENÁRIOS DE RISCO	384
	APÊNDICE VII – SEGURANÇA DA INFORMAÇÃO APLICADA À LGPD E AO SISTEMA FINANCEIRO	387
	PARTE 1/2 – FUNDAMENTOS, MAPA DE CONTROLES E CHECKLISTS MÍNIMOS	387
1.	OBJETIVO E USO PRÁTICO	387
2.	FUNDAMENTOS JURÍDICOS DA SEGURANÇA DA INFORMAÇÃO NO SFN.....	388
3.	MAPA DE CONTROLES: DA LEI PARA A INFRAESTRUTURA TÉCNICA.....	389
4.	CHECKLIST 1 – CONTROLES TÉCNICOS MÍNIMOS (LGPD + SFN).....	389
5.	CHECKLIST 2 – CONTROLES PARA OPEN FINANCE, PIX, APIS E DREX.....	392
6.	SÍNTESE INTERPRETATIVA – PARTE 1.....	393
	PARTE 2/2 – PLAYBOOKS DE INCIDENTES, FLUXOS INTEGRADOS E CASOS FICTÍCIOS	393
1.	PLAYBOOKS TÉCNICO-JURÍDICOS DE RESPOSTA A INCIDENTES.....	393
2.	FLUXOS INTEGRADOS – SEGURANÇA, TI, JURÍDICO, DPO E COMPLIANCE.....	397
3.	CASOS FICTÍCIOS – SEGURANÇA BEM FEITA X SEGURANÇA DE FACHADA	398
4.	SÍNTESE INTERPRETATIVA – PARTE 2.....	399
	APÊNDICE VIII – LITÍGIOS, PROVA DIGITAL E ESTRATÉGIA CONTENCIOSA EM PRIVACIDADE.....	401
	PARTE 1/2 – VISÃO GERAL, MATRIZ PROBATÓRIA E MODELOS INICIAIS	401
1.	OBJETIVO E USO PRÁTICO	401
2.	DIRETRIZES GERAIS – CONTENCIOSO NA GUERRA DOS DADOS.....	402
3.	MODELO 1 – MATRIZ DE EVIDÊNCIAS E PROVA DIGITAL PÓS-INCIDENTE	402
4.	MODELO 2 – ESTRUTURA DE CONTESTAÇÃO EM AÇÃO INDIVIDUAL (VAZAMENTO DE DADOS).....	404

5. CASO FICTÍCIO – “FINTECH PULSO DIGITAL” E A ONDA DE AÇÕES	406
PARTE 2/2 – AÇÕES COLETIVAS, FLUXOS INTEGRADOS E PRONTUÁRIO PROBATÓRIO	407
1. MODELO 3 – ESTRATÉGIA EM AÇÕES CIVIS PÚBLICAS / COLETIVAS	408
2. MODELO 4 – FLUXO INTEGRADO ANPD + PROCONS + JUDICIÁRIO	410
3. CHECKLIST – “PRONTUÁRIO PROBATÓRIO” PÓS-INCIDENTE.....	412
4. CASOS FICTÍCIOS – POSTURA REATIVA X PROATIVA	414
APÊNDICE IX – PROGRAMA DE GOVERNANÇA EM PRIVACIDADE	419
PARTE 1/2 – VISÃO, ESTRUTURA E ROADMAP	419
1. OBJETIVO E USO PRÁTICO	419
2. PRINCÍPIOS DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE.....	419
3. MODELO 1 – MAPA DE GOVERNANÇA (PAPÉIS, FÓRUNS E DOCUMENTOS-CHAVE).....	420
4. MODELO 2 – ROADMAP EM ONDAS (90/180/360 DIAS)	422
5. MODELO 3 – INDICADORES (KPIS/KRIS) PARA RELATO À ALTA ADMINISTRAÇÃO	424
6. CASO FICTÍCIO – “GRUPO AURORA” MONTANDO O PROGRAMA EM 12 MESES	425
PARTE 2/2 – REGIMENTO, RELATÓRIO ANUAL E EVIDÊNCIAS DE PROGRAMA VIVO	426
1. MODELO 4 – REGIMENTO INTERNO DO COMITÊ DE PRIVACIDADE.....	426
2. MODELO 5 – RELATÓRIO ANUAL DE PRIVACIDADE PARA ALTA ADMINISTRAÇÃO	428
3. MODELO 6 – PLANO ANUAL DE TREINAMENTO E COMUNICAÇÃO	430
4. CHECKLIST FINAL – EVIDÊNCIAS DE UM PROGRAMA VIVO	432
APÊNDICE X – POLÍTICAS EXTERNAS, AVISOS E TRANSPARÊNCIA AO TITULAR	435
PARTE 1/2 – POLÍTICA DE PRIVACIDADE (SITE/APP) E ESTRUTURA GERAL.....	435
1. OBJETIVO E USO PRÁTICO	435
2. MODELO 1 – POLÍTICA DE PRIVACIDADE PARA SITE / APLICATIVO (B2C)	435
3. MODELO 2 – POLÍTICA DE PRIVACIDADE PARA COLABORADORES E CANDIDATOS (RESUMO).....	440
PARTE 2/2 – AVISOS RÁPIDOS (COOKIES, CÂMERAS, GRAVAÇÕES, WI-FI) E CASO FICTÍCIO	441
1. MODELOS DE AVISOS RÁPIDOS.....	441
2. CASO FICTÍCIO – PLATAFORMA “MERCADO URBANO” EM FISCALIZAÇÃO CONJUNTA.....	443
3. REFERÊNCIAS BIBLIOGRÁFICAS.....	445
4. COMENTÁRIO FINAL	448