

DARIO JOSÉ KIST

*Mestre em Direitos Fundamentais,
Doutorando em Ciências Jurídico-Criminais pela Universidade Clássica de Lisboa,
Professor de Direito Penal e Processual Penal,
Promotor de Justiça.*

PROVA DIGITAL NO PROCESSO PENAL



JHMIZUNO
EDITORA DISTRIBUIDORA

15
Anos
Desde 2003

Sumário

PARTE I A ERA DIGITAL

1. Sociedade da informação e da comunicação.....	25
2. Sociedade do conhecimento?	26
3. As Tecnologias da Informação e da Comunicação (TICs) e a ampliação dos fluxos informacionais e comunicacionais.....	28
3.1. Ampliação dos fluxos informacionais e comunicacionais.....	31
3.1.1. Comunicação aberta e fechada	32
3.1.2. Comunicação presencial e não presencial ou a distância	33
3.2. A <i>World Wide Web</i>	38
3.3. Aplicações ou aplicativos de mensagens eletrônicas instantâneas	40
4. Ciberespaço	42
4.1. Uma tentativa de definição.....	42
4.2. Caracterização do ciberespaço.....	47
4.2.1. Deslocalização geográfica	47
4.2.2. Transnacionalidade	47
4.2.3. Neutralidade.....	48
4.2.4. Ausência de centralização	48
4.2.5. Espaço universal e popularizado	49
4.2.6. Espaço anonimizado.....	49
4.2.7. Espaço aberto e sujeito à (r)evolução permanente	50
4.3. Perspectivas jurídicas do ciberespaço.....	53

PARTE II CIBERCRIMINALIDADE

1. Prolegômenos	59
2. Noções sobre o surgimento e a designação dos cibercrimes	61

3. Tipologia dos cibercrimes	65
4. Tipificação dos cibercrimes	70
5. Lugar do cibercrime e desafios à territorialidade da lei penal: entre a impunidade e o <i>bis in idem</i>	76
5.1. Infrações internacionais ou transnacionais	76
5.2. Lugar do cibercrime e a territorialidade da lei penal	80
5.3. Jurisdição e soberania	87
5.4. Entre a impunidade e o <i>bis in idem</i>	92
5.5. Critérios para identificar a melhor jurisdição penal. É possível?	96

PARTE III

A PROVA DIGITAL NO PROCESSO PENAL

CAPÍTULO I

CONCEITUAÇÃO E CARACTERIZAÇÃO DA PROVA DIGITAL	105
1. Aproximações conceituais	105
1.1. Noções gerais	105
1.2. Dados digitais e sistema binário	106
1.3. Prova eletrônica ou prova digital	108
1.4. Tipologia de dados envolvidos em comunicação eletrônica	109
1.5. Endereço IP – <i>Internet Protocol</i>	112
1.6. Computação em nuvem	114
2. Caracterização da prova digital	115
2.1. Noções	115
2.2. Imaterialidade ou invisibilidade	118
2.3. Volatilidade e fragilidade	119
2.4. Dispersão	120
3. Recolha da prova digital em ambiente digital	121
3.1. Aproximações	121
3.2. Ambiente digital	122
3.3. Método de recolha da prova digital e suas etapas	123
3.3.1. Da Ciência Forense Computacional para a Ciência Forense Digital	124
3.3.2. Fases do método	125
3.3.2.1. Recolha	127
3.3.2.2. Exame	133
3.3.2.3. Análise	134

3.3.2.4. Relatório.....	134
4. Tipologia de meios de obtenção da prova digital	136

CAPÍTULO II

OS MEIOS DE OBTENÇÃO DA PROVA DIGITAL	137
1. CONSERVAÇÃO EXPEDITA DE DADOS	137
1.1. Noções conceituais	137
1.2. Tipos de dados a serem conservados	139
1.3. Importância da preservação de dados informáticos.....	140
1.4. Pessoas cujos dados podem ser conservados	140
1.5. Revelação expedita de dados de tráfego.....	142
2. INJUNÇÃO PARA APRESENTAÇÃO DE DADOS OU CONCESSÃO DE ACESSO	145
2.1. Noções conceituais	145
2.2. Tipos de dados passíveis da injunção	148
2.3. Modos de cumprimento da ordem de injunção	149
2.4. Utilidade do meio de obtenção de prova.....	150
2.5. Destinatários da injunção	150
2.6. Pessoas cujos dados podem ser objeto de injunção	151
2.7. Recusa à ordem	151
3. PESQUISA OU BUSCA E APREENSÃO DE DADOS INFORMÁTICOS.....	154
3.1. Parâmetros convencionais e legais.....	154
3.2. Pesquisa ou busca informática	158
3.2.1. Definição e natureza	158
3.2.2. Local da busca: pesquisa presencial e pesquisa remota.....	159
3.2.3. Catálogo de alvos	161
3.3. Apreensão de dados informáticos	162
3.3.1. Objeto.....	163
3.3.2. Ações precedentes.....	163
3.3.3. Local da apreensão.....	164
3.3.4. Apreensão de dados íntimos.....	164
3.3.5. Formas de execução da medida.....	166
3.3.6. Apreensão de correio eletrônico e registros de comunicações de natureza semelhante	169
4. INTERCEPTAÇÃO DE DADOS INFORMÁTICOS	173
4.1. Delineamento geral	173
4.2. Recolha de dados informáticos relativos ao tráfego	175
4.3. Interceptação de dados informáticos relativos ao conteúdo	178

4.4. Concretização da recolha e registo de dados de tráfego e da interceptação das comunicações informáticas.....	181
4.4.1. Noções gerais	181
4.4.2. Catálogo de crimes e outros requisitos.....	183
4.4.3. Pessoas visadas pela interceptação de dados e segredos	184
5. OBTENÇÃO DE MEIOS DE PROVA COM RECURSO A AÇÕES ENCOBERTAS EM MEIO DIGITAL.....	185
5.1. Aproximações metodológicas.....	185
5.2. Importância das ações encobertas em meio digital	185
5.3. O agente que realiza ações encobertas – o “homem de confiança”	187
5.3.1. Agente encoberto	189
5.3.2. Agente infiltrado	191
5.3.3. Agente provocador.....	192
5.3.4. Irrelevância da distinção entre agente encoberto e agente infiltrado.....	194
5.3.5. Diferenças entre ações encobertas no plano físico e no plano informático-digital	195
5.3.6. Ações encobertas em ambiente digital praticadas por terceiro não policial.....	199
5.4. Os meios para promover ações encobertas em ambiente digital – as buscas <i>on-line</i>	201
5.4.1. Pesquisa informática remota <i>on-line</i>	203
5.4.2. Busca <i>on-line</i> com recurso a <i>malware</i>	204
5.4.2.1. Perspectiva do instrumento: o <i>malware</i>	205
5.4.2.2. Perspectiva das finalidades: vigilância da atividade virtual e apreensão de dados mediante cópia	209
5.4.2.2.1. Observação ou vigilância <i>on-line</i> com recurso a <i>malware</i>	209
5.4.2.2.2. Apreensão <i>on-line</i> de dados informáticos com recurso a <i>malware</i> ..	211
5.4.3. Concretizações do uso de <i>malware</i> como ação encoberta	211
5.4.3.1. O caso português.....	211
5.4.3.2. A experiência norte-americana	213
5.4.3.3. O caso da Alemanha.....	214
5.4.3.4. Situação na Espanha.....	214
5.4.4. Síntese conclusiva	215
6. ACESSO TRANSFRONTEIRIÇO A SISTEMAS INFORMÁTICOS	217
6.1. Delineamentos gerais.....	217
6.2. Tese da vedação, em regra, do acesso transfronteiriço unilateral a sistemas informáticos.....	222
6.2.1. Dados existentes em fonte aberta	225
6.2.2. Dados existentes em fonte não aberta – não publicamente disponíveis	227

6.2.2.1. Acesso a dados não publicamente disponíveis mediante consentimento de quem tem autoridade sobre eles	228
6.2.2.2. Acesso a dados não publicamente disponíveis e sem o consentimento de quem tem autoridade sobre eles	230
6.2.2.2.1. Hipótese de sistema informático, cuja localização é conhecida	231
6.2.2.2.2. Hipótese de sistema informático, cuja localização é desconhecida – o problema da <i>loss of location</i>	234
6.3. Tese da permissão do acesso transfronteiriço unilateral a sistemas informáticos	238
6.3.1. Efeitos da infração à norma internacional sobre a validade da prova	244
6.3.2. Uma condição de validade do acesso transfronteiriço.....	246
7. MEIOS DE OBTENÇÃO DE PROVA DIGITAL E A LEGISLAÇÃO BRASILEIRA.....	249
7.1. Aproximações.....	249
7.2. A Lei nº 9.296/96 e a interceptação de comunicações de natureza telemática	250
7.3. Meios de obtenção de prova digital contemplados na Lei nº 12.965/14 – Marco Civil da Internet	253
7.3.1. Aproximações conceituais.....	253
7.3.2. Regulamentação específica.....	255
7.3.2.1. Diretriz genérica.....	255
7.3.2.2. Tempo de guarda dos dados de tráfego	256
7.3.2.3. Obtenção de dados sem prévia autorização judicial	256
7.3.2.4. Dados que somente podem ser obtidos mediante ordem judicial	257
7.3.2.5. Obtenção dos dados de conteúdo.....	258
7.3.3. Meios de obtenção de prova contemplados pela Lei nº 12.965/14	262
7.3.3.1. Conservação expedita de dados	262
7.3.3.2. Injunção sobre terceiros para apresentação de dados.....	263
7.4. Infiltração policial na Internet para investigar crimes contra a dignidade sexual de crianças e adolescentes – Lei nº 13.441/17	264
7.4.1. Noções iniciais	264
7.4.2. Catálogo de crimes	264
7.4.3. Regras aplicáveis.....	266
7.4.4. Hipótese de irresponsabilidade criminal do agente infiltrado.....	268
7.4.4.1. <i>Ciberpatrulha</i> , investigação em fontes abertas e infiltração	268
7.4.4.2. Os parâmetros para a (ir)responsabilidade do agente infiltrado.....	272
7.5. Os demais meios de obtenção de prova digital no Direito brasileiro	274
7.5.1. A pesquisa e apreensão de dados informáticos.....	274
7.5.2. Infiltração por quem não integra corporação policial	276
7.5.3. Ações encobertas com recurso a <i>malware</i>	278

PARTE IV

PROVA DIGITAL E AFETAÇÃO DE DIREITOS FUNDAMENTAIS

1. Nota introdutória	283
2. Tipologia de dados envolvidos em comunicação eletrônica e afetação de direitos fundamentais.....	285
3. Privacidade e intimidade	289
3.1. Desenvolvimento do direito	289
3.2. Conteúdo da intimidade: o parâmetro dos diários íntimos	293
3.3. Privacidade e intimidade e a recolha da prova digital	302
4. A proteção do domicílio	304
5. A autodeterminação informacional	310
6. Autodeterminação comunicativa.....	313
6.1. Ferramenta da autodeterminação comunicativa: a inviolabilidade das comunicações privadas.....	315
7. Proibições de prova e prova digital	316

PARTE V

A COMUNICAÇÃO PELO *WHATSAPP* COMO MEIO DE PROVA NO PROCESSO PENAL BRASILEIRO

CAPÍTULO I

A COMUNICAÇÃO POR MEIO DO <i>WHATSAPP</i>	323
1. Aproximações	323
2. Aplicações ou aplicativos de mensagens instantâneas.....	324
3. Aplicativo <i>WhatsApp</i>	325
4. Aproximações conceituais necessárias.....	327

CAPÍTULO II

ACESSO EXTERNO ÀS COMUNICAÇÕES FEITAS POR MEIO DO <i>WHATSAPP</i>	331
1. O paradigma da interceptação de comunicação telefônica.....	331
2. Regime jurídico brasileiro para a interceptação da comunicação telefônica e telemática	335
3. Incidência/não incidência do regime jurídico da interceptação telefônica às comunicações feitas pelo <i>WhatsApp</i>	338
3.1. Chamadas de voz	339
3.2. Transmissão de mensagens escritas, imagens, áudios, vídeos e arquivos.....	340
3.2.1. Comunicação em curso	340

3.2.2. Comunicação telemática.....	340
3.2.3. Palavra escrita	341
3.2.4. Regime aplicável à interceptação de mensagens escritas	344

CAPÍTULO III

INFORMAÇÕES E DADOS ARMAZENADOS NA MEMÓRIA DE DISPOSITIVO ELETRÔNICO

1. Aproximações conceituais	349
2. Valores constitucionais afetados e em colisão no acesso aos arquivos digitais	350
2.1. Nota introdutória.....	350
2.2. Intimidade e comunicação pelo <i>WhatsApp</i>	351
2.3. A proibição do déficit ou da proteção insuficiente – colisão de direitos fundamentais..	356

CAPÍTULO IV

UM REGIME JURÍDICO PARA A APREENSÃO DOS DISPOSITIVOS INFORMÁTICO-ELETRÔNICOS E O ACESSO AOS DADOS NELES ARMAZENADOS

1. Aproximações	363
1.1. Portugal.....	364
1.2. Espanha	368
2. Possibilidades da legislação brasileira	372
2.1. Apreensão de dispositivos informáticos	372
2.2. Acesso aos dados armazenados na memória de dispositivos eletrônicos	374
2.2.1. Observações gerais	374
2.2.2. A imprestabilidade do regime de apreensão de correspondência	375
2.2.3. Incidência, ou não, da Lei nº 9.296/96 no acesso a dados guardados em suporte digital.....	379
2.2.3.1. Aplicação direta.....	379
2.2.3.2. Aplicação por analogia.....	379
3. Um regime jurídico para o acesso aos arquivos digitais no Brasil	382
3.1. Considerações iniciais.....	382
3.2. Requisitos para o acesso aos dados armazenados.....	383
3.2.1. Necessidade, ou não, de autorização judicial.....	383
3.2.1.1. Aproximações	383
3.2.1.2. Um olhar sobre a jurisprudência.....	384
3.2.1.3. A insuficiência da norma que condiciona o acesso à ordem judicial ..	394
3.2.1.4. Conclusões sobre a necessidade ou não de autorização judicial para o acesso aos arquivos digitais.....	397
3.2.1.4.1. Regra geral.....	397

3.2.1.4.2. Situações excepcionais	398
a) Apreensão em busca domiciliar	398
b) Autorização do titular/detentor do aparelho	399
c) Casos de urgência devidamente justificada	400
3.2.2. Momentos para o acesso e a necessária formalização	400
3.2.3. Responsáveis pelo acesso e conhecimento do conteúdo armazenado em suporte digital.....	405
4. Dispositivo guardado por senha e privilégios contra a autoincriminação	406
4.1. Aproximações.....	406
4.2. Implicações da presunção de inocência	407
4.2.1. Âmbito de proteção decorrente da presunção de inocência.....	412
4.2.1.1. Presunção de inocência como regra de tratamento	413
4.2.1.2. Presunção de inocência como regra probatória	414
4.3. Presunção de inocência, privilégios contra a autoincriminação e direito ao silêncio	416
4.3.1. Extensão do princípio <i>nemo tenetur se ipsum accusare</i>	419
4.3.2. Natureza e fontes do princípio <i>nemo tenetur se ipsum accusare</i>	420
4.4. Há casos de colaboração coativa?	423
4.5. Compatibilização entre colaboração coativa e privilégios contra a autoincriminação ..	428
4.5.1. Reserva legal	432
4.5.2. Proporcionalidade ampla	432
4.5.3. Reserva de juiz	442
4.6. Colaboração coativa no Direito brasileiro.....	443
4.7. Soluções e conclusões sobre a revelação coativa de senha.....	449
REFERÊNCIAS	453
ÍNDICE ALFABÉTICO REMISSIVO	467