

ÍNDICE GERAL

LISTA DE SIGLAS E ABREVIATURAS	5
NOTA PRÉVIA	11

CAPÍTULO I – EPISTEMOLOGIA DA PROVA

§ 1. MODELO INTEGRADO DE PROVA APLICADO A DETERMINADO CASO	19
---	----

João Gomes Neto

Introdução	20
I. A evolução do modelo de prova	22
II. O caso	25
III. Fonte de evidência e proposição	27
1. Força das generalizações	28
2. Confronto dos argumentos inferidos	29
IV. Suporte à narrativa e raciocínio abduativo	32
1. Ação central e coerência de uma narrativa	35
2. Risco da visão de túnel	36
V. Juízo de probabilidade	38
Conclusão	41
Bibliografia citada	42
Jurisprudência citada	44
Apêndice	45

§ 2. A PRODUÇÃO DA PROVA TESTEMUNHAL POR VIDEOCONFERÊNCIA: O DIREITO AO CONFRONTO E O PRINCÍPIO DA IMEDIAÇÃO	47
---	----

Alexssandra Muniz Mardegan

Introdução	48
I. O caso Maryland v. Craig	49
II. O direito ao confronto (<i>right of confrontation</i>)	51
1. Breve noção histórica do <i>right of confrontation</i> e distinção da <i>hearsay</i>	51

2. O direito ao confronto e o princípio do contraditório: conteúdo e dimensão	54
3. A distinção entre o contraditório e o direito ao confronto	56
III. O TEDH, o direito ao confronto e o processo equitativo	58
IV. O direito ao confronto é admitido no ordenamento jurídico brasileiro?	61
V. A testemunha remota e a utilização de sistema de videoconferência na produção da prova oral	65
VI. A oitiva da testemunha por videoconferência: mediação virtual?	70
Conclusão	75
Bibliografia citada	76
Jurisprudência citada	80
 § 3. A ENTOMOLOGIA FORENSE COMO MEIO DE OBTENÇÃO DE PROVA NO PROCESSO PENAL: UMA ANÁLISE DO CASO R v. TRUSCOTT	 83
<i>Analu Peixoto Barbosa</i>	
Introdução	84
I. Caso R v. Truscott	84
1. Apresentação do caso	85
2. Revisão do caso: instauração da <i>Segunda Reference Question</i>	86
3. O corpo probatório	87
II. A prova pericial entomológica	89
1. A Entomologia Forense	89
1.1. Noções gerais de aplicação	90
1.2. Estimativa de IPM	92
1.3. Limitações e confiabilidade científica	94
2. A Prova entomológica em R v. Truscott	95
III. A valoração probatória	99
1. O sistema da prova livre e a cientificidade da prova	100
2. Credibilidade do entomologista e fiabilidade das informações	103
Conclusão	107
Bibliografia citada	108
Jurisprudência citada	110
 § 4. RECONHECIMENTO DE PESSOAS NO PROCESSO PENAL: TRATAMENTO JURÍDICO ADEQUADO E ADMISSIBILIDADE DE SUA FORMA ATÍPICA	 111
<i>Maria Luiza Mezzomo</i>	
Introdução	112
I. Reconhecimento de pessoas e erro de identificação	113
II. O tratamento no direito comparado	115
1. A irrepetibilidade do meio de prova	115

2. O procedimento do reconhecimento de pessoas	117
2.1. Descrição inicial	117
2.2. Número de pessoas para comparação	119
2.3. As características similares	121
2.4. Comparação sequencial ou simultânea	123
2.5. A participação da defesa técnica	125
2.6. A presença do juiz	126
2.7. Outros aspectos	128
3. Os reconhecimentos atípicos	130
III. O reconhecimento de pessoas no Brasil	135
1. Requisitos	135
2. Os reconhecimentos atípicos	138
IV. O tratamento jurídico adequado	140
Conclusão	144
Bibliografia citada	145
Jurisprudência citada	148

CAPÍTULO II – PROVA DIGITAL

§ 5. DESENCRIPTAÇÃO DE DADOS: DEVER DO FABRICANTE? O CASO TELEGRAM	153
<i>Antonio Camilo Alberto de Brito</i>	
Introdução	154
I. O caso do bloqueio ao aplicativo <i>Telegram</i> na Rússia	155
1. O aplicativo <i>Telegram</i> e o litígio judicial na Rússia	156
2. O modelo legal russo	159
3. Precedente no TEDH: <i>Zakharov v. Rússia</i>	160
II. Privacidade v. segurança pública	161
1. Dados encriptados e direito à privacidade do usuário	161
2. Desencriptação para garantia da segurança pública	162
3. Conflito de interesses entre o fabricante e os órgãos de persecução penal	162
3.1. Ordem judicial para desencriptação de dados	164
3.2. Vulneração em massa de dados de usuários não investigados	164
3.3. Direito de resistência à ordem judicial?	166
III. Paradigmas no direito brasileiro: bloqueios ao aplicativo <i>WhatsApp</i>	166
1. Os bloqueios determinados pela justiça brasileira	167
2. A constitucionalidade das ordens de bloqueio segundo o STF	168
3. A audiência pública no âmbito das ações constitucionais referente ao <i>WhatsApp</i>	169
IV. A possível solução tecnológica: contornar a criptografia	170
1. O problema jurídico ao sabor das tecnologias?	170

2. A solução adotada na dogmática alemã	171
3. O que fazer no caso brasileiro?	172
Conclusão	173
Bibliografia citada	175
Jurisprudência citada	180
§ 6. O USO DE DISPOSITIVO DE LOCALIZAÇÃO POR GPS COMO MEIO DE OBTENÇÃO DE PROVA NO PROCESSO PENAL BRASILEIRO	181
<i>Fabrizio Pinto Weiblen</i>	
Introdução	182
I. O caso U.S. v. Jones	183
II. Tratamento no direito comparado	184
1. A privacidade como bem jurídico atingido: locais públicos e expectativas razoáveis de privacidade	184
2. A reserva de lei como exigência para métodos ocultos de investigação	188
3. Os meios de obtenção de prova atípicos	193
4. O uso da analogia nos meios de obtenção de prova	196
III. O GPS como meio de obtenção de prova no ordenamento jurídico brasileiro	200
1. Atipicidade e inovações tecnológicas no direito brasileiro	200
2. A solução quanto à localização por meio de dispositivo GPS	206
IV. O tratamento jurídico adequado	210
1. A questão da reserva de jurisdição	210
2. Outros aspectos do regime legal	214
Conclusão	218
Bibliografia citada	220
Jurisprudência citada	230
§ 7. A ATUAÇÃO DOS AGENTES ENCOBERTOS E INFILTRADOS NOS CANAIS ABERTOS E FECHADOS DE COMUNICAÇÃO EM AMBIENTE INFORMÁTICO-DIGITAL	235
<i>Frederico Pellucci</i>	
Introdução	236
I. A infiltração <i>online</i> como meio legal e constitucional de obtenção de prova	241
1. Situações hipotéticas	241
2. Infiltração policial virtual: conceito e características	242
3. Legislações processuais investigadas (Espanha, Portugal e Brasil)	246
3.1. Espanha	246
3.2. Portugal	246
3.3. Brasil	247
4. Breves considerações acerca dos princípios constitucionais atingidos pela infiltração virtual e a ponderação de valores	249

II. Os limites e as dificuldades da infiltração virtual	252
1. Os canais abertos e fechados de comunicação como limites da atuação policial	252
2. O engano e o consentimento viciado do investigado, fruto de confiança artificialmente induzida, como gerador da necessária autorização judicial	256
3. A necessidade de se separar o agente encoberto virtual do agente infiltrado virtual	260
4. <i>A infiltración de corta duración</i> e o <i>agente encubierto</i> como reforço à separação dogmática apresentada	263
5. Os contatos prévios e a validade da obtenção de prova nos canais de comunicação	265
Conclusão	269
Bibliografia citada	272
Jurisprudência citada	275
§ 8. APREENSÃO DE CORREIO ELETRÔNICO EM PORTUGAL: PRESENTE E FUTURO DE UMA QUESTÃO DE “MANIFESTA SIMPLICIDADE”	277
<i>Ricardo Wittler Contardo</i>	
Introdução	278
I. Contexto geral: evolução social e a era digital	279
II. Um caso de manifesta simplicidade	281
III. Quem deve ler primeiro?	284
IV. E agora? Um futuro possível da controvérsia	291
V. Uma outra realidade: os EUA e sua quarta emenda	293
VI. Privacidade	294
VII. Algumas formas de obtenção da prova digital	298
VIII. <i>Plain view doctrine</i>	302
Conclusão	307
Bibliografia citada	307
Jurisprudência citada	313
§ 9. PESQUISA EM SMARTPHONES NÃO ENCRIPТАDOS PELA AUTORIDADE POLICIAL, DURANTE PRISÃO EM FLAGRANTE	315
<i>Oscar Fioravanti Junior</i>	
Introdução	316
I. Caso <i>Riley v. California</i> – um novo paradigma nas buscas incidentais a prisão	317
1. Da aferição do risco à segurança – os <i>smartphones</i> podem ser usados como armas?	318
2. Da mínima possibilidade de ocultação/destruição das provas	319

II. As buscas sem mandado judicial acabaram? As exceções ao caso Riley	320
1. Buscas em regiões de fronteira – <i>border-search doctrine</i>	320
2. <i>Public school children</i>	321
3. Consentimento	322
4. <i>Parolee</i>	322
5. <i>Probationer</i>	323
6. <i>Third-party doctrine</i>	324
7. <i>Exigent circumstances</i>	325
8. <i>Abandonment</i>	326
9. Boa-fé (<i>good faith</i>)	326
III. O acesso aos dados armazenados em <i>smartphones</i> no processo penal brasileiro	327
1. Análise da CFB e das Leis n.ºs 9.296/1996 e 12.965/2014	327
2. Precedentes judiciais (Tribunais Estaduais, STJ e STF)	328
3. O problema da ausência de exceção legal ao mandado judicial prévio	330
4. O legado em Riley	334
Conclusão	335
Bibliografia citada	336
Jurisprudência citada	338
§ 10. BENEFÍCIOS DA COLETA E ARMAZENAMENTO DE EVIDÊNCIAS ELETRÔNICAS DISPONÍVEIS NA INTERNET ATRAVÉS DA TECNOLOGIA <i>BLOCKCHAIN</i> EM COMPARAÇÃO COM AS PROVAS TRADICIONALMENTE DISPONÍVEIS AOS PARTIULARES EM PORTUGAL	339
<i>Jasmine Souto Lavrador</i>	
Introdução	340
I. Tecnologia <i>Blockchain</i> e sua implementação para coleta, armazenamento e autenticação de evidências eletrônicas disponíveis na internet	342
1. A tecnologia <i>Blockchain</i>	342
2. Coleta, armazenamento e autenticação de evidências eletrônicas disponíveis na internet através da tecnologia <i>Blockchain</i> : uma realidade atualmente disponível aos particulares	345
3. Das legislações pioneiras na regulamentação de evidências eletrônicas facilitadas pela tecnologia <i>Blockchain</i> : Vermont (EUA) e China	348
II. Das provas tradicionais e das evidências facilitadas pela tecnologia <i>Blockchain</i>	350
1. Dos meios de provas tradicionalmente disponíveis aos particulares e suas falhas: certificado de fato e <i>print screen</i>	350
2. Benefícios da coleta e armazenamento de evidências eletrônicas em <i>Blockchain</i>	355
Conclusão	360

Bibliografia citada	362
Jurisprudência citada	365

CAPÍTULO III – PROVA DO BRANQUEAMENTO

§ 11. DA SUJEIÇÃO DOS <i>VIRTUAL ASSET SERVICE PROVIDERS</i> AO CUMPRIMENTO DE DEVERES DE PREVENÇÃO DO BRANQUEAMENTO DE CAPITAIS	369
<i>João Rodrigues Brito</i>	
Introdução	370
I. Primeiros conceitos	371
1. Moeda virtual: noções básicas	371
1.1. A moeda física	371
1.2. A moeda digital, a moeda virtual e a criptomoeda	371
2. As características das criptomoedas que lhes conferem um risco acrescido de utilização ilícita	373
3. Breve abordagem às vantagens das criptomoedas que podem ser prejudicadas pela sua sujeição a apertados controlos, bem como à possibilidade da previsão de sistemas de autorregulação	376
4. Intervenientes relevantes	377
4.1. Utilizadores (<i>users</i>)	377
4.2. Mineradores (<i>miners</i>)	377
4.3. Prestadores de serviços de câmbio (<i>exchanges</i>)	378
4.4. Plataformas de <i>trading</i>	379
4.5. Prestadores de serviços de carteiras digitais (<i>wallet providers</i>)	379
4.6. <i>Mixers</i> ou <i>Tumblers</i>	380
4.7. Inventores (<i>inventors</i>)	381
4.8. Emitentes ou oferentes (<i>issuers or offerors</i>)	381
II. A experiência americana	382
1. A <i>guidance</i> da FinCEN de 2013	382
2. O caso Ripple Labs	384
3. O caso BTC-e	385
4. A <i>guidance</i> da FinCEN de 2019	387
III. A atuação do GAFI e a criação da categoria dos <i>virtual asset service providers</i>	388
IV. A prevenção do branqueamento através de moeda virtual na UE: em especial, a quinta diretiva europeia do branqueamento de capitais	390
V. As respostas de algumas jurisdições e o caso português	394
Conclusão	397
Bibliografia citada	400

§ 12. REPORTE DE INFORMAÇÕES SOBRE OPERAÇÕES SUSPEITAS DE BRANQUEAMENTO DE CAPITAIS E A SUA UTILIZAÇÃO COMO PROVA NO PROCESSO PENAL	405
<i>Augusto Cesar Piaskoski</i>	
Introdução	406
I. O sistema internacional de repressão ao branqueamento de capitais e a intensificação dos mecanismos preventivos	408
II. A experiência brasileira na incorporação dos mecanismos de repressão e prevenção ao branqueamento de capitais (Lei nº 9.613/1998)	413
III. A experiência portuguesa na incorporação dos mecanismos de repressão e prevenção ao branqueamento de capitais (Lei nº 83/2017)	417
IV. Mecanismos repressivos e preventivos ao branqueamento de capitais no direito comparado	419
1. Espanha	420
2. França	421
3. Alemanha	422
4. Suíça	424
5. EUA	426
6. Quadro sinóptico	428
7. Análise comparada das medidas de repressão e prevenção ao branqueamento de capitais	430
V. Mecanismos preventivos e os deveres de comunicação de operações suspeitas	433
1. Sujeitos obrigados a reportar informações	434
2. Operações suspeitas objeto do reporte	435
3. Destinatários das informações reportadas	439
4. Sanções pela violação ao dever de comunicação	440
5. A natureza jurídica das informações reportadas	440
6. A natureza jurídica das averiguações preliminares	441
VI. O problema da utilização de informações obtidas por iniciativa privada como prova no processo penal	444
Conclusão	447
Bibliografia citada	448
Jurisprudência citada	450

CAPÍTULO IV – INCERTEZAS DAS PROIBIÇÕES DE PROVA

§ 13. A PROVA ILÍCITA OBTIDA POR PARTICULARES	453
<i>Diego Machado Tinoco de Carvalho</i>	
Introdução	454
I. O problema da prova ilícita obtida por particulares em casos concretos	455
1. Lista Falciani	455

1.1. Decisão da Audiência Provincial de Madrid 280/2016, de 29/04	456
1.2. STS 116/2017, de 23/02	457
2. Caso Liechtenstein	465
II. As proibições de prova e o direito comparado	468
1. EUA	469
2. Alemanha	472
2.1. Proibições de produção de prova e proibições de valoração de prova	473
2.2. Entendimento do <i>clean hands</i> e solução constitucional	474
2.3. Princípio da ponderação	475
2.4. Sistema estadunidense e sistema germânico: confronto	476
3. Espanha	479
III. Caso da lista Falciani	480
1. Direito à privacidade	480
2. Necessidade de realização de um juízo de proporcionalidade	481
Conclusão	481
Bibliografia citada	483
Jurisprudência citada	485
§ 14. PROVA COMPRADA: O CASO LIECHTENSTEIN LGT (2008)	487
<i>Diogo Cipriano</i>	
Introdução	488
I. O caso Liechtenstein LGT (2008)	490
1. Generalidades	490
2. Mandado de busca domiciliária à residência de KS e MS	491
3. Processo perante o AG Bochum	492
4. Processo perante o LG Bochum	494
5. Processo perante o BVerfG	495
6. Processo perante o TEDH	497
7. Apontamento conclusivo	498
II. Proposta de uma perspectiva alternativa	499
1. Do instituto das proibições de prova à teoria da ponderação	499
2. Crítica à teoria da ponderação	503
3. Do direito fundamental à autodeterminação informativa à teoria do domínio da informação	505
III. Da (in)admissibilidade de utilização/valoração da prova comprada	515
1. Ponto de ordem	515
2. Responsabilidade criminal de K. (ex-funcionário e “comerciante” de dados)	516
3. Quanto à (in)admissibilidade da compra de dados e as suas consequências	517
Conclusão	526

Bibliografia citada	529
Jurisprudência citada	532
§ 15. A REGULAÇÃO DOS MERCADOS FINANCEIROS E PROCESSO PENAL: INFORMAÇÕES OBTIDAS PELAS ENTIDADES ADMINISTRATIVAS E A SUA ADMISSIBILIDADE PROBATÓRIA EM PROCESSO	533
<i>Raquel Goldschmidt</i>	
Introdução	534
I. O mercado de valores mobiliários	535
1. A CMVM e os seus poderes: o sistema português	537
1.1. Poderes de supervisão	539
1.2. Poderes sancionatórios	540
1.3. Deveres de colaboração	541
2. Breve excuroso ao Direito Comparado	542
2.1. O paradigma alemão	542
2.2. O paradigma italiano	545
II. Supervisão financeira e processo penal	547
1. Os processos de averiguações preliminares	547
1.1. Natureza jurídica	549
1.2. Da constitucionalidade das averiguações preliminares	552
2. O princípio do <i>nemo tenetur se ipsum accusare</i>	554
2.1. Os fundamentos jurídicos do <i>nemo tenetur</i>	555
2.2. <i>Nemo tenetur</i> na CEDH	557
III. Elementos obtidos pela autoridade reguladora do mercado dos valores mobiliários e sua admissibilidade probatória em processo penal	557
1. Deveres de colaboração e direito à não auto-incriminação	557
1.1. Jurisprudência nacional	560
1.2. Restrições ao dever de colaboração no âmbito das averiguações preliminares: do direito de recusa	564
2. Proibições de prova no Processo Penal	576
2.1. Enquadramento	576
2.2. Dos meios enganosos	578
3. Análise crítica e proposta de compatibilização	581
Conclusão	584
Bibliografia citada	589
Jurisprudência citada	592